

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

---

Math Department: Class Notes and Learning  
Materials

Mathematics, Department of

---

2010

## Class Notes for Math 901/902: Abstract Algebra, Instructor Tom Marley

Laura Lynch

University of Nebraska - Lincoln, llynch@ccga.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/mathclass>



Part of the [Science and Mathematics Education Commons](#)

---

Lynch, Laura, "Class Notes for Math 901/902: Abstract Algebra, Instructor Tom Marley" (2010). *Math Department: Class Notes and Learning Materials. 2.*

<https://digitalcommons.unl.edu/mathclass/2>

This Article is brought to you for free and open access by the Mathematics, Department of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Math Department: Class Notes and Learning Materials by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

## Class Notes for Math 901/902: Abstract Algebra, Instructor Tom Marley

Topics include: Free groups and presentations; Automorphism groups; Semidirect products; Classification of groups of small order; Normal series: composition, derived, and solvable series; Algebraic field extensions, splitting fields, algebraic closures; Separable algebraic extensions, the Primitive Element Theorem; Inseparability, purely inseparable extensions; Finite fields; Cyclotomic field extensions; Galois theory; Norm and trace maps of an algebraic field extension; Solvability by radicals, Galois' theorem; Transcendence degree; Rings and modules: Examples and basic properties; Exact sequences, split short exact sequences; Free modules, projective modules; Localization of (commutative) rings and modules; The prime spectrum of a ring; Nakayama's lemma; Basic category theory; The Hom functors; Tensor products, adjointness; Left/right Noetherian and Artinian modules; Composition series, the Jordan-Holder Theorem; Semisimple rings; The Artin-Wedderburn Theorem; The Density Theorem; The Jacobson radical; Artinian rings; von Neumann regular rings; Wedderburn's theorem on finite division rings; Group representations, character theory; Integral ring extensions; Burnside's  $p^a q^b$  Theorem; Injective modules.

Prepared by Laura Lynch, University of Nebraska-Lincoln

August 2010

# 1 Chapter 1: Groups

## 1.1 Free Groups and Presentations

**Definition 1.1.** Let  $S$  be a set. Then a **free group** on  $S$  is a group  $F$  together with a map  $i : S \rightarrow F$ , usually referred to as  $(F, i)$ , with the following “universal” property: If  $G$  is any group and  $j : S \rightarrow G$  is any map, then  $\exists!$  group homomorphism  $f : F \rightarrow G$  such that  $fi = j$ , i.e., the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{i} & F \\ j \downarrow & \swarrow \exists! f & \\ G & & \end{array}$$

**Theorem 1.2.** Let  $S$  be any set. Then a free group on  $S$  exists.

*Proof.* See Lang. □

**Proposition 1.3.** Let  $S$  and  $T$  be sets of the same cardinality. Then any free group on  $S$  is isomorphic to any free group on  $T$ .

*Proof.* Let  $\ell : S \rightarrow T$  be a bijection. Let  $(F, i)$  and  $(G, j)$  be free groups on  $S$  and  $T$ , respectively.

$$\begin{array}{ccc} S & \xrightarrow{i} & F \\ \ell \downarrow & & \downarrow \\ T & \xrightarrow{j} & G \\ \ell^{-1} \downarrow & & \downarrow \\ S & \xrightarrow{i} & F \end{array}$$

Then, by the universal property  $\exists! f : F \rightarrow G$  and  $\exists! g : G \rightarrow F$ . Compacting the above commutative diagram, we see

$$\begin{array}{ccc} S & \xrightarrow{i} & F \\ i=i\ell^{-1}\ell \downarrow & \swarrow gf & \\ F & & \end{array}$$

by the uniqueness of the universal property, as we have the homomorphism  $gf : F \rightarrow F$  and the identity homomorphism  $1_F : F \rightarrow F$ , that  $gf = 1_F$ . Similarly, by swapping the  $S$  and  $T$  in the diagrams above, we see  $fg = 1_G$ . Thus  $f$  and  $g$  are bijective homomorphisms and thus  $f$  is an isomorphism. □

**Corollary 1.4.** Let  $S$  be a set and  $(F_1, i_1)$  and  $(F_2, i_2)$  free groups on  $S$ . Then  $\exists!$  isomorphism  $f : F_1 \rightarrow F_2$  such that  $fi_1 = i_2$ .

Thus we can now talk about the unique (up to isomorphism) free group on a set.

**Proposition 1.5.** Let  $S$  be a set and  $(F, i)$  the free group on  $S$ . Then  $i$  is injective.

*Proof.* Suppose not, that is,  $i(x) = i(y)$  for  $x \neq y \in S$ . Consider the homomorphism  $j : S \rightarrow \mathbb{Z}_2$  defined by  $s \mapsto 0$  for  $s \neq x$  and  $x \mapsto 1$ . Then we have the commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{i} & F \\ j \downarrow & \swarrow f & \\ \mathbb{Z}_2 & & \end{array}$$

where  $f$  is the unique homomorphism given by the universal property of free groups. Now

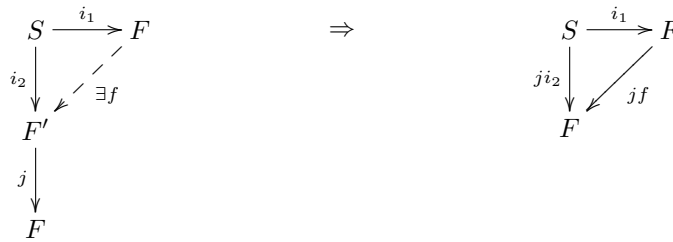
$$0 = j(y) = fi(y) = fi(x) = j(x) = 1,$$

which is clearly a contradiction. □

Thus, we can now identify  $S$  with its image  $i(S) \subseteq F$ . For simplicity we will simply say  $S \subseteq F$ . Also, we will now simply say  $F(S)$  is the free group for  $S$ .

**Proposition 1.6.** *The set  $S$  generates  $F(S)$ .*

*Proof.* Let  $F'$  be the subgroup of  $F = F(S)$  generated by  $S$ .



By the uniqueness of the universal property,  $jf = 1_{F'}$ . Thus  $jf$  is a surjection, which implies  $j$  is surjective. Thus  $F' = F$ . □

If  $|S| = n$ , call  $F(S)$  the free group on  $n$  generators. So  $F(S) = \{s_1^{e_1} \cdots s_k^{e_k} \mid s_i \in S, e_i = \pm 1\}$ . Note that since homomorphisms preserve order and commutativity we can not have any conditions like  $s^n = 1$  or  $s_1s_2 = s_2s_1$  as these conditions do not hold in all groups. Thus there are no relations on the elements of  $S$ , which is why we say  $F(S)$  is the *free* group. [For example, say  $s^n = 1$  and consider  $j : S \rightarrow \mathbb{Z}$  where  $j(s) = 2$ . Then, there exists a homomorphism  $f : F(S) \rightarrow \mathbb{Z}$ . Then  $2 = j(s) = f(i(s)) = f(s)$ . If  $s^n = 1$ , then  $2^n = 1$ , a contradiction].

**Example.** What is the free group on one element, i.e.,  $S = \{x\}$ ?

Since  $S$  generates  $F(S)$ , we know  $F(S) = \langle x \rangle$ . By above,  $x$  does not have finite order. Thus  $F(S)$  is infinite cyclic, which says  $F(S) \cong \mathbb{Z}$ . Note: This is the only abelian free group.

**Definition 1.7.** Let  $F$  be the free group on a set  $S$  and  $R$  any subset of  $F$ . Let  $N$  be the intersection of all normal subgroups of  $F$  containing  $R$  (i.e.,  $N$  is the smallest normal subgroup containing  $R$ ). Then  $F/N$  is called the group generated by  $S$  with relations  $R = 1$ . Write  $F/N = \langle S \mid R = 1 \rangle$  and call it a **presentation** for  $F/N$ .

**Definition 1.8.** Say a group  $G$  has the presentation  $\langle S \mid R = 1 \rangle$  if  $G \cong F(S)/N$  where  $N$  is the smallest normal subgroup of  $F(S)$  containing  $R$ . Here  $G$  is defined by the generators  $S$  and relations  $R$ .

**Example.** What group  $G$  is defined by the presentation  $\langle x, y \mid x^2 = 1, y^3 = 1, xyxy = 1 \rangle$ ?

Here,  $G = \langle x, y \rangle$  where  $x^2 = 1, y^3 = 1, yx = xy^2$ . Thus  $G = \{x^i y^j \mid i = 0, 1, j = 0, 1, 2\}$ . Clearly,  $G$  could be the trivial group, but let's see if there is a nontrivial group for this presentation.

Define  $j : \{x, y\} \rightarrow S_3$  by  $x \mapsto (12)$  and  $y \mapsto (123)$ . By the universal property of the free group,  $\exists!$  group homomorphism  $f : F(\{x, y\}) \rightarrow S_3$  such that  $f(x) = (12)$  and  $f(y) = (123)$ . Note that since  $(12)$  and  $(123)$  generate  $S_3$ ,  $f$  is surjective.

With a little work, we see  $x^2, y^3, xyxy \in \ker f$  and since  $\ker f \triangleleft F(\{x, y\})$  and  $N$  is the smallest normal subgroup containing  $x^2, y^3, xyxy$ , we have  $N \subseteq \ker f$ . Thus we have

$$G \cong F(S)/N \twoheadrightarrow F(S)/\ker f \twoheadrightarrow S_3$$

by the First Isomorphism Theorem. Therefore we have the surjective homomorphism  $\psi : G \twoheadrightarrow S_3$ . Of course, as  $|G| \leq 6$  we see  $G \cong S_3$ .

Here, we saw that the trivial group could be presented by any given presentation. However, in practice we want to find the largest group that satisfies the relations.

**Claim:** Let  $D_{2n}$  be the group of symmetries of a regular  $n$ -gon. Let  $f$  be any reflection and  $r$  a rotation by  $2\pi/n$  radians. Then  $D_{2n}$  has the presentation  $G = \langle x, y \mid x^2 = 1, y^n = 1, xyxy = 1 \rangle$ .

*Proof.* By the same argument as above,  $|G| \leq 2n$ . Now, define a homomorphism  $f : F(\{x, y\}) \rightarrow D_{2n}$  by  $x \mapsto f$  and  $y \mapsto r$ . As above,  $x^2, y^n, xyxy \in \ker f$  which gives us the surjective mapping  $F/N \twoheadrightarrow F/\ker f \twoheadrightarrow D_{2n}$ . Thus we find  $F/N \cong D_{2n}$ .  $\square$

## 1.2 Automorphisms

**Definition 1.9.** Let  $G$  be a group. An **automorphism** of  $G$  is an isomorphism  $f : G \rightarrow G$ . Let  $\mathbf{Aut}(G)$  denote the group of all automorphisms of  $G$ . Let  $g \in G$ . An **inner automorphism** of  $G$  is an isomorphism of the form  $\psi_g : G \rightarrow G$  such that  $x \mapsto gxg^{-1}$ . Clearly  $(\psi_g)^{-1} = \psi_{g^{-1}}$  and  $\psi_g\psi_h = \psi_{gh}$ . Thus the set of inner automorphisms forms a group, which we will denote  $\mathbf{Inn}(G)$ . In fact,  $\mathbf{Inn}(G) \triangleleft \mathbf{Aut}(G)$ . Thus, we can define  $\mathbf{Aut}(G)/\mathbf{Inn}(G)$  as the group of **outer automorphisms**.

**Notation.** Let  $R$  be a ring with 1. Let  $R^* = \{u \in R \mid u \text{ is a unit in } R\}$ . This is a group under multiplication.

**Theorem 1.10.** Let  $C_n = \langle a \rangle$  denote the cyclic group of order  $n$ . Then  $\mathbf{Aut}(C_n) \cong \mathbb{Z}_n^*$ .

*Proof.* Define  $\phi : \mathbb{Z}_n^* \rightarrow \mathbf{Aut}(C_n)$  by  $\bar{k} \mapsto \psi_{\bar{k}}$  where  $\psi_{\bar{k}} : C_n \rightarrow C_n$  is such that  $a \mapsto a^k$ . Since if  $\gcd(k, n) = 1$ , then  $|a^k| = n$ , we know  $\langle a^k \rangle = \langle a \rangle = C_n$ . Thus  $\psi$  is surjective and therefore injective (as the image has the same order). Therefore  $\psi$  is an isomorphism and  $\phi$  is well-defined. Clearly,  $\phi$  defines a homomorphism. Thus it remains to show it is injective and surjective. Notice if  $\bar{k} \in \ker \phi$ , then  $\psi_{\bar{k}} = 1_{C_n}$  which implies  $\psi_{\bar{k}} = a^k = a$ . Thus  $n \mid k - 1$ , that is,  $\bar{k} = 1$  which implies  $\ker \phi = \{1\}$  and  $\phi$  is injective. Also  $\psi_{\bar{k}} \in \mathbf{Aut}(G)$  if and only if  $\langle a^k \rangle = \langle a \rangle$  which happens if and only if  $\gcd(k, n) = 1$ . Thus  $\phi$  is surjective and therefore an isomorphism.  $\square$

**Example.**  $\mathbf{Aut}(C_{15}) \cong \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ . As none of those elements have order 8, the group is not cyclic. Thus  $\mathbf{Aut}(G)$  is not always cyclic. In general, let  $n = pq$  where  $p, q$  are odd primes. By the Chinese Remainder Theorem,  $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$ . Thus  $\mathbb{Z}_n^* \cong (\mathbb{Z}_p \times \mathbb{Z}_q)^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$ . Since  $p-1, q-1$  are not relatively prime (they are both even), this is not cyclic.

**Theorem 1.11.** Let  $F$  be a field and  $H$  a finite subgroup of  $F^*$ . Then  $H$  is cyclic.

*Proof.* Since a field is commutative,  $H$  is a finite abelian group. Thus all subgroups of  $H$  are normal and, in particular, the Sylow subgroups are unique by the Second Sylow Theorem. Therefore  $H$  is the internal direct product of its Sylow subgroups, that is,  $H \cong P_1 \times \cdots \times P_l$  where  $P_i$  are the Sylow subgroups. If we show all of the  $P_i$  are cyclic, we will be done. WLOG, assume  $|H| = p^n$ , that is, there is only one Sylow subgroup. By the Fundamental Structure Theorem for finitely generated groups,  $H \cong C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}$  where  $n_1 \geq n_2 \geq \cdots \geq n_k$ . Since  $p^{n_i} \mid p^{n_1}$  for all  $i$ ,  $h^{p^{n_1}} = 1$  for all  $h \in H$ . Since  $F$  is a field, every element of  $H$  is therefore a root of  $x^{p^{n_1}} - 1$ . This polynomial has  $\leq p^{n_1}$  roots, which implies  $|H| \leq p^{n_1}$ . Then  $H \cong C_{p^{n_1}}$  and thus  $H$  is cyclic.  $\square$

**Corollary 1.12.** For a prime  $p$ ,  $\mathbb{Z}_p^*$  is cyclic, as  $\mathbb{Z}_p$  is a field.

**Corollary 1.13.**  $\mathbf{Aut}(C_p) \cong \mathbb{Z}_p^* \cong C_{p-1}$ .

**Example.** Find an automorphism of  $C_{13}$  of order 6.

By above,  $\mathbf{Aut}(C_{13}) \cong C_{12}$ , which has an element of order 6. By brute force, we see  $o(4) = 6$ . Thus, if  $C_{13} = \langle a \rangle$ , then the automorphism  $a \mapsto a^4$  has degree 6.

**Example.** Find an automorphism of  $C_{55}$  of order 20.

By the Chinese Remainder Thm,  $\text{Aut}(C_{55}) \cong \mathbb{Z}_{55}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_{11}^* \cong C_4 \times C_{10}$ . We know 2 is an element of  $C_4$  of order 4 and 4 is an element of  $C_{10}$  of order 5. Thus we want  $x \in \mathbb{Z}_{55}^*$  such that  $x \equiv 2 \pmod{5}$  and  $x \equiv 4 \pmod{11}$ . Brute force tells us  $x = 37$  works. Thus  $\phi : C_{55} \rightarrow C_{55}$  defined by  $a \mapsto a^{37}$  is an automorphism of order 20.

**Theorem 1.14.** *Let  $p$  be an odd prime,  $n \geq 1$ . Then  $\text{Aut}(C_{p^n})$  is cyclic of order  $p^n - p^{n-1}$ .*

*Proof.* We know  $|\text{Aut}(C_{p^n})| = |\mathbb{Z}_{p^n}^*| = p^n - p^{n-1}$ .

Claim: Let  $p$  be prime,  $n \geq 1$ . Let  $1 \leq i \leq p^n$ . Write  $i = p^j x$  where  $p \nmid x$ . Then  $p^{n-j} \mid \binom{p^n}{i}$  but  $p^{n-j+1} \nmid \binom{p^n}{i}$ .

Claim: Let  $p$  be prime. Then  $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ .

Proof: By the Binomial Theorem,  $(1+p)^{p^{n-1}} = \sum_{i=0}^{p^n} \binom{p^{n-1}}{i} p^i$ . Let  $1 \leq i \leq p^n, i = p^j x$  as above. Note that  $i \geq p^j \geq j+1$ . Thus  $p^{j+1} \mid p^i$ . Also  $p^{n-j-1} \mid \binom{p^{n-1}}{i}$ . Multiplying these together gives us  $p^n \mid \binom{p^{n-1}}{i} p^i$ , which implies  $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ .

Claim: Let  $p > 2$ . Then  $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$ .

Proof: Let  $1 \leq i \leq p^n, i = p^j x$  as above. If  $j = 0$ , then  $p^{n-2} \mid \binom{p^{n-2}}{i}$ . Since, for  $i \geq 2$ , we have  $p^2 \mid p^i$  we know  $p^n \mid \binom{p^{n-2}}{i} p^i$ . If  $j \geq 1, i \geq p^j \geq j+2$  and so  $p^{j+2} \mid p^i$ . Also  $p^{n-j-2} \mid \binom{p^{n-2}}{i}$ . Combining these, we see  $p^n \mid \binom{p^{n-2}}{i} p^i$ . Thus the only nonzero terms are  $i = 0, 1$ . Thus  $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \not\equiv 1 \pmod{p^n}$ .

Thus  $1+p$  is an element of order  $p^{n-1}$  in  $\mathbb{Z}_{p^n}^*$ . As  $\mathbb{Z}_{p^n}^*$  is abelian, all its subgroups are normal, which implies the Sylow subgroups are unique and  $\mathbb{Z}_{p^n}^*$  is the internal direct product of its Sylow subgroups. Thus it is enough to show every Sylow subgroup is cyclic. Note  $|\mathbb{Z}_{p^n}^*| = p^{n-1}(p-1)$ . Consider the Sylow  $p$ -subgroup. Since  $1+p$  has order  $p^{n-1}$ , it is a generator for the Sylow subgroup and thus the Sylow  $p$ -subgroup is cyclic. Let  $q$  be any other prime such that  $q \mid p^{n-1}(p-1)$ . Let  $Q$  be the Sylow  $q$ -subgroup of  $\mathbb{Z}_{p^n}^*$ . Define the homomorphism  $\psi : \mathbb{Z}_{p^n}^* \rightarrow \mathbb{Z}_p^*$  by  $[a]_{p^n} \mapsto [a]_p$ , that is, send an element to its corresponding residue class. Since  $\gcd(a, p^n) = 1$  if and only if  $\gcd(a, p) = 1$ , the map is well-defined. Clearly the map is surjective and  $|\ker \psi| = p^{n-1}$ . Thus  $Q \cap \ker \psi = 1$  and  $\psi|_Q$  is injective. So  $Q$  is isomorphic to a subgroup of  $\mathbb{Z}_p^*$ , a cyclic group. Since subgroups of cyclic groups are cyclic,  $Q$  is cyclic. Thus all Sylow subgroups are cyclic and therefore  $\mathbb{Z}_{p^n}^*$  is cyclic.  $\square$

**Note.** If  $p = 2$ , then  $\mathbb{Z}_{2^n}^*$  is not cyclic for  $n > 2$ . For example, in  $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ , all nontrivial elements have order 2.

**Example.** If  $F$  is a field, then  $\text{GL}_n(F) = \{\phi : F^n \rightarrow F^n \mid \phi \text{ is a vector space isomorphism}\}$ .

**Remark 1.15.** *Suppose  $|F| = q$ . Then  $|\text{GL}_n(F)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ .*

*Proof.* Fix a basis  $e_1, \dots, e_n$  for  $F^n$ . Then  $\phi$  is determined by the values  $\phi(e_1), \dots, \phi(e_n)$ , which must be a basis for  $F^n$ . Then  $|\text{GL}_n(F)|$  = the number of distinct ordered bases for  $F^n$ . There are  $q^n - 1$  choices for  $e_1, q^n - q$  for  $e_2$ , etc.  $\square$

**Proposition 1.16.** *Let  $G = \underbrace{C_p \times \cdots \times C_p}_n$ . Then  $\text{Aut}(G) \cong \text{GL}_n(\mathbb{Z}_p)$ . Thus  $|\text{Aut}(G)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ .*

*Proof.* Using additive notation,  $G \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_n$ . This is a  $\mathbb{Z}_p$  vector space. Thus any group homomorphism  $\phi : G \rightarrow G$  is actually a  $\mathbb{Z}_p$  linear transformation as  $\phi(\overline{a(h_1, \dots, h_n)}) = \overline{a\phi(\overline{h_1}, \dots, \overline{h_n})}$ . So every bijective linear transformation of  $G$  is a group homomorphism and vice versa. Thus  $\text{Aut}(G) \cong \text{GL}_n(\mathbb{Z}_p)$ .  $\square$

### 1.3 Semi Direct Products

Let  $H, K$  be groups and  $\phi : K \rightarrow \text{Aut}(H)$ , a group homomorphism. Define

$$H \rtimes_{\phi} K = \{(h, k) | h \in H, k \in K\}$$

and

$$(h_1, k_1)(h_2, k_2) = (h_1\phi(k_1)(h_2), k_1k_2).$$

**Claim.**  $H \rtimes_{\phi} K$  is a group.

Proof: Clearly,  $(1, 1)$  is the identity. Also  $(h, k)^{-1} = (\phi(k^{-1})(h^{-1}), k^{-1})$  as

$$\begin{aligned} (h, k)(\phi(k^{-1})(h^{-1}), k^{-1}) &= (h\phi(k)(\phi(k^{-1})(h^{-1})), kk^{-1}) \\ &= (h(\phi(k)\phi(k^{-1}))(h^{-1}), 1) \\ &= (h\phi(kk^{-1})(h^{-1}), 1) \\ &= (hh^{-1}, 1) \\ &= (1, 1) \end{aligned}$$

and

$$\begin{aligned} (\phi(k^{-1})(h^{-1}), k^{-1})(h, k) &= (\phi(k^{-1})(h^{-1})\phi(k^{-1})h, k^{-1}k) \\ &= (\phi(k^{-1})(h^{-1}h), 1) \\ &= (\phi(k^{-1})(1), 1) \\ &= (1, 1). \end{aligned}$$

Lastly, associativity holds. □

**Definition 1.17.** Say  $H \rtimes_{\phi} K$  is the (**external**) **semidirect product** of  $H$  and  $K$  (and  $\phi$ ). (Note: If  $\phi(k) = 1$  for all  $k \in K$ , then the semidirect product is the usual direct product.)

**Example.** Find a nonabelian group of order 21.

Take  $K = C_3 = \langle a \rangle$  and  $H = C_7 = \langle b \rangle$ . To find  $\phi$  we want to send  $a$  to an element of order  $o(a)$  in  $\text{Aut}(C_7)$ . So let  $\phi : C_3 \rightarrow \text{Aut}(C_7)$  be defined by  $a \mapsto \psi$  where  $\psi : C_7 \rightarrow C_7$  is such that  $b \mapsto b^2$ . Thus we can now define  $G = C_7 \rtimes_{\phi} C_3$ . We know  $G$  is nonabelian as

$$(b, 1)(1, a) = (b\phi(1)(1), a) = (b, a)$$

and

$$(1, a)(b, 1) = (\phi(a)(b), a) = (b^2, a).$$

For simplicity, let's say  $\bar{a} = (1, a)$  and  $\bar{b} = (b, 1)$ . Notice  $(b^i, a^j) = (b^i, 1)(1, a^j) = (b, 1)^i(1, a)^j = \bar{b}^i \bar{a}^j$ . Then we see that  $\bar{a}^3 = 1, \bar{b}^7 = 1$ , and  $\bar{a}\bar{b} = \bar{b}^2\bar{a}$ .

What's a presentation for  $G$ ? Let  $H = \langle x, y | x^3 = 1, y^7 = 1, xy = y^2x \rangle$ . As before, we can show  $|H| \leq 21$  and map it onto  $G$ , so the map is bijective and thus  $G$  is isomorphic to  $H$ .

Let  $G = H \rtimes_{\phi} K$ . There are the natural injective homomorphisms  $i_1 : H \rightarrow G$  such that  $h \mapsto (h, 1)$  and  $i_2 : K \rightarrow G$  such that  $k \mapsto (1, k)$ . Let  $H' = i_1(H)$  and  $K' = i_2(K)$ .

**Remarks.**

1.  $G = H'K'$  as  $(h, k) = (h, 1)(1, k) \in H'K'$
2.  $H' \cap K' = \{(1, 1)\}$
3.  $H' \triangleleft G$  since  $(h', k)(h, 1)(h', k)^{-1} = (h', k)(h, 1)(\phi(k^{-1})(h'^{-1}), k^{-1}) = (*, 1) \in H'$ .

**Proposition 1.18.**  $K' \triangleleft H \rtimes_{\phi} K$  if and only if  $\phi$  is trivial. In this case, the semidirect product is exactly the direct product.

*Proof.* ( $\Leftarrow$ ): Easy

( $\Rightarrow$ ): Let  $h \in H, k \in K$ . Want to show  $\phi(k)(h) = h$ . Since  $H', K' \triangleleft G$  and  $H' \cap K' = \{(1, 1)\}$ , we know that  $h'k' = k'h'$  for all  $h' \in H', k' \in K'$ . Thus  $(h, k) = (h, 1)(1, k) = (1, k)(h, 1) = (\phi(k)h, k)$ . Thus  $\phi(k)h = h$ .  $\square$

**Corollary 1.19.**  $H \rtimes_{\phi} K$  is abelian if and only if  $\phi$  is trivial and  $H, K$  are abelian.

**Definition 1.20.** Let  $G$  be an abelian group. Then  $f : G \rightarrow G$  such that  $g \mapsto g^{-1}$  is an automorphism of the group, called the **inversion map**. Note  $o(f) = 2$ , except when every element is its own inverse.

**Example.** Let  $n > 2$ . Define  $\phi : C_2 \rightarrow \text{Aut}(C_n)$  where  $C_2 = \langle x \rangle$  and  $C_n = \langle y \rangle$  such that  $x \mapsto$  the inversion map. Then  $C_n \rtimes_{\phi} C_2$  is a nonabelian group of order  $2n$ . (In fact, its the dihedral group.) Notice

$$(1, x)(y, 1)(1, x)^{-1} = (\phi(x)y, x)(1, x^{-1}) = (\phi(x)y\phi(x)(1), 1) = (\phi(x)y, 1) = (y^{n-1}, 1).$$

Thus we get the presentation

$$\langle x, y \mid x^2 = 1, y^n = 1, xyx^{-1} = y^{n-1} \rangle.$$

**Theorem 1.21.** Let  $G$  be a group and  $H, K$  subgroups such that

$$(1) G = HK \quad (2) H \cap K = \{1\} \quad (3) H \triangleleft G$$

Then  $\phi : K \rightarrow \text{Aut}(H)$  defined by  $k \mapsto \psi_k(h) = khk^{-1}$  is a group homomorphism and  $G \cong H \rtimes_{\phi} K$ . In this case, we say  $G$  is the **internal semidirect product** of  $H$  and  $K$ .

*Proof.* Define  $f : H \rtimes_{\phi} K \rightarrow G$  by  $(h, k) \mapsto hk$ . Then  $f$  is a group homomorphism as

$$f((h_1, k_1)(h_2, k_2)) = f((h_1\phi(k_1)h_2, k_1k_2)) = f((h_1k_1h_2k_1^{-1}, k_1k_2)) = h_1k_1h_2k_2 = f((h_1, k_1))f((h_2, k_2)).$$

Also,  $f$  is surjective as  $G = HK$  implies that for  $g \in G$  there exists  $h, k$  such that  $g = hk$  and thus  $(h, k) \mapsto g$ . Finally,  $f$  is injective as if  $(h, k) \mapsto 1$  then  $hk = 1$  which implies  $k = h^{-1} \in H \cap K = \{1\}$  and so  $k = 1$  and similarly  $h = 1$  and thus  $\ker f = \{(1, 1)\}$ .  $\square$

**Theorem 1.22.** Let  $G$  be a group of order  $2p$  where  $p$  is an odd prime. Then  $G \cong C_{2p}$  or  $G \cong D_{2p}$ .

*Proof.* Let  $P$  be the Sylow  $p$ -subgroup (By 3ST, there exists only one and it is normal). Let  $Q$  be the Sylow 2-subgroup. Then, since  $|P \cap Q| = 1$ , we know  $G = PQ$ . Thus there exists  $\phi : Q \rightarrow \text{Aut}(P)$  such that  $G \cong P \rtimes_{\phi} Q$ . Since  $|Q| = 2$ , we know  $Q \cong C_2 = \langle x \rangle$ . Similarly,  $P \cong C_p = \langle y \rangle$ . Now,  $\text{Aut}(C_p) \cong \mathbb{Z}_p^*$  and so we have two cases.

Case 1: If  $\phi(x) = 1_P$ , then  $G \cong P \times Q \cong C_{2p}$ .

Case 2: If  $|\phi| = 2$ , there exists a unique element of order 2, as  $\mathbb{Z}_p^*$  is cyclic. Clearly, its  $-1$ . Then  $\phi(x)(y) = y^{-1}$ , that is,  $\phi$  is the inversion map. By our previous example, this says  $G \cong D_{2p}$ .  $\square$

**Theorem 1.23.** Let  $K$  be a cyclic group of order  $n$  and  $H$  be any group. Suppose  $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$  are group homomorphisms. If  $\phi_1(K)$  and  $\phi_2(K)$  are conjugate in  $\text{Aut}(H)$  (that is,  $\phi_1(k) = \psi\phi_2(k)\psi^{-1}$  for  $\psi \in \text{Aut}(H)$ ), then  $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$ .

**Special Cases.**

1. If  $|\phi_1(K)| = |\phi_2(K)|$  and  $\text{Aut}(H)$  is cyclic, since there is only one subgroup of each order, they are equal.
2. If  $\phi_1(K), \phi_2(K)$  are Sylow  $p$ -subgroups for some  $p$ , they are conjugate by 2ST.



**Example.** Classify all groups of order  $75 = 3 \cdot 5^2$ .

Let  $P \in \text{Syl}_3(G)$  and  $Q \in \text{Syl}_5(G)$ . By 3ST,  $Q \triangleleft G$ . So  $G = Q \rtimes_{\phi} P$  for some  $\phi$ . Now  $P \cong C_3 = \langle x \rangle$  and since  $Q$  has order  $5^2$  it is abelian and thus either  $Q \cong C_{25}$  or  $Q \cong C_5 \times C_5$ .

Case 1:  $Q \cong C_{25}$ . Then  $|\text{Aut}(Q)| = |\mathbb{Z}_{25}^*| = 25 - 5 = 20$ . Since  $3 \nmid 20$ ,  $\phi$  is trivial. Thus we have  $G \cong C_3 \times C_{25} \cong C_{75}$ .

Case 2:  $Q \cong C_5 \times C_5 = \langle y, z \rangle$ . Then  $\text{Aut}(Q) = GL_2(\mathbb{Z}_5)$ , which has order  $(5^2 - 5)(5^2 - 1) = 20 \cdot 24$ . Now if we have  $\phi = 1$ , then  $G \cong C_{15} \times C_5$ . Otherwise,  $|\phi| = 3$  which implies it is a Sylow 3-subgroup and thus all  $\phi$  of this order yield an isomorphic semidirect product. Now, let's try to find a presentation for this group. We know  $x^3 = 1, y^5 = z^5 = 1, yz = zy$ , however we need to know what  $xyx^{-1}$  and  $xzx^{-1}$  are. One can see that  $\begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$  has order 3 in  $GL_2(\mathbb{Z}_5)$ . This corresponds to  $\psi : Q \rightarrow Q$  such that  $y \mapsto yz^2$  and  $z \mapsto yz^3$  (take  $y = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $z = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ ). Thus we see that  $G$  is presented by  $\langle x, y, z \mid x^3 = y^5 = z^5 = 1, yz = zy, xy = yz^2x, xz = yz^3x \rangle$ .

**Example.** Classify all groups of order  $20 = 2^2 \cdot 5$ .

Let  $Q \in \text{Syl}_5(G)$  and  $P \in \text{Syl}_2(G)$ . Then, by the 3ST,  $Q \triangleleft G$  and also we know  $Q \cong C_5 = \langle y \rangle$ . Now  $P$  has order  $2^2$  which implies it is abelian and thus  $P \cong C_4$  or  $P \cong C_2 \times C_2$ . Define  $G = Q \rtimes_{\phi} P$  where  $\phi : P \rightarrow \text{Aut}(Q) \cong \mathbb{Z}_5^*$ .

Case 1:  $P = C_4 = \langle x \rangle$ .

Case 1a:  $\phi$  is trivial. Then  $G = C_5 \times C_4 = C_{20}$ .

Case 1b:  $|\phi(P)| = 2$ . There is only one subgroup of  $\mathbb{Z}_5^*$  of order 2, since it's cyclic. Since  $y \mapsto y^4$  works, we're done. So  $xyx^{-1} = y^4$  and this group is presented by  $\langle x, y \mid x^4 = 1, y^5 = 1, xyx^{-1} = y^{-1} \rangle$ .

Case 1c:  $|\phi(P)| = 4$ . Then  $\phi(P)$  is a Sylow subgroup, which says all possible  $\phi$  here will be isomorphic- so we can choose any one. We see  $y \mapsto y^2$  works, so  $xyx^{-1} = y^2$ . This group is presented by  $\langle x, y \mid x^4 = 1, y^5 = 1, xyx^{-1} = y^2 \rangle$ .

We just need to check that these are different. In case 1b, we see  $x^2 \in Z(G)$ . We will show that  $Z(G) = 1$  in case 1c. Let  $Z$  be the center of  $G$  and suppose  $Z \neq \{1\}$ . First note that  $Z \cap Q = \{1\}$ . If not, then (as the order of  $Q$  is prime)  $Q \subseteq Z$ . But this means  $Q$  commutes with every element of  $P$ , implying that  $\phi = \{1\}$ . Thus, if  $Z \neq \{1\}$ , it must contain an element, say  $z$ , of order 2. But as  $z$  is in some Sylow 2-subgroup and every Sylow 2-subgroup is conjugate to  $P$ , we must have  $z \in P$  (a conjugate of  $z$  is still  $z$ !). But then  $\phi(z) = \text{identity map}$ , contradicting that  $\phi$  is an isomorphism. Hence,  $Z = 1$ . Thus the groups really are different.

Case 2:  $P = C_2 \times C_2$

Case 2a:  $\phi$  is trivial. Then  $G \cong C_2 \times C_{10}$ .

Case 2b:  $|\phi(P)| = 4$ . This would say  $\phi$  was an isomorphism, contradiction since  $P$  is not cyclic but  $\mathbb{Z}_5^*$  is.

Case 2c:  $|\phi(P)| = 2$ . Then  $|\ker \phi| = 2$ . Let  $x \in \ker \phi \setminus \{1\}$  and  $z \in P \setminus \{\ker \phi\}$ . Then  $P = \langle x, z \rangle$ . ( $P$  is generated by any 2 nonidentity elements.) Since  $x \in \ker \phi$ ,  $x \in Z(G)$ . Let  $Q' = Z(G)Q = \langle x, y \rangle \cong C_{10} = \langle xy \rangle$  and  $P' = \langle z \rangle \cong C_2$ . Note  $G = P'Q'$  (since  $G$  is generated by  $x, y, z$ ),  $P' \cap Q' = \{1\}$ ,  $Q' \triangleleft G$ . Therefore  $G \cong C_{10} \rtimes_{\phi'} C_2$  which implies  $D_{20}$ . This is clearly not isomorphic to the other 2 as the Sylow 2 subgroup is  $C_2 \times C_2$ .

**Example.** Classify all groups of order 30.

Let  $G$  be a group,  $|G| = 30$ . Let  $P \in \text{Syl}_2(G), Q \in \text{Syl}_3(G), R \in \text{Syl}_5(G)$ . By Sylows Theorems,  $n_3 \in \{1, 10\}, n_5 \in \{1, 6\}$ . If  $n_3 = 10$ , there exists 20 elements of order 3 and if  $n_5 = 6$ , there exists 24 elements of order 5, but there are only 30 elements total. So either  $n_3 = 1$  or  $n_5 = 1$ . Thus either  $Q$  or  $R$  is normal. So  $QR$  is indeed a subgroup (since one of  $Q$  and  $R$  are normal). But  $[G : QR] = 2$  implies  $QR \triangleleft G$  and further  $QR$  is cyclic (since it is of the form  $pq$  where  $p \nmid q - 1$ .) [Note: This shows  $Q$  and  $R$  are normal: Let  $Q' \in \text{Syl}_3(G)$ . Then  $Q' = xQx^{-1}$  for some  $x \in G$ . As

$Q \subseteq QR \triangleleft G, Q' = xQx^{-1} \subseteq xQRx^{-1} = QR$ . Since  $QR$  is cyclic, it has only 1 subgroup of order 3 which implies  $Q' = Q$ . Hence  $n_3 = 1$  and  $Q \triangleleft G$ . Similarly,  $R \triangleleft G$ .] Let  $QR = \langle b \rangle$  and  $P = \langle a \rangle$ . Since  $G = P(QR), QR \cap P = \{1\}$  and  $QR \triangleleft G$ , we get  $G = QR \rtimes_{\phi} P$  for  $\phi : P \rightarrow \text{Aut}(QR)$ . Now,  $|\phi(P)| \mid 2$  and  $|\phi(P)| \mid |\text{Aut}(QR)|$ . Since  $\text{Aut}(QR) \cong \mathbb{Z}_{15}^*$  which has 3 elements of order 2: 4, 11, 14, there are 3 possibilities for a nontrivial  $\phi$ .

Case 1:  $\phi_1(a) = \psi_1 : QR \rightarrow QR$  defined by  $b \mapsto b^{-1}$ . Then  $G_1 \cong D_{30}$ .

Case 2:  $\phi_2(a) = \psi_2 : QR \rightarrow QR$  defined by  $b \mapsto b^4$ . Then  $G_2$  is presented by  $\langle x, y \mid x^2 = y^{15} = 1, xyx^{-1} = y^4 \rangle$ .

Case 3:  $\phi_3(a) = \psi_3 : QR \rightarrow QR$  defined by  $b \mapsto b^{11}$ . Then  $G_3$  is presented by  $\langle x, y \mid x^2 = y^{15} = 1, xyx^{-1} = y^{11} \rangle$ .

Case 4:  $\phi$  is trivial and  $G_4 \cong C_{30}$ .

How do we know  $G_1, G_2, G_3$  are different? Since  $G_i/Z(G_i)$  cyclic implies  $G$  is abelian,  $|Z(G_i)| \in \{1, 2, 3, 5\}$ . If  $|Z(G_i)| = 2$ , some Sylow 2 subgroup is in the center which implies all Sylow 2 subgroups are in the center (since the Sylow 2 subgroups are conjugate), which implies  $n_2 = 1$ , that is  $P \triangleleft G$ . Thus  $G$  is abelian, a contradiction. So  $|Z(G_i)| \in \{1, 3, 5\}$ . If  $|Z(G_i)| = 3$ , then  $Z(G_i) = Q = \langle b^5 \rangle$  (since there is only one Sylow 3 subgroup) and if  $|Z(G_i)| = 5$ , then  $Z(G_i) = R = \langle b^3 \rangle$ . In  $G_1, ab^3a^{-1} = b^{-3} = b^{12}$  which implies  $b^3 \notin Z(G_1)$ . Similarly  $b^5 \notin Z(G_1)$ . Thus  $Z(G_1) = 1$ . In  $G_2$ , we see  $ab^5a^{-1} = b^{20} = b^5$ . Thus  $Z(G_2) = \langle b^5 \rangle$ . Similarly,  $Z(G_3) = \langle b^3 \rangle$ . Thus they are all different. Now, we know  $Z(S_3 \times C_5) \geq 5$ , so  $G_3 \cong S_3 \times C_5$ . Similarly,  $G_2 \cong D_{10} \times C_3$ .

Suppose  $m \mid n$ . Then  $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  defined by  $[a]_n \mapsto [a]_m$  is a surjective ring homomorphism.

**Lemma 1.24.** *Suppose  $m \mid n$ . Then the group homomorphism  $f^* : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_m^*$  is surjective.*

*Proof.* Suppose  $n = p^s$  for some prime  $p$ . Then  $m = p^r$  where  $r \leq s$ . If  $[a]_{p^r} \in \mathbb{Z}_{p^r}^*$ , then  $[a]_{p^s} \in \mathbb{Z}_{p^s}^*$ . So  $f^*$  is surjective. In general, let  $n = p_1^{s_1} \cdots p_k^{s_k}$  for  $p_1, \dots, p_k$  distinct primes. Then  $m = p_1^{r_1} \cdots p_k^{r_k}$  where  $r_i \leq s_i$ . Using the Chinese Remainder Theorem, we see

$$\begin{array}{ccc} \mathbb{Z}_n^* & \longrightarrow & \mathbb{Z}_m^* \\ \downarrow \cong & & \downarrow \cong \\ \mathbb{Z}_{p_1^{s_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{s_k}}^* & \longrightarrow & \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^* \end{array}$$

By the previous case, the bottom map is surjective. Since the bottom three maps are surjective, the top is as well.  $\square$

**Corollary 1.25.** *Suppose  $m \mid n$  and  $\gcd(a, m) = 1$ . Then there exists  $t \in \mathbb{Z}$  such that  $\gcd(a + tm, n) = 1$ .*

*Proof.* Let  $[a]_m \in \mathbb{Z}_m^*$ . As  $f^* : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_m^*$  is onto, there exists  $[c]_n \in \mathbb{Z}_n^*$  such that  $f([c]_n) = [a]_m$ . Thus  $\gcd(c, n) = 1$  and  $c \equiv a \pmod{m}$  which implies  $c = a + tm$ .  $\square$

**Corollary 1.26.** *Let  $\phi : C_n \rightarrow C_m$  be a surjective group homomorphism (thus  $m \mid n$ ). Let  $C_n = \langle a \rangle$  and  $C_m = \langle b \rangle$ . Then  $b = \phi(a)^r$  where  $\gcd(r, n) = 1$ .*

*Proof.* Since  $\langle \phi(a) \rangle = C_m = \langle b \rangle$ ,  $b = \phi(a)^s$  where  $\gcd(s, m) = 1$ . By the previous corollary, there exists  $t \in \mathbb{Z}$  such that  $\gcd(s + tm, n) = 1$ . Let  $r = s + tm$ . Then  $\phi(a)^r = \phi(a)^{s+tm} = \phi(a)^s \phi(a)^{tm} = \phi(a)^s = b$ .  $\square$

**Theorem 1.27.** *Let  $K$  be a cyclic group of order  $n$  and  $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$  be group homomorphisms, where  $H$  is some group. Suppose  $\phi_1(K)$  and  $\phi_2(K)$  are conjugate. Then  $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$ .*

*Proof.* Let  $\sigma \in \text{Aut}(H)$  be such that  $\phi_2(K) = \sigma \phi_1(K) \sigma^{-1}$ . Let  $K = \langle a \rangle$ . Then  $\phi_2(K) = \sigma \langle \phi_1(a) \rangle \sigma^{-1} = \langle \sigma \phi_1(a) \sigma^{-1} \rangle$ . Then  $\phi_2 : K \rightarrow \langle \sigma \phi_1(a) \sigma^{-1} \rangle$  is a surjective group homomorphism. By the corollary, there exists  $r \in \mathbb{Z}$  with  $\gcd(r, n) = 1$  such that  $\sigma \phi_1(a) \sigma^{-1} = \phi_2(a)^r$ . Let  $x \in K$ . Then  $x = a^s$  for some  $s$ . Then

$$\sigma \phi_1(x) \sigma^{-1} = (\sigma \phi_1(a) \sigma^{-1})^s = (\phi_2(a)^r)^s = (\phi_2(a)^s)^r = \phi_2(x)^r.$$

Thus  $\sigma\phi_1(x) = \phi_2(x)^r\sigma$ . Define  $f : H \rtimes_{\phi_1} K \rightarrow H \rtimes_{\phi_2} K$  by  $(h, k) \mapsto (\sigma(h), k^r)$ . Then

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f((h_1\phi_1(k_1)(h_2), k_1k_2)) \\ &= (\sigma(h_1\phi_1(k_1)(h_2)), (k_1k_2)^r) \\ &= (\sigma(h_1)\sigma(\phi_1(k_1)(h_2)), k_1^rk_2^r) \\ &= (\sigma(h_1)\phi_2(k_1)^r\sigma(h_2), k_1^rk_2^r) \\ &= (\sigma(h_1), k_1^r)(\sigma(h_2), k_2^r) \\ &= f((h_1, k_1))f((h_2, k_2)). \end{aligned}$$

Thus  $f$  is a homomorphism. Also, we know it is 1-1 and onto as  $h \mapsto \sigma(h)$  and  $k \mapsto k^r$  are automorphisms (since  $\gcd(r, n) = 1$ ). Thus  $f$  is an isomorphism.  $\square$

## 1.4 Characteristic Groups

**Definition 1.28.** Let  $G$  be a group. A subgroup  $H$  of  $G$  is called *characteristic* if  $\sigma(H) = H$  for all  $\sigma \in \text{Aut}(G)$ . We denote this as  $H \text{ char } G$ .

**Example.**  $Z(G) \text{ char } G$ . To see this, let  $\sigma \in \text{Aut}(G)$ ,  $x \in Z(G)$  and  $y \in G$ . Then  $y = \sigma(z)$  for some  $z \in G$  and

$$\sigma(x)y = \sigma(x)\sigma(z) = \sigma(xz) = \sigma(zx) = \sigma(z)\sigma(x) = y\sigma(x).$$

So  $\sigma(x) \in Z(G)$ . So  $\sigma(Z(G)) \subseteq Z(G)$  for all  $\sigma \in \text{Aut}(G)$  which implies  $\sigma^{-1}(Z(G)) \subseteq Z(G)$  for all  $\sigma$  and applying  $\sigma$ , we see  $Z(G) \subseteq \sigma(Z(G))$ . Thus  $Z(G) = \sigma(Z(G))$ .

### Remarks.

1. If  $H$  is a unique subgroup of  $G$  of order  $|H|$ , then  $H \text{ char } G$ . Therefore, every subgroup of a cyclic group is characteristic.

**Example.** Let  $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ . Then  $\phi : G \rightarrow G$  defined by  $(a, b) \mapsto (b, a)$  is an automorphism but  $\phi(\langle (1, 0) \rangle) = \langle (0, 1) \rangle$ . So  $\langle (1, 0) \rangle$  is not characteristic in  $G$ .

2. Characteristic subgroups are always normal.

*Proof:* Let  $g \in G$ . Then  $\psi_g : G \rightarrow G$  defined by  $x \mapsto gxg^{-1}$  is an automorphism. If  $H \text{ char } G$ , then  $gHg^{-1} = \psi_g(H) = H$ . Thus  $H \triangleleft G$ .

**Note:** The converse is not true (see previous example).

3. Let  $P \in \text{Syl}_p(G)$ . Then  $P \text{ char } G$  if and only if  $P \triangleleft G$ .

*Proof:* ( $\Leftarrow$ ): If  $P \triangleleft G$ , then  $P$  is the only Sylow  $p$ -subgroup. Done by Remark 1.

**Note.** If  $K \triangleleft H$  and  $H \triangleleft G$  does NOT imply  $K \triangleleft G$ .

**Example.**  $D_8 = \langle x, y \mid x^2 = y^4 = 1, xy = y^3x \rangle$ . We see  $\langle xy \rangle \triangleleft \{1, xy, xy^3, y^2\} \triangleleft D_8$  (the first because a group of order 4 is abelian and the second because its index 2). However,  $\langle xy \rangle \not\triangleleft D_8$ .

### Remarks.

1.  $K \text{ char } H$  and  $H \text{ char } G$  implies  $K \text{ char } G$ .

*Proof:* Let  $\phi \in \text{Aut}(G)$ . As  $H \text{ char } G$ ,  $\phi(H) = H$  which implies  $\phi|_H \in \text{Aut}(H)$  and thus  $\phi(K) = \phi|_H(K) = K$  as  $K \text{ char } H$ . So  $K \text{ char } G$ .

2.  $K \text{ char } H$  and  $H \triangleleft G$  implies  $K \triangleleft G$ .

*Proof:* Let  $g \in G$  and consider  $\psi_g \in \text{Aut}(G)$  where  $\psi_g(x) = gxg^{-1}$ . As  $H \triangleleft G$ ,  $\psi_g(H) = H$ . In particular,  $\psi_g|_H \in \text{Aut}(H)$ . Since  $K \text{ char } H$ ,  $\psi_g(K) = \psi_g|_H(K) = K$ . Thus  $K \triangleleft G$ .

**Example.** (Old Comp Problem) Let  $P \in \text{Syl}_p(G)$ . Then  $N_G(N_G(P)) = N_G(P)$ , where  $N_G(H) = \{g \in G | gHg^{-1} = H\}$ .

*Proof.* Clearly,  $P \triangleleft N_G(P)$  implies  $P$  char  $N_G(P)$  (since Sylow  $p$ -subgroups are normal if and only if they are characteristic). But  $N_G(P) \triangleleft N_G(N_G(P))$ . By Remarks 2,  $P \triangleleft N_G(N_G(P))$ . Thus  $N_G(N_G(P)) \subseteq N_G(P)$  and since the other containment is obvious, they are equal.

## 1.5 Solvable Groups

**Definition 1.29.** Let  $G$  be a group and  $x, y \in G$ . Define the **commutator** of  $x$  and  $y$  by

$$[x, y] := xyx^{-1}y^{-1}.$$

The commutator subgroup of  $G$ , denoted  $[G, G]$  or  $G'$ , is the subgroup of  $G$  generated by all its commutators.

**Remarks.**

1.  $x, y$  commute if and only if  $[x, y] = 1$ .
2.  $G$  is abelian if and only if  $G' = \{1\}$ .
3.  $G'$  char  $G$

*Proof:* Let  $\phi \in \text{Aut}(G)$ ,  $x, y \in G$ . Then  $\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = [\phi(x), \phi(y)]$ . So  $\phi(G') \subseteq G'$ . If  $[x, y]$  is a generator of  $G'$ , then there exists  $a, b \in G$  such that  $\phi(a) = x, \phi(b) = y$  which implies  $\phi([a, b]) = [x, y]$ . Thus  $G' \subseteq \phi(G')$  and so they are equal.

**Lemma 1.30.** Let  $G$  be a group. Then

1.  $G' \triangleleft G$  and  $G/G'$  is abelian.
2. If  $H \supseteq G'$ , then  $H \triangleleft G$  and  $G/H$  is abelian.
3. If  $H \triangleleft G$  and  $G/H$  is abelian, then  $H \supseteq G'$ .

*Proof.* 1. As  $G'$  char  $G$ ,  $G' \triangleleft G$ . Let  $\bar{x}, \bar{y} \in G/G'$ . Then  $\overline{xyx^{-1}y^{-1}} = \bar{1}$  which implies  $\overline{xy} = \overline{yx}$  which implies  $G/G'$  is abelian.

2. If  $H \supseteq G'$ ,  $H/G' \triangleleft G/G'$  which is abelian. Thus  $H/G' \triangleleft G/G'$  which implies  $H \triangleleft G$ . Note  $G/H \cong \frac{G/G'}{H/G'}$  is abelian as  $G/G'$  was.

3. Let  $[x, y]$  be a commutator. Then, as  $G/H$  is abelian,  $\overline{[x, y]} = \overline{[x, y]} = \overline{xyx^{-1}y^{-1}} = \bar{1}$ . Thus  $[x, y] \in H$  and therefore  $H \supseteq G'$ . □

**Definition 1.31.** A sequence of subgroups  $\cdots G_i \triangleleft G_{i-1} \triangleleft \cdots G_0 = G$  is called a **normal series**. The **derived normal series** is  $\cdots G''' \triangleleft G'' \triangleleft G' \triangleleft G$ . For simplicity, we will take  $G^{(0)} = G$ ,  $G^{(1)} = G'$ , and  $G^{(i)} = (G^{(i-1)})'$  for  $i \geq 2$ .

**Example.** Let  $G = S_3$ . Then,  $G' = \langle (123) \rangle$ .

*Proof.* As  $\langle (123) \rangle \triangleleft S_3$  (index 2) and  $G / \langle (123) \rangle$  is abelian (its cyclic), the above lemma says  $\langle (123) \rangle \supseteq S_3'$ . As  $S_3'$  is nonabelian,  $S_3' \neq \{1\}$ . So  $S_3' = \langle (123) \rangle$ .

Now  $\langle (123) \rangle$  is abelian, so  $(S_3)'' = \{1\}$ . Thus

$$\{1\} \triangleleft \langle (123) \rangle \triangleleft S_3$$

is the derived normal series for  $S_3$ .

**Definition 1.32.** A group is **solvable** if  $G^{(n)} = \{1\}$  for some  $n$ .

**Remark.** Suppose  $\phi : A \rightarrow B$  is a surjective group homomorphism. Then  $\phi(A^{(i)}) = B^{(i)}$  for all  $i$ .

*Proof.* Induct on  $i$ . If  $i = 0$ , clear. Suppose true for  $i - 1$ . Want to show  $\phi((A^{(i-1)})') = (B^{(i-1)})'$ . For simplicity, we can take  $i = 1$ . Know  $\phi([a, b]) = [\phi(a), \phi(b)]$ . Thus  $\phi(A') \subseteq B'$ . On the other hand, as  $\phi$  is surjective, any commutator of  $B$  is the image of a commutator of  $A$ .

**Special Case.** Suppose  $H \triangleleft G$  and  $\phi : G \rightarrow G/H$  is the natural homomorphism. Then  $\overline{G^{(i)}} = \overline{G}^{(i)}$ .

**Proposition 1.33.** *Let  $G$  be a group and  $H \leq G$ .*

1. *If  $G$  is solvable, then so is  $H$ . Furthermore, if  $H \triangleleft G$ , the  $G/H$  is solvable.*

2. *If  $H \triangleleft G$  and  $H$  and  $G/H$  are solvable, then so is  $G$ .*

*Proof.* 1. For some  $n$ ,  $G^{(n)} = \{1\}$ . But  $H^{(i)} \subseteq G^{(i)}$  for all  $i$ . Thus  $H^{(n)} = \{1\}$ . Also, if  $H \triangleleft G$ , then  $(G/H)^{(n)} = \overline{G^{(n)}} = \overline{\{1\}}$ .

2. Since  $G/H$  is solvable, there exists  $n$  such that  $\overline{G^{(n)}} = (G/H)^{(n)} = \{1\}$ . Thus  $G^{(n)} \subseteq H$ . Since  $H$  is solvable, there exists  $m$  such that  $H^{(m)} = \{1\}$ . Then  $G^{(n+m)} \subseteq H^{(m)} = \{1\}$ . Thus  $G$  is solvable.  $\square$

**Proposition 1.34.** *Let  $G$  be a group of order  $p^n$ ,  $p$  prime. Then  $G$  is solvable.*

*Proof.* Induct on  $n$ . If  $n = 0, 1, 2$ , then  $G$  is abelian and thus  $G' = \{1\}$ . So suppose  $n \geq 3$ . Recall that  $p$ -groups have nontrivial center. Since  $Z(G)$  is abelian, it is solvable. Now  $|G/Z(G)| = p^r$  for some  $r < n$ . Thus  $G/Z(G)$  is solvable by induction and by Proposition 1.33,  $G$  is solvable.  $\square$

**Fact.**  $A_n$  is not solvable for  $n \geq 5$ . We know  $A_n$  is simple and nonabelian for  $n \geq 5$ . Since the commutator is a normal subgroup,  $(A_n)^{(i)} = A_n$  for all  $i \geq 1$ . Thus  $A_n$  is not solvable. By Prop 1.33, we see  $S_n$  is therefore not solvable for  $n \geq 5$  as then its subgroup  $A_n$  would be. Note:  $A_4$  is solvable (see later)

**Note.** Since  $G'$  char  $G$  and  $G^{(2)}$  char  $G'$ , we know that  $G^{(2)}$  char  $G$  and by induction,  $G^{(n)}$  char  $G$ . In particular, this says  $G^{(n)} \triangleleft G$ .

**Definition 1.35.** *A solvable series for a group  $G$  is a normal series*

$$\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$$

*such that  $G_i/G_{i-1}$  is abelian for all  $i$ .*

**Proposition 1.36.**  *$G$  is solvable if and only if  $G$  has a solvable series.*

*Proof.* ( $\Rightarrow$ ): The derived normal series is a solvable series for  $G$ .

( $\Leftarrow$ ): Let  $\{1\} = G_n \triangleleft \cdots \triangleleft G_0 = G$  be a solvable series for  $G$ . Induct on  $n$ . If  $n = 0$ , then  $G = \{1\}$  and we are done. Let  $n > 0$ . Then  $G_1$  has a solvable series of length  $n - 1$ . So  $G_1$  is solvable by induction. Also  $G/G_1$  is abelian, which implies it is solvable. Then, since  $G_1$  and  $G/G_1$  is solvable,  $G$  is solvable by Prop 1.33.  $\square$

**Fact.**  $A_4$  is solvable. We see it has the solvable series

$$\{1\} \triangleleft \{(1), (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \triangleleft S_4.$$

Thus  $A_4$  and  $S_4$  are solvable.

**Lemma 1.37.** *If  $|G| = pq$  for primes  $p, q$ , then  $G$  is solvable.*

*Proof.* If  $p = q$ , then  $G$  is abelian and thus solvable. Say  $p < q$ . By ST, the Sylow  $q$ -subgroup is normal and solvable (since abelian). Of course  $|G/Q| = p$  implies  $G/Q$  is abelian and thus solvable. Thus by Prop 1.33,  $G$  is solvable.  $\square$

**Proposition 1.38.** *Every group of order  $pqr$  for primes  $p, q, r$  is solvable.*

*Proof.* Case 1:  $p = q = r$ . Then done by Prop 1.36.

Case 2:  $p < q < r$ . By counting arguments, at least one of the Sylow subgroups is normal and hence solvable, say  $H$ . Then  $|G/H| = p'q'$  for primes  $p', q'$  and is thus solvable by the lemma. Thus by Prop 1.33,  $G$  is solvable.

Case 3:  $|G| = p^2q, p < q$ . Similar.

Case 4:  $|G| = pq^2, p < q$ . Similar. □

## 2 Fields

**Definition 2.1.** A **field** is a commutative ring with identity such that every nonzero element has a multiplicative inverse. Let  $R$  be a ring with identity. Consider the ring homomorphism  $\phi : \mathbb{Z} \rightarrow R$  defined by  $n \mapsto n \cdot 1_R$ . Say  $R$  has **characteristic 0** if  $\phi$  is injective. Otherwise, if  $\ker \phi = (n)$ , then  $R$  has **characteristic  $n$** . In this case  $\mathbb{Z}/(n) \hookrightarrow R$ . If  $R$  is a domain, then so is  $\mathbb{Z}/(n)$  which says  $(n)$  is prime. In particular, if  $R$  is a field, then  $\text{char } R = 0$  or  $(p)$  for some prime  $p$ . Let  $R$  be a commutative domain. Then the **fraction field** or **quotient field** of  $R$  is  $Q(R) = \{\frac{a}{b} | a, b \in R, b \neq 0\}$ .

**Note.** Instead of saying a field  $F$  has characteristic 0, it is often said that  $F$  contains the rationals. This is because if  $\mathbb{Z} \rightarrow F$  defined by  $n \mapsto n \cdot 1$  is injective, then  $\mathbb{Z} \subseteq F$  which implies its quotient field  $Q(F) = \mathbb{Q} \subseteq F$ .

**Remark.** If  $R$  is a domain, then  $R[x]$  is a domain. In this case,  $Q(R[x]) = Q(R)(x) = \{\frac{f}{g} | f, g \in Q(R)[x], g \neq 0\}$ .

**Notation.** Let  $F \subseteq E$  be fields. Usually, we will say  $E/F$  is a field extension.

### 2.1 Algebraic Extensions

**Definition 2.2.** Let  $E/F$  be a field extension,  $\alpha \in E$ . Then  $\alpha$  is **algebraic** over  $F$  if there exists  $f(x) \in F[x] \setminus \{0\}$  such that  $f(\alpha) = 0$ . If  $\alpha$  is not algebraic, we say it is **transcendental**. The **degree** of  $E/F$ , denoted  $[E : F]$ , is the dimension of  $E$  as an  $F$ -vector space. We say  $[E : F]$  is finite if  $[E : F] < \infty$ .

**Examples.**

1. If  $x$  is an indeterminate, then  $F(x)/F$  is a field extension and  $[F(x) : F] = \infty$  as  $\{1, x, x^2, \dots\}$  is an  $F$ -basis for  $F(x)$ .
2.  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$  as  $\{1, \sqrt{2}\}$  is a  $\mathbb{Q}$ -basis.

**Lemma 2.3.** Let  $L \subseteq F \subseteq E$  be fields. Then  $[E : L] = [E : F][F : L]$ .

**Proposition 2.4.** Let  $\alpha \in E$ ,  $E/F$  a field extension. TFAE

1.  $\alpha$  is algebraic over  $F$ .
2.  $F[\alpha] = F(\alpha)$ .
3.  $[F(\alpha) : F] < \infty$ .

*Proof.* (1)  $\Rightarrow$  (2) : Define  $\phi : F[x] \rightarrow F[\alpha]$  by  $f(x) \mapsto f(\alpha)$ . Then  $\phi$  is a surjective ring homomorphism. Thus  $F[\alpha] \cong F[x]/(\ker \phi)$ . Since  $F[x]$  is a PID, we know  $\ker \phi = (h(x))$  for some  $h(x) \in F[x]$ . Since  $\alpha$  is algebraic over  $F$ , we know  $\ker \phi \neq 0$ . So  $h(x) \neq 0$ . Since  $F[\alpha] \subseteq F(\alpha)$ , it's an integral domain. Thus  $\ker \phi$  is prime and  $h(x)$  is irreducible over  $F$  (as if it factored, the factors would be zero divisors). So  $(h(x))$  is a maximal ideal which implies  $F[x]/(h(x))$  is a field. Thus  $F[\alpha] = F(\alpha)$ .

(2)  $\Rightarrow$  (3) : If  $\alpha = 0$ , trivial. So let  $\alpha \neq 0$ . Then  $\frac{1}{\alpha} \in F(\alpha) = F[\alpha]$ . So  $\frac{1}{\alpha} = c_0 + c_1\alpha + \dots + c_n\alpha^n$  for  $c_n \neq 0$ . Multiplying by  $\frac{\alpha}{c_n}$ , we see  $\alpha^{n+1} \in \text{Span}_F\{1, \alpha, \dots, \alpha^n\}$  which implies  $\alpha^i \in \text{Span}_F\{1, \alpha, \dots, \alpha^n\}$  for all  $i$ . Then  $\dim_F F[\alpha] \leq n + 1$  which implies  $[F(\alpha) : F] \leq n + 1$ .

(3)  $\Rightarrow$  (1) : Say  $[F(\alpha) : F] = n$ . Then  $\{1, \alpha, \dots, \alpha^n\}$  is a linearly dependent set over  $F$ . Thus there exists  $c_0, \dots, c_n \in F$  (not all zero) such that  $c_0 \cdot 1 + \dots + c_n\alpha^n = 0$  which implies  $\alpha$  is a root of  $f(x) = c_0 + \dots + c_nx^n$ . Thus  $\alpha$  is algebraic.  $\square$

**Corollary 2.5.** Let  $\{\alpha_1, \dots, \alpha_n\} \in E$ ,  $E/F$  a field extension. TFAE

1.  $\alpha_1, \dots, \alpha_n$  is algebraic over  $F$ .
2.  $F[\alpha_1, \dots, \alpha_n] = F(\alpha_1, \dots, \alpha_n)$ .
3.  $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$ .

**Proposition 2.6.** If  $[E : F] < \infty$ , then  $E/F$  is algebraic.

*Proof.* Let  $\alpha \in E$ . Then  $[F(\alpha) : F] \leq [E : F] < \infty$ . By Prop 2.4,  $\alpha$  is algebraic.  $\square$

**Note.** The converse is not true. Consider  $\mathbb{Q} \subseteq \mathbb{C}$  and let  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ . Clearly,  $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$  and  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ .

**Proposition 2.7.** Suppose  $E/F$  and  $F/L$  are algebraic. Then  $E/L$  is also algebraic.

*Proof.* Let  $\alpha \in E$ . Then  $\alpha$  is algebraic over  $F$  which implies  $[F(\alpha) : F] < \infty$ . Say  $f(\alpha) = 0$  where  $f(x) = c_nx^n + \dots + c_0 \in F[x] \setminus \{0\}$ . Let  $K = L(c_0, \dots, c_n)$ . Then  $K/L$  is finite and  $\alpha$  is algebraic over  $K$ . Then  $[K(\alpha) : L] = [K(\alpha) : K][K : L] < \infty$ . Thus  $\alpha$  is algebraic over  $L$ .  $\square$

**Proposition 2.8.** Let  $E/F$  be a field extension,  $\alpha \in E$  algebraic over  $F$ . Say  $h \in F[x] \setminus \{0\}$  such that  $h(\alpha) = 0$ . TFAE

1.  $h(x)$  is irreducible over  $F$ .
2.  $h \mid f$  for all  $f(x) \in F[x]$  such that  $f(\alpha) = 0$ .
3.  $h(x) = \ker \phi$  for  $\phi : F[x] \rightarrow F[\alpha]$ .

If  $h$  is monic and satisfies the above, say  $h$  is the **minimal polynomial** for  $\alpha$  over  $F$  and denote it by  $\text{Irred}(\alpha, F)$  or  $\text{Min}(\alpha, F)$ .

**Proposition 2.9.** Suppose  $\alpha$  is algebraic over  $F$ . Then  $[F(\alpha) : F] = \deg \text{Irred}(\alpha, F)$ .

**Definition 2.10.** Let  $F$  be a field and  $f(x) \in F[x] \setminus F$ . Then a **splitting field** for  $f(x)$  over  $F$  is a field  $L \supseteq F$  such that  $f(x)$  factors into linear factors in  $L[x]$  and  $f(x)$  does not split in  $E[x]$  for all  $F \subseteq E \subsetneq L$ .

**Remark.** Let  $f(x) \in F[x]$  and  $E \supseteq F$  such that  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$  in  $E[x]$ . Then a splitting field for  $f(x)$  over  $F$  is  $F[\alpha_1, \dots, \alpha_n]$ .

**Examples.**

1. Find the splitting field of  $x^4 - 2$  over  $\mathbb{Q}$ .

The roots of  $x^4 - 2$  are  $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ . So  $\mathbb{Q}(\sqrt[4]{2}, i)$  is the splitting field.

$$\begin{array}{l|l} \mathbb{Q}(\sqrt[4]{2}, i) & \\ \hline | 2 & \text{since } x^2 + 1 \text{ is irreducible as } i \notin (\sqrt[4]{2}). \\ \mathbb{Q}(\sqrt[4]{2}) & \\ \hline | 4 & \text{since } x^4 - 2 \text{ is irreducible (by Eisenstein).} \\ \mathbb{Q} & \end{array}$$

Thus  $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$ .

2. Find the splitting field for  $x^6 + 3$  over  $\mathbb{Q}$ .

First, let's find the roots. In polar coordinates,  $z^6 = -3 = 3e^{i\pi} = r^6 e^{i6\theta}$ . Thus  $r^6 = 3$  and  $6\theta = \pi + 2\pi k$  which implies  $\theta = \frac{\pi}{6} + \frac{\pi k}{3}$ . Thus the roots are  $\sqrt[6]{3}e^{\frac{\pi i}{6}}(e^{\frac{\pi i}{3}})^k$  for  $k = 0, \dots, 5$ .

$$\begin{array}{l} \mathbb{Q}(\sqrt[6]{3}e^{\frac{\pi i}{6}}, e^{\frac{\pi i}{3}}) \\ | \quad m \leq 2 \quad \text{since the cyclotomic polynomial works.} \\ \mathbb{Q}(\sqrt[6]{3}e^{\frac{\pi i}{6}}) \\ | \quad 6 \quad \text{since } x^6 + 3 \text{ is irreducible (by Eisenstein).} \\ \mathbb{Q} \end{array}$$

In fact,  $m = 1$  as  $(\sqrt[6]{3}e^{\frac{\pi i}{6}})^3 = \sqrt{3}i$  implies  $\frac{1 \pm \sqrt{3}i}{2} \in \mathbb{Q}(\sqrt[6]{3}e^{\frac{\pi i}{6}})$  which is the roots of the cyclotomic polynomial.

3. Find the splitting field of  $x^5 - 2$  and its degree.

We see the roots are  $\omega^i \sqrt[5]{2}$  for  $i = 0, \dots, 4$  where  $\omega = e^{\frac{2\pi i}{5}}$ . So the splitting field is  $\mathbb{Q}(\sqrt[5]{2}, \omega)$ .

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt[5]{2}, \omega) & \\ \leq 4 / & & \backslash \\ \mathbb{Q}(\sqrt[5]{2}) & & \mathbb{Q}(\omega) \quad \text{since } x^5 - 2 \text{ and the cyclotomic} \\ 5 \backslash & & / 4 \quad \leftarrow \text{polynomials are irreducible} \\ & \mathbb{Q} & \text{over } \mathbb{Q} \text{ by Eisenstein.} \end{array}$$

Then  $D = [\mathbb{Q}(\sqrt[5]{2}, \omega) : \mathbb{Q}] \leq 20$ . Of course  $4|D$  and  $5|D$  implies  $20|D$ . Thus  $D = 20$ .

**Note.** This says  $x^4 + x^3 + x^2 + x + 1$  is irreducible over  $\mathbb{Q}(\sqrt[5]{2}, \omega)$ .

**Lemma 2.11.** Let  $K$  be a field and  $f(x) \in K[x]$  a nonconstant polynomial. Then there exists a field extension  $E \supseteq K$  such that  $[E : K] \leq \deg f$  and  $f(x)$  has a root in  $E$ .

*Proof.* Let  $p(x)$  be an irreducible factor of  $f(x)$ . It is enough to show true for  $p(x)$ . Let  $t$  be an indeterminate over  $K$  and  $E = K[t]/(p(t))$ , a field as  $p(t)$  is irreducible in  $K[t]$ . Let  $\alpha = t + (p(t)) = \bar{t}$ . Then  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a  $K$ -basis for  $E$  where  $n = \deg p(t)$ . Define  $\sigma : K \rightarrow E$  by  $a \mapsto a + (p(t))$ . Since there does not exist constants in  $(p(t))$  we see  $\ker \phi = \{0\}$  and  $\sigma$  is an injective field map. So by identifying  $K$  with  $\sigma(K)$ , we can assume  $K \subseteq E = K(\alpha)$ . Note  $p(\alpha) = p(t) + (p(t)) = \bar{0}$ . So  $\alpha \in E$  is a root of  $p(x)$  and  $[E : K] = n$ .  $\square$

**Lemma 2.12.** Let  $K$  be a field. Then there exists a field  $E \supseteq K$  such that every nonconstant polynomial  $f \in K[x]$  has a root in  $E$ .

*Proof.* For each nonconstant  $f \in K[x]$ , let  $t_f$  be an indeterminate. Let  $R = K[\{t_f\}_{f \in K[x] \setminus K}]$  and  $I$  an ideal of  $R$  generated by  $\{f(t_f)\}_{f \in K[x] \setminus K}$ .

**Claim.**  $I \neq R$ .

*Proof:* Suppose  $I = R$ . Then  $1 \in I$  which implies

$$1 = r_1 f_1(t_{f_1}) + \dots + r_s f_s(t_{f_s}) \tag{1}$$

for  $f_1, \dots, f_s \in K[x] \setminus K$  and  $r_1, \dots, r_s \in R$ . For ease of notation, let  $t_i := t_{f_i}$ . Let  $t_1, \dots, t_s, \dots, t_n$  be all the indeterminants involved in  $r_1, \dots, r_s$  along with  $t_1, \dots, t_s$ . Now, define  $F_1 \supseteq K$  such that  $f_1(t_1)$  has a root in  $F_1$ . Iteratively define  $F_i \supseteq F_{i-1}$  such that  $f_i(t_i)$  has a root in  $F_i$ . Then  $F_s \supseteq K$  is such that  $f_i(t_i)$  has a root  $\alpha_i$  in  $F_s$  for all  $i = 1, \dots, s$ . Plug in  $\alpha = (\alpha_1, \dots, \alpha_s)$  into Equation (1) to get  $1 = 0$ , a contradiction. Thus  $I \neq R$ .



Let  $M$  be a maximal ideal of  $R$  containing  $I$  (this exists by Zorn's Lemma) and let  $E = R/M$ , a field. Define  $\sigma : K \hookrightarrow R \rightarrow R/M$  by  $a \mapsto a + M$ . Here, we see  $\ker \sigma = \{0\}$  as if  $a + M = 0$  then  $a \in M$  which implies  $M$  contains a unit. Thus  $\sigma$  is injective and so we can identify  $K$  with its image  $\sigma(K)$  and conclude  $K \subseteq E$ . Let  $f(x) \in K[x]$  be a nonconstant polynomial and  $\alpha_f = t_f + M$ . Then  $f(\alpha_f) = f(t_f) + M = 0$  since  $f(t_f) \in I \subseteq M$ . So  $\alpha_f$  is a root of  $f$  in  $E$ .  $\square$

**Definition 2.13.** A field  $F$  is **algebraically closed** if every nonconstant polynomial  $f(x) \in F[x]$  has a root in  $F$ . Equivalently,  $f(x)$  splits completely in  $F[x]$ . An **algebraic closure** of a field  $F$  is a field  $\bar{F} \supseteq F$  such that  $\bar{F}$  is algebraically closed and  $\bar{F}/F$  is algebraic.

**Proposition 2.14.** If  $F \subseteq L$  and  $L$  is algebraically closed, then  $\bar{F} = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$  is an algebraic closure of  $F$ .

*Proof.* First, we want to show that this is a field. Given  $\alpha, \beta \in \bar{F}$ , we want to show  $\alpha\beta, \alpha \pm \beta, \frac{\alpha}{\beta}$  are algebraic over  $F$ . Since  $\alpha, \beta$  are algebraic,  $[F(\alpha, \beta) : F] < \infty$  by the Corollary. But  $\alpha\beta, \alpha \pm \beta, \frac{\alpha}{\beta} \in F(\alpha, \beta)$  where every element is algebraic over  $F$  (since the degree is finite). Thus they are algebraic over  $F$  and thus in  $\bar{F}$ . Now, we show  $\bar{F}$  is algebraically closed. Let  $f(x) \in \bar{F}[x] \setminus F$ . Then  $f(x)$  has a root  $\alpha \in L$ . So  $\bar{F}(\alpha)/\bar{F}$  is algebraic and  $\bar{F}/F$  is algebraic which implies  $\bar{F}(\alpha)/F$  is algebraic. Thus  $\alpha$  is algebraic over  $F$  which implies  $\alpha \in \bar{F}$ .  $\square$

**Theorem 2.15.** Let  $F$  be a field. Then there exists an algebraic closure of  $F$ .

*Proof.* Let  $E_0 = F$ . For  $n \geq 1$ , define  $E_n \supseteq E_{n-1}$  to be a field such that every nonconstant polynomial in  $E_{n-1}[x]$  has a root in  $E_n$ . Let  $L = \cup_{i=1}^{\infty} E_i$ . This is a field as the  $E_i$ 's are nested.  $L$  is also algebraically closed as for  $f(x) \in L[x] \setminus L$ , there exists  $n$  such that  $f(x) \in E_n[x]$ . Then  $f(x)$  has a root in  $E_{n+1} \subseteq L$ . Now, let  $\bar{F} = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$ . Then by the above proposition,  $\bar{F}$  is an algebraic closure for  $F$ .  $\square$

**Corollary 2.16.** Let  $f(x) \in F[x] \setminus F$ . Then there exists a splitting field for  $f(x)$ .

*Proof.* Let  $\bar{F}$  be an algebraic closure of  $F$ . Then  $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$  in  $\bar{F}[x]$ . Then  $F(\alpha_1, \dots, \alpha_n)$  is a splitting field for  $f(x)$  over  $F$ .  $\square$

**Definition 2.17.** Let  $E/F$  and  $E'/F'$  be field extensions. Let  $\sigma : F \rightarrow F'$  and  $\tau : E \rightarrow E'$  be field homomorphisms. Say  $\tau$  **extends**  $\sigma$  if  $\tau|_F = \sigma$ . As a special case, if  $F = F'$  and  $\sigma = 1_F$ , then  $\tau$  extends  $\sigma$  if and only if  $\tau$  fixes  $F$ .

**Remarks.** Suppose  $\tau$  extends  $\sigma$ .

1.  $\sigma$  extends to a ring homomorphism  $\tilde{\sigma} : F[x] \rightarrow F'[x]$  by  $a_0 + a_1x + \dots + a_nx^n \mapsto \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n$ . Write this as  $p(x) \mapsto p^\sigma(x)$ . Check:  $(fg)^\sigma = f^\sigma g^\sigma$  and  $(f + g)^\sigma = f^\sigma + g^\sigma$ .

2. Suppose  $\alpha \in E$  is a root of  $p(x)$  in  $F[x]$ . Then  $\tau(\alpha)$  is a root of  $p^\sigma(x)$  :

$$p^\sigma(\tau(\alpha)) = \sigma(a_0) + \sigma(a_1)\tau(\alpha) + \dots + \sigma(a_n)\tau(\alpha)^n = \tau(a_0) + \tau(a_1\alpha) + \dots + \tau(a_n\alpha^n) = \tau(p(\alpha)) = \tau(0) = 0.$$

Note that in general  $p^\sigma(\tau(\alpha)) = \tau(p(\alpha))$  for all  $\alpha$  (i.e., not just roots).

3. If  $F = F'$ ,  $\sigma = 1_F$ . If  $\alpha \in E$  is a root of  $p(x)$ , then  $\tau(\alpha)$  is also a root of  $p(x)$ .

**Proposition 2.18.** Let  $E/F$  be an algebraic extension and  $\tau : E \rightarrow E$  a field homomorphism fixing  $F$ . Then  $\tau$  is an isomorphism.

*Proof.* Clearly  $\tau$  is 1-1. So its enough to show  $\tau$  is surjective. Let  $\alpha \in E$ . As  $\alpha$  is algebraic over  $F$ , there exists some  $p(x) \in F[x] \setminus F$  such that  $p(\alpha) = 0$ . Let  $R = \{\alpha = \alpha_1, \alpha_2, \dots, \alpha_n\}$  be all the roots of  $p(x)$  in  $E$ . Then  $\tau(\alpha_i) \in R$  for all  $i$ . We know  $\tau|_R$  is 1-1 and since finite it is also onto. Thus  $\tau(\alpha_j) = \alpha$  for some  $j$ .  $\square$

**Theorem 2.19.** Let  $\sigma : F \rightarrow K$  be a nonzero field homomorphism where  $K = \bar{K}$ . Suppose  $E/F$  is an algebraic extension. Then there exists  $\tau : E \rightarrow K$  extending  $\sigma$ .

*Proof.* Let  $\Lambda = \{(T, \phi) | F \subseteq T \subseteq E, T \text{ is a field, } \phi : T \rightarrow K \text{ extends } \sigma\}$ . Note that  $\Lambda \neq \emptyset$  as  $(F, \sigma) \in \Lambda$ . Define a partial order on  $\Lambda$  by  $(T_1, \phi_1) \subseteq (T_2, \phi_2)$  if and only if  $T_1 \subseteq T_2$  and  $\phi_2|_{T_1} = \phi_1$ . Let  $C$  be a totally ordered subset of  $\Lambda$  (i.e., a chain). Let  $T_0 = \cup T$  such that  $(T, \phi) \in C$ , a field (since the  $T$ 's are nested), and  $F \subseteq T_0 \subseteq E$ . Define  $\psi : T_0 \rightarrow K$  by  $t \mapsto \phi(t)$  if  $t \in T$  for some  $(T, \phi) \in C$ . Check this is well-defined and  $\psi$  is a field homomorphism. Clearly  $\psi|_T = \phi$  for all  $(T, \phi) \in C$ . Then  $(T_0, \psi) \in \Lambda$  is an upper bound for  $C$ . By Zorn's Lemma, there exists a maximal element  $(M, \delta) \in \Lambda$ . Want to show  $M = E$ . Let  $N \cong \delta(M) \subseteq K$ . We can extend  $\delta$  to  $\bar{\delta} : M[x] \rightarrow N[x]$  by  $p(x) \mapsto p^\delta(x)$ . This is an isomorphism as  $\delta$  is. Suppose there exists  $\alpha \in E \setminus M$ . Let  $f(x) = \text{Irred}(\alpha, M)$ . Then  $f^\delta(x)$  is irreducible in  $N[x] \subseteq K[x]$ . As  $K$  is algebraically closed,  $f^\delta(x)$  has a root  $\beta \in K$ . Of course  $\text{Irred}(\beta, N) = f^\delta(x)$ . Then

$$\delta' : M(\alpha) \rightarrow M[x]/(f) \rightarrow N[x]/(f^\delta) \rightarrow N(\beta) \subseteq K$$

defined by  $g(\alpha) \mapsto \overline{g(x)} \mapsto \overline{g^\delta(x)} \mapsto g^\delta(\beta)$ . So  $\delta' : M(\alpha) \rightarrow K$ . We can see  $\delta'|_M = \delta$ . So  $(M, \delta) < (M(\alpha), \delta')$ , a contradiction. Thus  $M = E$ . □

**Corollary 2.20.** *Using the notation of the above theorem, suppose  $E$  is algebraically closed and  $K$  is algebraic over  $\sigma(F)$ . Then  $\tau$  is an isomorphism.*

*Proof.* Since  $\ker \tau$  is an ideal, it is either  $(0)$  or  $E$ . Since  $\sigma$  is nonzero,  $\ker \tau \neq E$ . Thus  $\tau$  is injective. So it is enough to show  $\tau$  is surjective. Note  $\tau(E) \cong E$  and since  $E$  is algebraically closed,  $\tau(E)$  is. Since  $K/\sigma(F)$  is algebraic, so is  $K/\tau(E)$  since  $\sigma(F) \subseteq \tau(E) \subseteq K$ . But  $\tau(E)$  is algebraically closed, so  $K = \tau(E)$ . □

**Corollary 2.21.** *Let  $F$  be a field. Then any two algebraic closures of  $F$  are isomorphic via an isomorphism fixing  $F$ .*

*Proof.* Let  $L_1, L_2$  be algebraic closures of  $F$ . Consider  $\sigma : F \rightarrow L_2$ . We can extend  $\sigma$  to  $\tau : L_1 \rightarrow L_2$ . By previous corollary,  $\tau$  is an isomorphism fixing  $F$ . □

**Definition 2.22.** *Let  $F$  be a field and  $S \subseteq F[x] \setminus F$ . A **splitting field** for  $S$  over  $F$  is a field  $L \supseteq F$  such that every  $f \in S$  splits in  $L[x]$  and  $L$  is minimal with respect to this property.*

**Remark.** Let  $F, S$  be as above and fix an algebraic closure  $\overline{F}$  of  $F$ . Then there exists a unique splitting field  $L \subseteq \overline{F}$  of  $S$  over  $F$ . Namely  $L = F(T)$  where  $T = \{\alpha \in \overline{F} | f(\alpha) = 0 \text{ for some } f \in S\}$ .

**Proposition 2.23.** *Let  $F$  be a field and  $S \subseteq F[x] \setminus F$ . Any two splitting fields for  $S$  over  $F$  are isomorphic via an isomorphism fixing  $F$ .*

*Proof.* Let  $L_1, L_2$  be splitting fields for  $S$  over  $F$  and  $\overline{L_1}, \overline{L_2}$  their algebraic closures. Since  $L_1, L_2$  are algebraic over  $F$ ,  $\overline{L_1}, \overline{L_2}$  are also algebraic closures for  $F$ . Define  $T_i = \{\alpha \in \overline{L_i} | f(\alpha) = 0 \text{ for some } f \in S\}$ . Then  $L_i = F(T_i)$ . Extend  $1_F$  to  $\tau : \overline{L_1} \rightarrow \overline{L_2}$ . By the corollary,  $\tau$  is an isomorphism. Since  $\tau$  fixes  $F$ ,  $\tau(T_1) = T_2$ . Thus  $\tau(L_1) = \tau(F(T_1)) = F(\tau(T_1)) = F(T_2) = L_2$ . So  $\tau|_{L_1} : L_1 \rightarrow L_2$  is an isomorphism. □

**Remark.** With the above notation,  $\rho : L_1 \rightarrow \overline{L_2}$  which fixes  $F$  is an isomorphism from  $L_1$  to  $L_2$ .

**Proposition 2.24.** *Let  $F$  be a field,  $S \subseteq F[x] \setminus F$  and  $\overline{F}$  an algebraic closure of  $F$ . Let  $L \subset \overline{F}$  be a splitting field for  $S$  over  $F$ . Then any field map  $\sigma : L \rightarrow \overline{F}$  which fixes  $F$  is an automorphism of  $L$ .*

*Proof.* Apply previous proposition with  $L_1 = L_2 = L$ . □

## 2.2 Normality

**Theorem 2.25.** Let  $F$  be a field and  $\bar{F}$  an algebraic closure of  $F$ . Let  $F \subseteq E \subseteq \bar{F}$  be a field. Then TFAE

1.  $E$  is a splitting field for some  $S \in F[x] \setminus F$ .
2. Any embedding  $\sigma : E \rightarrow \bar{F}$  which fixes  $F$  is an automorphism of  $E$ .
3. Any irreducible polynomial in  $F[x]$  with a root in  $E$  splits in  $E$ .

If  $E/F$  satisfies the above, we say  $E/F$  is **normal**.

*Proof.* (1) $\Rightarrow$ (2) Previous Proposition

(2) $\Rightarrow$ (3) Let  $f(x) \in F[x] \setminus F$  be irreducible and have a root  $\alpha \in E$ . Let  $\beta$  be another root of  $f(x)$  in  $\bar{F}$ . Consider  $F(\alpha) \rightarrow F(\beta) \hookrightarrow \bar{F}$  defined by  $p(\alpha) \mapsto p(\beta)$ . Extend  $\sigma$  to  $\tau : E \rightarrow \bar{F}$ . Then  $\tau$  fixes  $F$  and by (2),  $\tau(E) = E$ . So  $\beta = \tau(\alpha) \in E$ . Thus all the roots of  $f$  are in  $E$  which implies  $f(x)$  splits.

(3) $\Rightarrow$ (1) Let  $S = \{f(x) \in F[x] \mid f(x) \text{ is irreducible and has a root in } E\}$ . Let  $L$  be the splitting field in  $\bar{F}$  for  $S$  over  $F$ . Want to show  $E = L$ . By (3), every polynomial in  $S$  splits in  $E$  so  $L \subseteq E$ . Let  $\alpha \in E \subseteq \bar{F}$ . Let  $f(x) = \text{Irred}(\alpha, F)$ . Then  $f(x) \in S$  implies  $\alpha \in L$ . Thus  $L = E$ . □

### Remarks.

1. If  $[E : F] = 2$ , then  $E/F$  is normal as (3) is true.
2.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is not normal since  $x^3 - 2$  is irreducible in  $\mathbb{Q}[x]$  and has a root in  $\mathbb{Q}(\sqrt[3]{2})$  but the other two roots are not in  $\mathbb{Q}(\sqrt[3]{2})$  as they are complex.
3. If  $K \subseteq F \subseteq E$  and  $E/K$  is normal, so is  $E/F$ . If  $E$  is a splitting field for  $S$  over  $K$  then it is also the splitting field for  $S$  over  $F$ . Note that  $F/K$  need not be normal. For example  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ .
4. If  $F/K$  and  $E/F$  are normal, then  $E/K$  need not be normal. For example  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$  as  $x^4 - 2$  does not split in  $\mathbb{Q}(\sqrt[4]{2})$ .

**Note.** If we say normal, we imply algebraic.

**Proposition 2.26.** Let  $F$  be a field,  $\bar{F}$  an algebraic closure of  $F$ , and  $\{E_\lambda\}$  a family of subfields of  $\bar{F}$  containing  $F$ . If each  $E_\lambda/F$  is normal, then  $\cap E_\lambda/F$  is normal.

*Proof.* Let  $f(x)$  be an irreducible polynomial in  $F[x]$  with a root in  $\cap E_\lambda$ . Then it has a root in each  $E_\lambda$  which implies it splits in each  $E_\lambda$  as they are normal. Thus  $f$  splits in  $\cap E_\lambda$ . □

**Definition 2.27.** Let  $E/F$  be an algebraic extension. The **normal closure** of  $E/F$  in  $\bar{F}$  is

$$\bigcap_{E \subset L \subset \bar{F}, L/F \text{ normal}} L,$$

the smallest normal extension of  $F$  containing  $E$ .

**Remark.** Suppose  $E = F(\alpha_1, \dots, \alpha_n)$  is algebraic over  $F$ . Let  $L$  be the splitting field for

$$\{\text{Irred}(\alpha_1, F), \dots, \text{Irred}(\alpha_n, F)\}$$

over  $F$ . Then  $L$  is the normal closure of  $E/F$ .

**Example.** Let  $E = \mathbb{Q}(\sqrt[3]{2})$ . The normal closure of  $E/\mathbb{Q}$  is  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ .

**Definition 2.28.** Let  $E_1, E_2$  be subfields of a field  $L$ . The **compositum** (or **join**) of  $E_1$  and  $E_2$  is

$$E_1E_2 = \bigcap_{E_1 \cup E_2 \subset F \subset L, F \text{ a field}} F,$$

the smallest subfield of  $L$  containing  $E_1$  and  $E_2$ .

**Remarks.** Let  $E_1, E_2 \subseteq L$ .

1.  $E_1E_2 = E_1(E_2) = E_2(E_1) = \left\{ \sum \frac{\alpha_i \beta_i}{\gamma_j \delta_j} \mid \alpha_i, \gamma_j \in E_1, \beta_i, \delta_j \in E_2 \right\}$ .
2. If  $E_1, E_2$  are algebraic over  $F$  then  $E_1E_2 = \left\{ \sum \alpha_i \beta_i \mid \alpha_i \in E_1, \beta_i \in E_2 \right\}$  since if  $\alpha$  is algebraic over  $F$  then the smallest field containing it is the smallest ring containing it.
3.  $E_1 = K(\alpha_1, \dots, \alpha_n), E_2 = K(\beta_1, \dots, \beta_n)$ . Then  $E_1E_2 = K(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n)$ .

**Proposition 2.29.** Suppose  $E_1/F$  and  $E_2/F$  are normal. Then  $E_1E_2/F$  is normal.

*Proof.* Suppose  $\sigma : E_1E_2 \rightarrow \bar{F}$  is an embedding which fixes  $F$ . Now  $\sigma|_{E_1}, \sigma|_{E_2}$  are embeddings of  $E_1, E_2$  into  $\bar{F}$  which fix  $F$ . Thus  $\sigma(E_1) = E_1$  and  $\sigma(E_2) = E_2$ . Now  $\underbrace{\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)}_{\text{this requires work}} = E_1E_2$ . So  $E_1E_2/F$  is normal.

The work: Let  $\alpha \in E_1E_2$ . Then  $\alpha = e_1\ell_1 + \dots + e_n\ell_n$ . Then  $\sigma(\alpha) = \sigma(e_1)\sigma(\ell_1) + \dots + \sigma(e_n)\sigma(\ell_n) \in \sigma(E_1)(\sigma(E_n))$ . Similarly,  $\sigma(E_1)\sigma(E_2) \subseteq \sigma(E_1E_2)$ . □

## 2.3 Separability

**Definition 2.30.** Let  $f(x) \in F[x] \setminus F$ . A root  $\alpha \in \bar{F}$  of  $f(x)$  is called a **multiple root** of  $f(x)$  if  $(x - \alpha)^2 \mid f(x)$  in  $\bar{F}[x]$ . Otherwise,  $\alpha$  is a **simple root**.

**Definition 2.31.** Let  $f(x) \in F[x]$  and say  $f(x) = a_nx^n + \dots + a_1x + a_0$ . The **derivative**  $f'$  of  $f(x)$  is  $f'(x) = na_nx^{n-1} + \dots + a_1$  where  $ka_k = \underbrace{a_k + \dots + a_k}_{k \text{ times}}$ .

**Note.** One can check  $(f + g)' = f' + g', (cf)' = cf', (fg)' = fg' + f'g, (f(g))' = f'(g)g'$

**Example.** Consider  $f(x) = x^6 + 2x^5 + x^3 + 2 \in \mathbb{Z}_3[x]$ . Then  $f' = 6x^5 + 10x^4 + 3x^2 = 10x^4$ .

**Proposition 2.32.** Let  $f(x) \in F[x] \setminus F$  and  $\alpha \in \bar{F}$ . Then  $\alpha$  is a multiple root in  $f(x)$  if and only if  $f(\alpha) = f'(\alpha) = 0$ .

*Proof.*  $\Rightarrow$  Say  $f(x) = (x - \alpha)^2 g(x)$  for  $g(x) \in \bar{F}[x]$ . Then  $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ . Clearly  $f'(\alpha) = f(\alpha) = 0$ .

$\Leftarrow$  As  $f(\alpha) = 0$ , we can say  $f = (x - \alpha)g(x)$  for some  $g(x) \in \bar{F}[x]$ . Taking the derivative, we see  $f'(x) = g(x) + (x - \alpha)g'(x)$  and plugging in  $\alpha$  we see  $0 = g(\alpha)$ . Thus  $g(x) = (x - \alpha)h(x)$  for some  $h(x) \in \bar{F}[x]$ . Then  $f(x) = (x - \alpha)^2 h(x)$ . □

**Proposition 2.33.** Let  $f \in F[x]$ . Then  $f(x)$  has no multiple roots in  $\bar{F}$  if and only if  $\gcd(f, f') = 1$ .

*Proof.* Suppose  $\gcd(f, f') = h \neq 1$ . Let  $\alpha$  be a root of  $h$  in  $\bar{F}$ . Then  $\alpha$  is a root of  $f$  and  $f'$  which implies  $\alpha$  is a multiple root. Now suppose  $f$  has a multiple root  $\alpha \in \bar{F}$ . Let  $h = \text{Irred}(\alpha, F)$ . Since  $f(\alpha) = f'(\alpha) = 0$ , we see  $h \mid f$  and  $h \mid f'$ . Thus  $h \mid \gcd_F(f, f')$  which implies  $\gcd(f, f') > 1$ . □

**Proposition 2.34.** Let  $F$  be a field and  $f(x)$  an irreducible polynomial in  $F[x]$ .

1. If  $\text{char } F = 0$ , then  $f$  has no multiple roots.
2. If  $\text{char } F = p > 0$ , then  $f(x)$  has a multiple root if and only if  $f(x) = g(x^p)$  for some  $g(x) \in F[x]$ .

*Proof.* 1. Let  $f = a_nx^n + \dots + a_1x + a_0$ . Then  $f' = na_nx^{n-1} + \dots + a_1 \neq 0$ . Since  $f$  is irreducible and  $\deg f' < \deg f$ , we see  $\gcd(f, f') = 1$ . Thus  $f$  has no multiple roots by the previous proposition.

2. By the same argument,  $f$  has multiple roots if and only if  $f' = 0$ . Of course,  $f' = 0$  if and only if  $ia_i = 0$  for all  $i$  which occurs if and only if  $i = 0 \pmod p$  or  $a_i = 0 \pmod p$  for all  $i$  as  $F$  is an integral domain. This is if and only if  $f(x) = a_{pm}x^{pm} + a_{p(m-1)}x^{p(m-1)} + \cdots + a_0 = g(x^p)$  for some  $g(x) \in F[x]$ .  $\square$

**Theorem 2.35.** Let  $E/F$  be an algebraic extension and let  $\sigma : F \rightarrow L_1$  and  $\tau : F \rightarrow L_2$  be embeddings of  $F$  into algebraically closed fields  $L_1$  and  $L_2$ . Let  $S_\sigma = \{\pi : E \rightarrow L_1 | \pi|_F = \sigma\}$  and  $S_\tau = \{\pi : E \rightarrow L_2 | \pi|_F = \tau\}$ . Then  $|S_\sigma| = |S_\tau|$ .

*Proof.* Consider the isomorphism  $\tau\sigma^{-1} : \sigma(F) \rightarrow F \rightarrow \tau(F) \hookrightarrow L_2$ . Then there exists an extension  $\lambda : \overline{\sigma(F)} \rightarrow L_2$  such that  $\lambda|_{\sigma(F)} = \tau\sigma^{-1}$  where  $\overline{\sigma(F)}$  is the algebraic closure of  $\sigma(F)$  in  $L_1$ . In fact, if  $\overline{\tau(F)}$  is the algebraic closure of  $\tau(F)$  in  $L_2$ , then  $\lambda : \overline{\sigma(F)} \rightarrow \overline{\tau(F)}$  is an isomorphism. Let  $\pi \in S_\sigma$ . Since  $E/F$  is algebraic and  $\pi$  extends  $\sigma$ , we see  $\pi(E)$  is algebraic over  $\sigma(F)$ . So  $\pi(E) \subseteq \overline{\sigma(F)}$ . Then  $\lambda\pi : E \rightarrow \overline{\sigma(F)} \rightarrow L_2$  and  $\lambda\pi|_F = \lambda\sigma = \tau$ . Thus  $\lambda\pi \in S_\tau$ . Thus we have a map  $\tilde{\lambda} : S_\sigma \rightarrow S_\tau$  defined by  $\pi \mapsto \lambda\pi$ . This is injective as  $\lambda$  is. Similarly, we can define  $\tilde{\lambda}^{-1} : S_\tau \rightarrow S_\sigma$  which is again injective. Clearly  $\tilde{\lambda}\tilde{\lambda}^{-1}(\pi) = \tilde{\lambda}\lambda^{-1}(\pi) = \lambda\lambda^{-1}(\pi) = \pi$  and  $\tilde{\lambda}^{-1}\tilde{\lambda}(\pi) = \pi$ . Thus  $\lambda$  is bijective which implies  $|S_\tau| = |S_\sigma|$ .  $\square$

**Definition 2.36.** Let  $E/F$  be an algebraic extension. The **separable degree** of  $E/F$ , denoted  $[E : F]_S$ , is  $|S_\sigma| = |\{\pi : E \rightarrow \overline{F} | \pi|_F = 1_F\}|$ .

**Proposition 2.37.** Let  $E = F(\alpha)$  where  $\alpha$  is algebraic over  $F$ . Then  $[E : F]_S =$  the number of distinct roots of  $\text{Irred}(\alpha, F)$  in  $\overline{F} \leq \deg \text{Irred}(\alpha, F) = [E : F]$ .

*Proof.* Let  $f(x) = \text{Irred}(\alpha, F) \in F[x]$ . Let  $\pi : F(\alpha) \rightarrow \overline{F}$  such that  $\pi$  fixes  $F$ . Clearly  $\pi$  is determined by  $\pi(\alpha)$ . Also  $\pi(\alpha)$  is a root of  $f(x)$  as  $\pi$  fixes  $F$ . So  $[F(\alpha) : F]_S \leq$  the number of distinct roots of  $f(x)$  in  $\overline{F}$ . Let  $\beta$  be any root of  $f(x)$ . Then  $\pi : F(\alpha) \rightarrow F[x]/(f(x)) \rightarrow F(\beta) \subseteq \overline{F}$  is an embedding of  $f(\alpha)$  into  $\overline{F}$  taking  $\alpha \mapsto \beta$ . So  $[F(\alpha) : F]_S \geq$  the number of distinct roots of  $f(x)$  in  $\overline{F}$ .  $\square$

**Theorem 2.38.** Let  $K \subseteq F \subseteq E$  be fields and  $E/K$  algebraic. Then  $[E : K]_S = [E : F]_S[F : K]_S$ . Moreover, if  $E/K$  is finite, then  $[E : K]_S \leq [E : K]$ .

*Proof.* Let  $\overline{E}$  be a fixed algebraic closure of  $E$ . Let  $S = \{\pi : F \rightarrow \overline{E} | \pi \text{ fixes } K\}$ . Then  $|S| = [F : K]_S$ . Let  $T_\pi = \{\tau : E \rightarrow \overline{E} | \tau|_F = \pi\}$  for all  $\pi \in S$ . By the Theorem,  $|T_\pi| = [E : F]_S$ . If  $\pi_1 \neq \pi_2 \in S$ , then  $T_{\pi_1} \cap T_{\pi_2} = \emptyset$ . If  $\tau \in T_\pi$ , then  $\tau|_K = 1_K$ . Therefore  $\cup_{\pi \in S} T_\pi \subseteq \{\sigma : E \rightarrow \overline{E} | \sigma \text{ fixes } K\}$ . On the other hand, if  $\sigma : E \rightarrow \overline{E}$  fixes  $K$ , then  $\sigma|_F : F \rightarrow \overline{E}$  fixes  $K$  which implies  $\sigma|_F \in S$ . Say  $\sigma|_F = \pi$ . Then  $\sigma \in T_\pi$ . So  $\cup_{\pi \in S} T_\pi = \{\sigma : E \rightarrow \overline{E} | \sigma \text{ fixes } K\}$ . Now

$$[E : K]_S = |\{\sigma : E \rightarrow \overline{E} | \sigma \text{ fixes } K\}| = |\cup_{\pi \in S} T_\pi| = \cup_{\pi \in S} |T_\pi| = |S||T_\pi| = [F : K]_S[E : F]_S.$$

Moreover, suppose  $[E : K] < \infty$ . Then  $E = K(\alpha_1, \dots, \alpha_n)$  for some  $n$ . If  $n = 1$ , done by previous proposition. If  $n > 1$ , let  $L = K(\alpha_1, \dots, \alpha_{n-1})$ . By induction on  $n$ ,  $[L : K]_S \leq [L : K]$ . Now  $E = L(\alpha)$  implies  $[E : L]_S \leq [E : L]$  by proposition. Thus, by the multiplicative property,  $[E : K]_S \leq [E : K]$ .  $\square$

**Definition 2.39.** A polynomial  $f(x) \in F[x]$  is called **separable** if  $f(x)$  has no multiple roots in an algebraic closure. Let  $\alpha$  be algebraic over  $F$ . Then  $\alpha$  is **separable** over  $F$  if  $\text{Irred}(\alpha, F)$  is separable. Let  $E/F$  be an algebraic extension. Then  $E/F$  is separable if and only if  $\alpha \in E$  is separable over  $F$  for all  $\alpha$ .

**Remarks.**

1. Suppose  $\alpha$  is algebraic over  $F$ . Then  $\alpha$  is separable over  $F$  if and only if  $[F(\alpha) : F]_S = [F(\alpha) : F]$ .
2. Let  $K \subseteq F \subseteq E$  be algebraic extensions. If  $E/K$  is separable, then  $E/F$  and  $F/K$  are separable.

*Proof.* Let  $\alpha \in E$ . Know  $\text{Irred}(\alpha, F) | \text{Irred}(\alpha, K)$  in  $F[x]$ . If  $\alpha$  is separable over  $K$ , then  $\text{Irred}(\alpha, K)$  has no multiple roots which implies  $\text{Irred}(\alpha, F)$  has no multiple roots. Thus  $\alpha$  is separable over  $F$ .  $\square$

**Theorem 2.40.** *Suppose  $E/F$  is finite. Then  $E/F$  is separable if and only if  $[E : F]_S = [E : F]$ .*

*Proof.* ( $\Leftarrow$ ) Let  $\alpha \in E$ . Consider  $F \subseteq F(\alpha) \subseteq E$ . We know

$$[E : F(\alpha)]_S [F(\alpha) : F]_S = [E : F]_S = [E : F] = [E : F(\alpha)] [F(\alpha) : F].$$

Since  $[F(\alpha) : F]_S \leq [F(\alpha) : F]$ , they are equal and thus  $\alpha$  is separable by remark 1.

( $\Rightarrow$ ) Assume  $E = F(\alpha_1, \dots, \alpha_n)$ . Induct on  $n$ . If  $n = 1$ , done by remark. Let  $L = F(\alpha_1, \dots, \alpha_{n-1})$ . Then  $L/F$  is separable by remark 2 and by the induction hypothesis  $[L : F]_S = [L : F]$ . Note  $E = L(\alpha_n)$ . Since  $E/F$  is separable, so is  $E/L$ . So  $[E : L]_S = [E : L]$  by the  $n = 1$  case. Thus

$$[E : F]_S = [E : F]_S [L : F]_S = [E : F] [L : F] = [E : F].$$

□

**Corollary 2.41.** *Suppose  $E = F(\alpha_1, \dots, \alpha_n)$ . Then  $E/F$  is separable if and only if each  $\alpha_i$  is separable over  $F$ .*

*Proof.* ( $\Rightarrow$ ) Clear

( $\Leftarrow$ ) Induct on  $n$ . If  $n = 1$ , done by remark and theorem. Let  $L = F(\alpha_1, \dots, \alpha_{n-1})$ . Then  $L/F$  is separable and thus  $[L : F]_S = [L : F]$ . Also  $E/L$  is separable by the  $n = 1$  case which implies  $[E : L]_S = [E : L]$ . Multiplying, we see  $[E : F]_S = [E : F]$  which implies  $E/F$  is separable. □

**Definition 2.42.** *Let  $E$  be an arbitrary algebraic extension of  $F$ . Then  $E$  is **separable** over  $F$  if every finitely generated subextension is separable.*

**Corollary 2.43.** *Suppose  $E = F(S)$ . Then  $E/F$  is separable if and only if  $\alpha$  is separable over  $F$  for all  $\alpha \in S$ .*

*Proof.* ( $\Rightarrow$ ) Clear

( $\Leftarrow$ ) Note that  $F(S) = \{\sum_{finite} a_i s_i | a_i \in F, s_i \in S\}$ . Thus, for all  $\alpha \in E$ , there exists a finitely generated subfield such that  $\alpha \in F(s_1, \dots, s_n)$ . By the finite case, each of these finitely generated subfields are separable. Thus, by definition,  $E$  is separable. □

**Proposition 2.44.** *Suppose  $K \subseteq F \subseteq E$  are fields. Then  $E/K$  is separable if and only if  $E/F$  and  $F/K$  are separable.*

*Proof.* ( $\Rightarrow$ ) Done (Remark 2 above)

( $\Leftarrow$ ) Let  $\alpha \in E$  and  $f(x) = \text{Irred}(\alpha, F) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ . Since  $\alpha$  is separable over  $F$ ,  $f$  is a separable polynomial. Let  $L = K(c_0, \dots, c_{n-1})$ . Then  $f(x) \in L[x]$  and  $f(x) = \text{Irred}(\alpha, L)$ . So  $f$  is separable, which implies  $\alpha$  is separable over  $L$ . Thus  $[L(\alpha) : L]_S = [L(\alpha) : L]$ . Since  $F/K$  is separable, each  $c_i$  is separable over  $K$ . So  $L = K(c_0, \dots, c_{n-1})$  is separable over  $K$ . Thus  $[L(\alpha) : K]_S = [L(\alpha) : K]$ . Thus  $L(\alpha)/K$  is separable, which implies  $\alpha$  is separable over  $K$ . □

**Proposition 2.45.** *Suppose  $E/F$  is separable and let  $L$  be the normal closure of  $E/F$ . Then  $L/F$  is separable.*

*Proof.* Let  $S = \{\text{Irred}(\alpha, F) | \alpha \in E\} \subseteq F[x]$ . Then  $L$  is the splitting field for  $S$  over  $F$ . Let

$$R = \{\alpha \in \overline{F} | \alpha \text{ is a root of } f(x) \text{ for some } f \in S\}.$$

Then  $L = F(R)$ . Since  $S$  is a set of separable polynomial, for all  $r \in R$  we see  $\text{Irred}(r, F) \in S$  which implies  $r$  is separable. Thus  $L$  is separable. □

**Definition 2.46.** A field  $F$  is called **separably closed** if whenever  $\alpha \in \overline{F}$  is separable over  $F$  we have  $\alpha \in F$ . Equivalently, every separable irreducible polynomial in  $F[x]$  is degree 1. A **separable closure** of a field  $F$  is a field  $E \supseteq F$  such that  $E$  is separably closed and  $E/F$  is separable.

**Proposition 2.47.** Separable closures exist.

*Proof.* Let  $F$  be a field,  $\overline{F}$  an algebraic closure of  $F$ , and  $E = \{\alpha \in \overline{F} | \alpha \text{ is separable over } F\}$ . This is a field as for  $\alpha, \beta \in E$ ,  $F(\alpha, \beta)$  is separable over  $F$  which implies  $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F(\alpha, \beta)$  which implies they are separable and thus in  $E$ . Clearly  $E/F$  is separable, so we need only to show it is separably closed. Suppose  $\alpha \in \overline{F} = \overline{E}$  is separable over  $E$ . Then  $E(\alpha)/E$  is separable and  $E/F$  is separable which implies  $E(\alpha)/F$  is separable. Thus  $\alpha$  is separable over  $F$  and therefore  $\alpha \in E$ .  $\square$

**Notation.**  $F^{\text{sep}}$  denotes a separable closure of  $F$ .

**Definition 2.48.** A field  $F$  is called **perfect** if every algebraic extension of  $F$  is separable. Equivalently,  $\overline{F}/F$  is separable.

**Proposition 2.49.** Every field of characteristic 0 is perfect.

*Proof.* Let  $\alpha$  be algebraic over  $F$  where  $\text{char } F = 0$  and  $f(x) = \text{Irred}(\alpha, F)$ . Then  $f$  has no multiple roots which implies  $\alpha$  is separable.  $\square$

Suppose  $\text{char } F = p$ . Then  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ . Thus there exists a field homomorphism  $\phi : F \rightarrow F$  defined by  $a \mapsto a^p$ . This is called the **Frobenius map**. Then  $\phi(F) = F^p = \{a^p | a \in F\}$  is a subfield of  $F$ .

**Proposition 2.50.** Suppose  $\text{char } F = p$ . Then  $F$  is perfect if and only if  $F = F^p$ .

*Proof.* ( $\Rightarrow$ ) Let  $a \in F$ . Consider  $f(x) = x^p - a \in F[x]$ . Let  $\alpha$  be a root of  $f(x)$  in some splitting field of  $f(x)$  over  $F$ . Let  $g(x) = \text{Irred}(\alpha, F)$ . Then  $g(x) | f(x)$ . Note  $\alpha^p = a$  implies  $x^p - a = x^p - \alpha^p = (x - \alpha)^p$ . Then  $g(x) = (x - \alpha)^m$  for  $m < p$  in the splitting field. But  $\alpha$  is separable over  $F$  as  $F$  is perfect. So  $m = 1$ . Then  $g(x) = x - \alpha \in F[x]$  which implies  $\alpha \in F$ . So  $a = \alpha^p \in F^p$ . So  $F = F^p$ .

( $\Leftarrow$ ) Let  $\alpha$  be an algebraic element over  $F$ . Let  $f(x) = \text{Irred}(\alpha, F)$ . Suppose  $\alpha$  is not separable, i.e.,  $f$  has multiple roots. This means  $f(x) = g(x^p)$  for some  $g(x) \in F[x]$ . Say  $g(x) = x^m + x_{m-1}x^{m-1} + \dots + c_0$ . As  $F = F^p$ , let  $c_i = d_i^p$ . Then

$$f(x) = g(x^p) = (x^m)^p + d_{m-1}^p(x^{m-1})^p + \dots + d_1^p x^p + d_0^p = (x^m + d_{m-1}x^{m-1} + \dots + d_1x + d_0)^p.$$

This contradicts the fact that  $f$  is irreducible. So  $\alpha$  is separable.  $\square$

**Corollary 2.51.** Every finite field is perfect.

*Proof.* First note a finite field  $F$  has characteristic  $p > 0$  where  $p$  is prime [Since  $\phi : \mathbb{Z} \rightarrow F$  defined by  $n \mapsto n \cdot 1$  is not injective (as  $F$  is finite), say  $\ker \phi = (p) \neq 0$ . Then  $\mathbb{Z}/(p) \hookrightarrow F$  and since  $F$  is a domain,  $p$  is prime.] Consider the Frobenius map  $\phi : F \rightarrow F$  defined by  $a \mapsto a^p$ . This is an injective homomorphism and since  $|F| < \infty$  it is surjective as well. Thus  $F = F^p$  which implies  $F$  is perfect.  $\square$

**Examples.**

- Let  $F$  be any field of characteristic  $p > 0$ . Let  $t$  be an indeterminate and  $E = F(t)$ . Then  $x^p - t \in E[x]$  is an irreducible nonseparable polynomial. Thus  $E$  is not perfect.

*Proof:* **Eisenstein:** Let  $R$  be a UFD,  $K$  its fraction field and  $f(x) = a_n x^n + \dots + a_0 \in R[x]$ . Suppose there exists a prime element  $p \in R$  such that  $p \nmid a_n, p | a_i$  for  $0 \leq i \leq n-1$ , and  $p^2 \nmid a_0$ . Then  $f(x)$  is irreducible over  $K[x]$ .

Apply Eisenstein with  $R = F[t]$ , a PID. Note  $t$  is a prime. Then  $f(x) = x^p - t \in R[x]$  is irreducible in  $E[x]$ , a quotient field. Note  $f'(x) = 0$ , so  $f(x)$  has multiple roots, which implies nonseparable.

- By the same proof,  $F(t)/F(t^p)$  is not separable as  $x^p - t^p = \text{Irred}(t, F(t^p))$  has multiple roots.

**Definition 2.52.** Let  $E/F$  be a field extension. A primitive element for  $E/F$  is an element  $\alpha \in E$  such that  $E = F(\alpha)$ .

**Theorem 2.53 (Primitive Element Theorem).** Let  $[E : F] < \infty$ . Then there exists a primitive element for  $E/F$  if and only if there are finitely many intermediate fields of  $E/F$ . Furthermore, if  $E/F$  is separable, then there exists a primitive element.

*Proof.* ( $\Rightarrow$ ) Suppose  $E = F(\alpha)$ . Let  $f(x) = \text{Irred}(\alpha, F)$ . Let  $L$  be a splitting field of  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ . Define a map

$$\lambda : \{\text{Intermediate fields of } E/F\} \rightarrow \{\text{monic factors of } f(x) \text{ in } L\},$$

such that  $K \mapsto \text{Irred}(\alpha, K)$ . Clearly, there are only finitely many factors of  $f(x)$  in  $L$ .

Claim:  $\lambda$  is injective.

*Proof:* It is enough to show  $K$  is determined by  $\text{Irred}(\alpha, K) = x^n + c_{n-1}x^{n-1} + \dots + c_0 = g(x)$ . Note  $[E : K] = [K(\alpha) : K] = n$ . Let  $L' = F(c_0, \dots, c_{n-1}) \subseteq K$ . Then  $g(x) \in L'[x]$  and is irreducible over  $L'$ . So  $g(x) = \text{Irred}(\alpha, L')$ . Since  $E = L'(\alpha)$ ,  $[E : L'] = [L'(\alpha) : L'] = n$ . So  $[K : L'] = 1$ , that is  $K = L'$ . Thus  $\lambda$  is injective.

( $\Leftarrow$ ) Suppose  $|F| < \infty$ . Since  $[E : F] < \infty$  we have  $|E| < \infty$ . Note that  $E^*$  is cyclic, so  $E^* = \langle \alpha \rangle$  for some  $\alpha \in E$ . Of course,  $E$  is a field, so everything but 0 is a unit. Thus  $E = F(\alpha)$ . Now suppose  $|F| = \infty$ . Let  $E = F(\alpha_1, \dots, \alpha_n)$ . We will induct on  $n$ . If  $n = 1$ , obvious. So let  $L = F(\alpha_1, \dots, \alpha_{n-1})$ . By induction,  $L = F(\gamma)$  for some  $\gamma \in L$ . Then  $E = F(\alpha_1, \gamma)$ . So it is enough to prove the result for  $E = F(\alpha, \beta)/F$ . Let  $\Lambda = \{F(\alpha + c\beta) \mid c \in F\}$ . This is a subset of the set of all intermediate fields of  $E/F$ . Thus  $\Lambda$  is finite. Since  $|F| = \infty$ , there exists  $c_1 \neq c_2 \in F$  such that  $F(\alpha + c_1\beta) = F(\alpha + c_2\beta) =: L$ . Then  $\alpha + c_1\beta, \alpha + c_2\beta \in L$ . Subtracting, we get  $(c_1 - c_2)\beta \in L$ . But  $0 \neq c_1 - c_2 \in F \subseteq L$ . Thus  $\beta \in L$  which implies  $\alpha \in L$ . So  $F(\alpha + c_1\beta) = F(\alpha, \beta)$ . Thus we have found a primitive root.

Finally, let  $E/F$  be finite and separable. As above, the finite case has a primitive element equal to the cyclic generator and we can reduce the infinite case to  $E = F(\alpha, \beta)/F$ . Let  $[E : F] = n = [E : F]_S$ . Let  $\{\sigma_1, \dots, \sigma_n\}$  be the distinct embeddings of  $E \rightarrow \overline{F}$  which fix  $F$ . Let  $P(x) = \prod_{i < j} (\sigma_i(\alpha) - \sigma_j(\alpha))x + (\sigma_i(\beta) - \sigma_j(\beta)) \in \overline{F}[x]$ . Note that  $P(x) \neq 0$  as  $\sigma_i \neq \sigma_j$  and  $\sigma_i$  are determined by  $\sigma_i(\alpha)$  and  $\sigma_i(\beta)$ . So  $P(x)$  has finitely many roots in  $F$ . Since  $|F| = \infty$ , there exists  $c \in F$  such that  $P(c) \neq 0$ . Thus, rearranging the terms of each factor of  $P(x)$  we see  $\sigma_i(c\alpha + \beta) \neq \sigma_j(c\alpha + \beta)$  for all  $i < j$ . Now  $c\alpha + \beta \in E$  and  $\sigma_i|_{F(c\alpha + \beta)}$  are distinct for  $i = 1, \dots, n$ . Thus  $[F(c\alpha + \beta) : F]_S \geq n$ . Of course,  $[F(c\alpha + \beta) : F]_S \leq [E : F]_S = n$ . So  $[F(c\alpha + \beta) : F] = n$  which implies  $E = F(c\alpha + \beta)$ . □

**Example.** Let  $F$  be a field of characteristic  $p$  (e.g.  $F = \mathbb{Z}_p$ ). Let  $t, u$  be algebraically independent elements over  $F$  (that is,  $t$  and  $u$  are indeterminants with no relations like  $u = t^2$ ). Consider

$$\begin{aligned} F(t, u) &= L(t) \\ &\quad \Big|_p \quad \text{since } x^p - t^p \text{ is irreducible over } L. \\ F(t^p, u) &= L = K(u) \\ &\quad \Big|_p \quad \text{since } x^p - u^p \text{ is irreducible over } K. \\ F(t^p, u^p) &= K \end{aligned}$$

Then  $[F(t, u) : F(t^p, u^p)] = p^2$ . We will show there does not exist a primitive element for this extension. Let  $g(t, u) \in F(t, u)$  and note that  $g(t, u)^p \in F(t^p, u^p)$ . So  $[F(t^p, u^p, g(t, u)) : F(t^p, u^p)] \leq p$ . So  $F(t, u) \neq F(t^p, u^p, g(t, u))$ . Thus there is no primitive element. Note that this also implies there are infinitely many intermediate fields between the two fields.



## 2.4 Finite Fields

Often, if  $\text{char } F = p$ , we say that  $\mathbb{Z}_p \subseteq F$ . We can do this by considering the embedding  $\mathbb{Z}_p \rightarrow F$  defined by  $\bar{1} \mapsto 1$  and identifying  $\mathbb{Z}_p$  with its image.

**Proposition 2.54.** *Let  $F$  be a finite field of characteristic  $p$ . Then  $|F| = p^n$ .*

*Proof.* Note that  $F$  is a  $\mathbb{Z}_p$  vector space with dimension  $n$ , for some  $n$ . Then  $F \cong \mathbb{Z}_p^n$  as vector spaces. This says  $|F| = p^n$ .  $\square$

**Proposition 2.55.** *Let  $p$  be a prime and  $n > 0$  an integer. Then there exists a field  $F$  such that  $|F| = p^n$ . In fact, any field of order  $p^n$  is a splitting field for  $x^{p^n} - x$  over  $\mathbb{Z}_p$ . Therefore, any two fields of order  $p^n$  are isomorphic and any algebraically closed field of characteristic  $p$  contains a unique field of order  $p^n$ .*

*Proof.* First we show existence. Let  $E$  be the splitting field for  $f(x) = x^{p^n} - x$  over  $\mathbb{Z}_p$ . Let  $F = \{\alpha \in E \mid \alpha^{p^n} - \alpha = 0\}$ . Since  $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$  and  $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$  for all  $\alpha, \beta \in F$ , we see that  $F$  is a subfield of  $E$ . Now  $|F| \leq p^n$  as  $x^{p^n} - x$  has at most  $p^n$  roots. Of course,  $\gcd(f, f') = 1$  as  $f' = -1$ , so  $x^{p^n} - x$  has distinct roots, which implies  $|F| = p^n$ . Thus, we have found a field of order  $p^n$ . To show uniqueness, let  $F$  be a field of order  $p^n$  and note that  $F^*$  is a group of order  $p^n - 1$ . So for all  $\alpha \in F \setminus \{0\}$ ,  $\alpha^{p^n-1} = 1$ , which implies  $\alpha^{p^n} = \alpha$ . Thus every element of  $F$  is a root of  $x^{p^n} - x = 0$ . As  $|F| = p^n$ , all the roots of  $x^{p^n} - x$  are in  $F$ . So  $F$  is a splitting field.  $\square$

**Proposition 2.56.** *Let  $F$  be a field of order  $p^n$ . Then  $F$  is a splitting field for an irreducible polynomial  $f(x) \in \mathbb{Z}_p[x]$  of degree  $n$ . Moreover, any irreducible polynomial of degree  $n$  in  $\mathbb{Z}_p[x]$  splits in  $F$ . Finally  $F \cong \mathbb{Z}_p[x]/(f(x))$  where  $f(x)$  is irreducible and  $\deg f = n$ .*

*Proof.* Recall (HW Exercise) that  $F$  is normal over  $\mathbb{Z}_p$ . Let  $F = \mathbb{Z}_p(\alpha)$ . (We can do this by the Primitive Element Theorem as every finite field is separable). Let  $f(x) = \text{Irred}(\alpha, \mathbb{Z}_p)$ . Since  $F/\mathbb{Z}_p$  is normal and  $f(x)$  has a root in  $F$ ,  $f(x)$  splits over  $F$ . Note that  $\mathbb{Z}_p[x]/(f(x))$  is a field of order  $p^n$  as  $f$  is irreducible of degree  $n$ . Let  $E$  be a splitting field for  $g(x)$  contained in  $\overline{F}$  where  $\deg g = n$ . Then  $E = \mathbb{Z}_p(\beta)$  where  $\beta$  is a root of  $g(x)$  and  $|E| = p^n$ . But, there exists a unique field of order  $p^n$  in  $\overline{F}$ . Thus  $E = F$ .  $\square$

## 2.5 Inseparability

**Theorem 2.57.** *Let  $F$  be a field of characteristic  $p > 0$  and  $\alpha \in \overline{F}$ .*

1.  $\alpha$  is separable over  $F$  if and only if  $F(\alpha) = F(\alpha^p)$ .
2. If  $\alpha$  is inseparable over  $F$ , then  $[F(\alpha) : F(\alpha^p)] = p$  and  $\text{Irred}(\alpha, F(\alpha^p)) = x^p - \alpha^p$ .
3. For all  $n \geq 1$ ,  $[F(\alpha^{p^n}) : F]_S = [F(\alpha) : F]_S$ .
4.  $\alpha^{p^n}$  is separable over  $F$  for all  $n \gg 0$ .
5. Let  $n$  be the smallest  $n \gg 0$  such that  $\alpha^{p^n}$  is separable over  $F$ . Then  $[F(\alpha) : F] = p^n [F(\alpha) : F]_S$ .

*Proof.* 1. ( $\Rightarrow$ ) Suppose  $\alpha$  is separable over  $F$ . Then  $\alpha$  is separable over  $F(\alpha^p)$ . Certainly,  $\alpha$  is a root of  $x^p - \alpha^p$ . So  $\text{Irred}(\alpha, F(\alpha^p)) \mid x^p - \alpha^p = (x - \alpha)^p$ . Since  $\alpha$  is separable, there are no multiple roots. Thus  $\text{Irred}(\alpha, F(\alpha^p)) = x - \alpha$ . So  $\alpha \in F(\alpha^p)$ . Thus  $F(\alpha) = F(\alpha^p)$ .

( $\Leftarrow$ ) Suppose  $F(\alpha) = F(\alpha^p)$ . Let  $f(x) = \text{Irred}(\alpha, F)$ . Suppose  $f(x)$  has a multiple root. Then  $f(x) = g(x^p)$  for some  $g(x) \in F[x]$ . Then  $g(\alpha^p) = f(\alpha) = 0$  which implies  $\text{Irred}(\alpha^p, F) \mid g(x)$ . Then  $[F(\alpha^p) : F] \leq \deg g < \deg f = [F(\alpha) : F]$ , a contradiction. Thus  $f$  has no multiple roots, which implies  $\alpha$  is separable.

2. Suppose  $\alpha$  is inseparable over  $F$ . Consider  $\text{Irred}(\alpha, F(\alpha^p))|(x - \alpha)^p$ . This says  $\text{Irred}(\alpha, F(\alpha^p)) = (x - \alpha)^m = x^m - m\alpha x^{m-1} - \dots \in F(\alpha^p)[x]$  where  $1 \leq m \leq p$ . If  $m < p$ , then  $m$  is a unit. But  $-m\alpha \in F(\alpha^p)[x]$ . Thus  $\alpha \in F(\alpha^p)$ . This says  $F(\alpha) = F(\alpha^p)$ , a contradiction to (1) as  $\alpha$  is inseparable. Thus  $m = p$  which implies  $[F(\alpha) : F(\alpha^p)] = p$ .
3. Consider  $[F(\alpha) : F(\alpha^p)]_S$ . This is the number of distinct roots of  $\text{Irred}(\alpha, F(\alpha^p))$ . By (1) and (2),  $[F(\alpha) : F(\alpha^p)]_S = 1$ . By induction (and the  $n = 1$  case),  $[F(\alpha^{p^n}) : F]_S = [F(\alpha^{p^{n-1}}) : F]_S = [F(\alpha) : F]_S$ .
4. Consider the descending chain of fields:  $F(\alpha) \supseteq F(\alpha^p) \supseteq F(\alpha^{p^2}) \supseteq \dots \supseteq F$ . This can be viewed as a descending chain of  $F$ -vector spaces, all of which are subspaces of the finite dimensional vector space  $F(\alpha)$ . Thus there exists  $n$  such that  $F(\alpha^{p^n}) = F(\alpha^{p^{n+1}})$  and by (1),  $\alpha^{p^n}$  is separable over  $F$ .
5. Let  $n$  be the least element such that  $\alpha^{p^n}$  is separable over  $F$ . Then

$$\begin{aligned}
[F(\alpha) : F] &= [F(\alpha) : F(\alpha^{p^n})][F(\alpha^{p^n}) : F] \\
&= p^n [F(\alpha^{p^n}) : F] \text{ by iterative applications of (2)} \\
&= p^n [F(\alpha^{p^n}) : F]_S \text{ as } \alpha^{p^n} \text{ is separable} \\
&= p^n [F(\alpha) : F]_S \text{ by (3)}.
\end{aligned}$$

□

**Corollary 2.58.** *Suppose  $E/F$  is finite and  $\text{char } F = p$ . Then  $[E : F] = p^n [E : F]_S$  for some  $n$ .*

*Proof.* Say  $E = F(\alpha_1, \dots, \alpha_k)$ . Induct on  $k$ . For  $k = 1$ , done by Theorem. Let  $L = F(\alpha_1, \dots, \alpha_{n-1})$ . By induction,  $[L : F] = p^{n_1} [L : F]_S$  and by  $k = 1$  case  $[E : L] = p^{n_2} [E : L]_S$ . By the multiplicative property of separable degrees, letting  $n = n_1 + n_2$ , done. □

**Definition 2.59.** *Let  $E/F$  be a finite extension. Define the **inseparable** degree of  $E/F$  to be*

$$[E : F]_i = \frac{[E : F]}{[E : F]_S} = \begin{cases} 1 & \text{if characteristic } 0, \\ p^n & \text{if characteristic } p. \end{cases}$$

**Remark.** If  $F \subseteq L \subseteq E$  where  $E/F$  is finite,  $[E : F]_i = [E : L]_i [L : F]_i$ .

**Definition 2.60.** *Let  $F$  be a field of characteristic  $p > 0$  and  $\alpha \in \overline{F}$ . Then  $\alpha$  is **purely inseparably (p.i.)** over  $F$  if  $\alpha^{p^n} \in F$  for some  $n \gg 1$ . An algebraic extension  $E/F$  is p.i. if  $\alpha \in E$  is p.i. over  $F$  for all  $\alpha \in E$ .*

**Lemma 2.61.** *Let  $\alpha \in \overline{F}$ . Then TFAE*

1.  $\alpha$  is p.i. over  $F$
2.  $[F(\alpha) : F]_S = 1$
3.  $[F(\alpha) : F]_i = [F(\alpha) : F]$

*Proof.* We know (2)  $\Leftrightarrow$  (3) by the definition of inseparable degree. So we have

$$\begin{aligned}
\alpha \text{ is p.i. over } F &\Leftrightarrow \alpha^{p^n} \in F \text{ for } n \gg 0 \\
&\Leftrightarrow [F(\alpha^{p^n}) : F] = 1 \text{ for } n \gg 0 \\
&\Leftrightarrow [F(\alpha^{p^n}) : F]_S = 1 \text{ by (4) of Thm} \\
&\Leftrightarrow [F(\alpha) : F]_S = 1 \text{ by (3) of Thm}
\end{aligned}$$

□

**Proposition 2.62.** *Let  $E = F(\alpha_1, \dots, \alpha_n)$  be algebraic over  $F$ . TFAE*

1.  $E/F$  is p.i.
2. Each  $\alpha_i$  is p.i. over  $F$
3.  $[E : F]_S = 1$
4.  $[E : F]_i = [E : F]$

*Proof.* (3) $\Leftrightarrow$ (4): By definition of inseparable degree.

(1) $\Rightarrow$ (2): Clear

(2) $\Rightarrow$ (3): Use induction on  $n$ . If  $n = 1$ , done by Lemma. Let  $n > 1$  and  $L = F(\alpha_1, \dots, \alpha_{n-1})$ . Then  $E = L(\alpha_n)$ . By induction  $[L : F]_S = 1$  and by the  $n = 1$  case (since  $\alpha_n$  p.i. over  $F$  implies  $\alpha_n$  is p.i. over  $L$ )  $[E : L]_S = 1$ . By multiplicative property, done.

(3) $\Rightarrow$ (1): Let  $\beta \in E$ . By the Lemma, it is enough to show  $[F(\beta) : F]_S = 1$ . But  $[F(\beta) : F]_S \leq [E : F]_S = 1$ . Thus  $[F(\beta) : F]_S = 1$  and  $\beta$  is p.i. □

**Example.** Let  $F$  be a field of characteristic  $p$  and  $t$  an indeterminate over  $F$ . Then  $F(t)/F(t^p)$  is p.i. Note that  $\overline{F(t)}/F(t^p)$  is inseparable, but not p.i.

## 2.6 Cyclotomic Field Extensions

Let  $U_n = \{z \in \mathbb{C} | z^n = 1\}$ . Note that  $U_n = \langle e^{2\pi i/n} \rangle = \langle e^{2\pi i k/n} \rangle$  for all  $k$  such that  $\gcd(k, n) = 1$ . Any cyclic generator of  $U_n$  is called a **primitive  $n$ th root of unity**. There are  $\phi(n)$  primitive  $n$ th roots of unity.

**Definition 2.63.** The  $n$ th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{1 \leq i \leq n, \\ \gcd(i, n) = 1}} (x - \omega^i)$$

where  $\omega$  is any primitive root of unity.

**Examples.**

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$

**Facts.**

1.  $x^n - 1 = \prod_{i=0}^{n-1} (x - \omega^i)$
2.  $x^n - 1 = \prod_{d|n, d>0} \Phi_d(x)$  since  $x^n - 1 = \prod_{d|n} \left( \prod_{\omega \text{ has order } d} (x - \omega^i) \right)$ .
3.  $\deg \Phi_n(x) = \phi(n)$ .

**Lemma 2.64.**  $\Phi_n(x) \in \mathbb{Z}[x]$ .

*Proof.* Induct on  $n$ . The  $n = 1$  case is trivial. Let  $n > 1$  and assume  $\Phi_d(x) \in \mathbb{Z}[x]$  for all  $d < n$ . By Fact 2,  $x^n - 1 = \prod_{d|n, d>0} \Phi_d(x) = f(x)\Phi_n(x)$  where  $f(x) \in \mathbb{Z}[x]$  by induction. Note that  $f(x)$  is monic, so by the Division Algorithm,  $x^n - 1 = f(x)q(x) + r(x)$  where  $q(x), r(x) \in \mathbb{Z}[x]$ . Thus it is also true in  $\mathbb{C}[x]$ , where we know  $x^n - 1 = f(x)\Phi_n(x)$ . By the uniqueness of quotients and remainders,  $r(x) = 0$  and  $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$ . □

**Theorem 2.65.**  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ .

*Proof.* Suppose not. Then by Gauss's Lemma, since  $\Phi_n(x) \in \mathbb{Z}[x]$ , there exists  $f, g \in \mathbb{Z}[x]$  such that  $\Phi_n(x) = fg$  where  $f, g$  are monic and  $f$  is irreducible over  $\mathbb{Q}$  (if not, take an irreducible factor of  $f$  and group the other factors into  $g$ ). Let  $\omega$  be a root of  $f$  (and therefore of  $\Phi_n(x)$ ) and  $p$  any prime such that  $p \nmid n$ . Since  $\gcd(p, n) = 1$  we see  $\omega^p$  is also a primitive  $n$ th root of unity and thus is a root of  $\Phi_n$ .

Claim:  $\omega^p$  is a root of  $f$ .

*Proof:* If not, then  $g(\omega^p) = 0$  which says  $\omega$  is a root of  $g(x^p)$ . Since  $f$  is monic and irreducible,  $f = \text{Irred}(\omega, \mathbb{Q})$ . Thus  $f|g(x^p)$  in  $\mathbb{Q}[x]$  (and thus in  $\mathbb{Z}[x]$  as it is monic). So  $g(x^p) = fh$  for some  $h \in \mathbb{Z}[x]$ . In  $\mathbb{Z}_p[x]$  we see  $(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}\bar{h}$ . Let  $\beta$  be any root of  $\bar{f}(x)$  in  $\overline{\mathbb{Z}_p}$ . Then  $\bar{G}(\beta) = 0$  as we are in an ID. Then  $\overline{\Phi_n(x)}$  has multiple roots, which says  $\overline{x^n - 1} = x^n - 1$  has multiple roots in  $\mathbb{Z}_p[x]$ . But  $\gcd(x^n - 1, nx^{n-1}) = 1$ , a contradiction. Thus  $\omega^p$  is a root of  $f$ .

Thus every primitive  $n$ th root of unity is a root of  $f$  which is enough to say  $f = \Phi_n$  and since  $f$  is irreducible,  $\Phi_n(x)$  is irreducible.  $\square$

**Corollary 2.66.** If  $\omega \in \mathbb{C}$  is a primitive  $n$ th root of unity, then  $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$  and  $\text{Irred}(\omega, \mathbb{Q}) = \Phi_n$ .

**Note.** The above extension is normal as it is the splitting field for  $\Phi_n(x)$ .

**Example.** Let  $\omega$  be a primitive 9th root of unity. Then  $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(9) = 6$ . To find the minimal polynomial, note that  $x^9 - 1 = \Phi_1\Phi_3\Phi_9 = (x^3 - 1)\Phi_9$ . Thus  $\text{Irred}(\omega, \mathbb{Q}) = \Phi_9(x) = x^6 + x^3 + 1$ .

**Definition 2.67.** An extension  $\mathbb{Q}(\omega)/\mathbb{Q}$  where  $\omega$  is a root of unity is called a **cyclotomic extension**.

## 2.7 Inseparable Closure

**Definition 2.68.** Say the **inseparable closure** of  $E/F$  is  $F^{\text{insep}} = \{\alpha \in E \mid \alpha^{p^n} \in F \text{ for } n \gg 0\}$ . Note that  $F^{\text{insep}}/F$  is p.i. and  $F^{\text{insep}}$  is a field by the Frobenius property.

**Proposition 2.69.** Let  $E/F$  be normal and inseparable. Then there exists  $\alpha \in E \setminus F$  such that  $\alpha$  is p.i. over  $F$ .

*Proof.* By assumption, there exists  $\beta \in E$  which is inseparable over  $F$ . Let  $f(x) = \text{Irred}(\beta, F)$ . Then, as  $E/F$  is normal,  $f(x)$  splits in  $E$ . Let  $E' \subseteq E$  be the splitting field of  $f$  over  $F$ . Then  $[E' : F] < \infty$ ,  $E'/F$  is normal, and  $E'/F$  is inseparable as  $\beta \in E'$  is inseparable. So it is enough to show there exists a p.i. element in  $E'$ . So, since inseparable, we may suppose the characteristic of  $F$  is  $p > 0$ . Then  $f(x) = g(x^p)$  for some  $g(x) \in F[x]$ . Since  $f$  is irreducible,  $g$  is. If  $g$  is inseparable, then  $g(x) = h(x^p)$ . So  $g(x) = h(x^{p^2})$ . Continue until  $f(x) = g(x^{p^n})$  where  $g(x)$  is irreducible and separable (we must stop as  $\deg f < \infty$ ). Say  $\deg g = r$  and let  $\alpha_1, \dots, \alpha_r \in \overline{F}$  be the roots of  $g$ . Then  $g(x) = (x - \alpha_1) \cdots (x - \alpha_r)$  (note that it is monic as  $f$  is). So  $f(x) = (x^{p^n} - \alpha_1) \cdots (x^{p^n} - \alpha_r)$ . Let  $\beta_i$  be a root of  $x^{p^n} - \alpha_i$ . Then  $f(x) = ((x - \beta_1) \cdots (x - \beta_r))^{p^n}$ . Thus  $f(x) = \ell(x)^{p^n}$  where  $\ell(x) \in E'[x]$ . Say  $\ell(x) = x^r + d_{r-1}x^{r-1} + \dots + d_0 \in E'[x]$  and  $g(x) = x^r + c_{r-1}x^{r-1} + \dots + c_0 \in F[x]$ . Then  $\ell(x)^{p^n} = x^{p^n r} + d_{r-1}^{p^n} x^{p^n(r-1)} + \dots + d_0^{p^n} = f(x) = g(x^{p^n})$ . Thus  $d_i^{p^n} = c_i$ . Note that if  $\ell(x) \in F[x]$ , then  $f$  would be reducible. So there exists some  $i$  such that  $d_i \in E' \setminus F$ . Then  $d_i$  is p.i. over  $F$ .  $\square$

**Theorem 2.70.** Let  $E/F$  be normal with  $K = F^{\text{sep}}$  and  $L = F^{\text{insep}}$ . Then

1.  $K, L$  are fields
2.  $E/K$  is p.i. and  $E/L$  is separable
3.  $E = KL$ .

*Proof.* 1. Easy

2.  $E/K$  p.i. is a HW exercise. So we will only show  $E/L$  is separable. Know  $E/L$  is normal as  $E/F$  is. If it were inseparable, then the previous proposition says there exists  $\alpha \in E \setminus L$  which is p.i. over  $L$ , that is  $\alpha^{p^n} \in L$  for some  $n \gg 0$ . But  $L/F$  is p.i. so there exists  $r \gg 0$  such that  $(\alpha^{p^n})^{p^r} \in F$  which says  $\alpha$  is p.i. over  $F$ , that is,  $\alpha \in L$ , a contradiction. Thus  $E/L$  is separable.

3. Certainly  $KL \subseteq E$ . We see that  $E/KL$  is p.i. as  $E/K$  was and  $E/KL$  is separable as  $E/L$  was. Thus  $E/KL$  is both p.i. and separable which says  $[E : KL] = 1$ . Thus  $E = KL$ .  $\square$

**Example.** Let  $F = \mathbb{Z}_2(s, t)$  where  $s, t$  are indeterminants. Let  $f(x) = x^4 + sx^2 + t$  and  $\beta$  be a root of  $f$  in  $\overline{F}$ . Then  $F(\beta)/F$  is inseparable, but there are no p.i. elements in  $F(\beta) \setminus F$ .

*Proof.* First, we need to show  $f$  is irreducible. Let  $D = \mathbb{Z}_2[s, t]$ . Then  $f(x) \in D[x]$  and, by Gauss' Lemma, if  $f$  is reducible over  $F[x]$ , then  $f = gh$  for some  $g, h \in D[x]$ .

Case 1:  $\deg g = 1$ . Then  $g = x - u$  for  $u \in D$ . Then  $f(u) = 0$ , which implies  $u^4 + su^2 + t = 0$ . If  $u$  is not constant, say  $p$  is an irreducible factor of  $u$ , then  $p^2 | t$  by the 2 out of 3 lemma, a contradiction. So  $u$  is constant, that is,  $u = 0$  or 1. But  $f(0), f(1) \neq 0$ . So  $\deg g \neq 1$ .

Case 2:  $\deg g = 2$ . Then

$$\begin{aligned} f(x) &= (x^2 + ux + v)(x^2 + ax + b) \\ &= x^4 + (u+a)x^3 + (ua+v+b)x^2 + (ub+va)x + bv. \end{aligned}$$

So we have

$$\begin{aligned} (1) \quad &u + a = 0 \\ (2) \quad &ua + v + b = s \\ (3) \quad &ub + va = 0 \\ (4) \quad &bv = t \end{aligned}$$

From (4) we can say WLOG  $b = t$  and  $v = 1$ . From (2) we can say  $u = a$ . Plugging these into (3) we get  $ut = u$ , which implies  $u = 0 = a$ . Plugging this into (2) gives  $s = t + 1$ , a contradiction as they are indeterminants.

Thus  $f$  is irreducible. This tells us that  $[F(\beta) : F] = 4$ . We also know that  $\beta$  is inseparable as  $f' = 0$ . So  $[F(\beta) : F]_S = 1$  or 2. On the other hand,  $g(x) = \text{Irred}(\beta^2, F) = x^2 + sx + t$  (which is irreducible as  $g(x^2) = f(x)$ , which is irreducible) and  $g(x)$  is separable (as  $f' \neq 0$ .) So  $F(\beta^2)$  is separable. [Note that by HW4 #1, this says  $F(\beta^2) = F^{sep}$ .] This gives  $[F(\beta) : F]_i = 2 = [F(\beta) : F]_S$ .

Claim:  $x^2 - t$  has no roots in  $F(\beta)$ .

*Proof:* Suppose  $\gamma \in F(\beta)$  satisfies  $\gamma^2 = t$ . Then  $\gamma = c_0 + c_1\beta + c_2\beta^2 + c_3\beta^3$ ,  $c_i \in F$  which implies  $t = \gamma^2 = c_0^2 + c_1^2\beta^2 + c_2^2\beta^4 + c_3^2\beta^6$ . For simplicity, define  $d_i = c_i^2 \in F^2 = \mathbb{Z}_2(s^2, t^2)$ . Then  $t = d_0 + d_1\beta^2 + d_2\beta^4 + d_3\beta^6$ . Of course, since  $f(\beta) = 0$ , we know

$$\begin{aligned} \beta^4 &= s\beta^2 + t \\ \beta^6 &= \beta^2(s\beta^2 + t) = s\beta^4 + t\beta^2 = s^2\beta^2 + st + t\beta^2. \end{aligned}$$

So

$$\begin{aligned} t &= d_0 + d_1\beta^2 + d_2(s\beta^2 + t) + d_3(s^2\beta^2 + st + t\beta^2) \\ &= (d_0 + d_2t + d_3st) + (d_1 + d_2s + d_3s^2 + d_3t)\beta^2. \end{aligned}$$

Since  $t \in F$  and the  $\beta$ 's form a basis for  $F(\beta)$ , we get

$$\begin{aligned} (1) \quad &t = d_0 + d_2t + d_3st \\ (2) \quad &0 = d_1 + d_2s + d_3s^2 + d_3t. \end{aligned}$$

Then (1) implies  $(1 + d_2 + d_3s)t = d_0$ . So  $d_0 = 0$ , and  $d_2 = 1 + d_3s$ . Plugging this into (2), we see

$$0 = d_1 + (1 + d_3s)s + d_3s^2 + d_3t = d_1 + s + d_3t$$

as we are in  $\mathbb{Z}_2$ . But this says  $s = d_1 + d_3t \in \mathbb{Z}_2(t, s^2)$ , a contradiction.  $\square$

Suppose  $\delta \in F(\beta) \setminus F$  is p.i over  $F$ . Then  $2 \leq [F(\delta) : F] = [F(\delta) : F]_i \leq [F(\beta) : F]_i = 2$ . So we see  $\delta^2 \in F$ . So  $[F(\beta) : F(\delta)] = 2$ . Consider  $x^2 + sx + t = (x - \alpha_1)(x - \alpha_2)$  in  $\overline{F}[x]$ . Suppose  $\beta^2 = \alpha_1$  and let  $\rho$  be a root of  $x^2 - \alpha_2$ . Then  $f(x) = (x - \beta)^2(x - \rho)^2$ . Since  $\beta$  is separable over  $F(\delta)$ , we see  $h(x) = \text{Irred}(\beta, F(\delta)) = (x - \beta)(x - \rho) = x^2 + (\beta + \rho)x + \beta\rho$ . Thus we see  $\beta\rho \in F(\delta) \subset F(\beta)$ . Also  $g(x)^2 = f(x)$ , which implies  $(\beta\rho)^2 = t$ , a contradiction to the above claim.

## 2.8 Galois Groups

**Definition 2.71.** Let  $E/F$  be a field extension. Then  $\text{Aut}(E/F) = \{\phi \in \text{Aut}(E) : \phi \text{ fixes } F\}$ .

**Remark.** Let  $E/F$  be a finite extension.

1.  $|\text{Aut}(E/F)| \leq [E : F]_S$  with equality if and only if  $E/F$  is normal.
2.  $|\text{Aut}(E/F)| = [E : F]$  if and only if the extension is normal and separable.

*Proof.* 1. By definition of the separable degree and normal.

2. We know  $|\text{Aut}(E/F)| \leq [E : F]_S \leq [E : F]$ . Then we get equality if and only if the extension is normal and separable by definition of normal and separable.  $\square$

**Definition 2.72.** Say  $E/F$  is **Galois** if  $E/F$  is normal and separable. In this case, we say  $\text{Aut}(E/F)$  is the **Galois Group** and denote it  $\text{Gal}(E/F)$ .

**Example.** Let  $E$  be the splitting field of  $x^3 - 2$  over  $\mathbb{Q}$ . Find  $\text{Gal}(E/\mathbb{Q})$ .

First note that this is a Galois extension as we are in characteristic 0 (thus every extension is separable) and  $E$  is a splitting field (thus normal). Further, since  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  and  $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ , which are relatively prime, we see  $[E : \mathbb{Q}] = 6$ . So  $|\text{Aut}(E/\mathbb{Q})| = 6$ . Further, we know that any automorphism of  $E$  sends roots of  $x^3 - 2$  to other roots and similarly for  $x^2 + x + 1$ . So let  $\sigma : E \rightarrow E$  be defined by  $\left\{ \begin{array}{l} \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} \\ \omega \mapsto \omega \end{array} \right\}$  and  $\tau : E \rightarrow E$  be defined by  $\left\{ \begin{array}{l} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{array} \right\}$ . Then  $\sigma^3 = 1_E, \tau^2 = 1_E$  and  $\sigma\tau \neq \tau\sigma$ . Thus (since there is only nonabelian group of order 6),

$$\text{Gal}(E/F) = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^2 \rangle.$$

**Example.** Let  $E$  be the splitting field of  $x^6 + 3$  over  $\mathbb{Q}$ . Recall (a test problem) that the splitting field is  $E = \mathbb{Q}(\omega \sqrt[6]{3})$  where  $\omega = e^{\pi i/6}$  and  $[E : \mathbb{Q}] = 6$ . Define  $\sigma_i : E \rightarrow E$  by  $\omega \sqrt[6]{3} \mapsto \omega^{2i+1} \sqrt[6]{3}$ . Then  $G = \text{Gal}(E/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_6\}$ . We just need to decide whether  $G$  is  $C_6$  or  $S_3$ . First note that  $\omega^2 = \frac{1}{2} + \frac{1}{2}(\omega \sqrt[6]{3})^3$  and thus  $\sigma_1(\omega^2) = \frac{1}{2} + \frac{1}{2}(\sigma_1(\omega \sqrt[6]{3}))^3 = \frac{1}{2} - \frac{i}{2}\sqrt{3} = \omega^{10}$ . Thus we see  $\sigma_1^2(\omega \sqrt[6]{3}) = \sigma_1(\omega^3 \sqrt[6]{3}) = \sigma_1(\omega^2)\sigma_1(\omega \sqrt[6]{3}) = \omega^{10}\omega^3 \sqrt[6]{3} = \omega \sqrt[6]{3}$ . Thus  $\sigma_1^2 = 1$ . Similarly, we can show  $\sigma_2^3 = 1$  and  $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$ . Thus  $G = S_3$ .

**Proposition 2.73.** Let  $\omega \in \mathbb{C}$  be a primitive  $n$ th root of unity. Then  $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_n^*$ .

*Proof.* By previous study, we know  $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ . Thus  $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\phi_i : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega) \mid \phi_i(\omega) = \omega^i, \text{ where } \gcd(i, n) = 1, 1 \leq i < n\}$ . Define  $\rho : \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \rightarrow \mathbb{Z}_n^*$  by  $\phi_i \mapsto [i]_n$ . Clearly,  $\rho$  is an isomorphism.  $\square$

**Remarks.** Let  $E/F$  be Galois and  $L$  an intermediate field.

1. Then  $E/L$  is Galois and  $\text{Gal}(E/L) < \text{Gal}(E/F)$ .

*Proof.* If  $E/F$  is separable and normal, then so is  $E/L$ . Also, any automorphism of  $E$  which fixes  $L$  also fixes  $F$ .  $\square$

2. Let  $H \leq \text{Gal}(E/F)$ . Then  $E_H = \{u \in E \mid \sigma(u) = u \text{ for all } \sigma \in H\}$  is an intermediate field of  $E/F$ . Call it the **fixed field** of  $H$ .

**Theorem 2.74.** *Let  $E/F$  be Galois and  $G = \text{Gal}(E/F)$ . Then  $E_G = F$ .*

*Proof.* Clearly,  $F \subseteq E_G$ . Let  $\alpha \in E_G$  and  $\sigma : F(\alpha) \rightarrow \bar{F}$  be an embedding which fixes  $F$ . Then we can extend  $\sigma$  to  $\tau : E \rightarrow \bar{F}$ . Since  $E/F$  is normal,  $\tau$  is an automorphism, which implies  $\tau \in G$ . Then  $\alpha \in E_G$  implies  $\tau(\alpha) = \alpha$  and thus  $\sigma(\alpha) = \alpha$ . So  $\sigma = 1_{F(\alpha)}$ . Then  $1 = [F(\alpha) : F]_S = [F(\alpha) : F]$ , since separable. Thus  $\alpha \in F$  and  $E_G = F$ .  $\square$

**Lemma 2.75.** *Let  $E/F$  be a separable extension such that  $[F(\alpha) : F] \leq n$  for all  $\alpha \in E$ . Then  $[E : F] \leq n$ .*

*Proof.* Choose  $\alpha \in E$  such that  $[F(\alpha) : F] = m$  is as large as possible (can do this as it is bounded above by  $n$ .) If  $E \neq F(\alpha)$ , let  $\beta \in E \setminus F(\alpha)$ . Then, by the Primitive Element Theorem, there exists  $\gamma \in E$  such that  $F(\gamma) = F(\alpha, \beta)$ . Then  $[F(\gamma) : F] > [F(\alpha) : F] = m$ , a contradiction. So  $E = F(\alpha)$  which says  $[E : F] = [F(\alpha) : F] \leq n$ .  $\square$

**Theorem 2.76 (Artin's Theorem).** *Let  $E$  be a field and  $G$  a finite subgroup of  $\text{Aut}(E)$ . Let  $F = E_G$ . Then*

1.  $E/F$  is finite, Galois, and  $[E : F] = |G|$
2.  $G = \text{Gal}(E/F)$ .

*Proof.* Let  $\alpha \in E$  and  $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\} \subseteq \{\phi(\alpha) \mid \phi \in G\}$  be maximal with respect to the property  $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$  are distinct. Let  $\tau \in G$ . Since  $\tau$  is injective,  $\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)$  are also distinct. Thus  $\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)$  is a permutation of  $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ . Let  $f_\alpha(x) = \prod_{i=1}^r (x - \sigma_i(\alpha))$ . Then for  $\tau \in G$ ,  $f_\alpha^\tau(x) = f_\alpha(x)$ . So  $f_\alpha(x) \in F[x]$ . Thus  $\text{Irred}(\alpha, F) \mid f_\alpha(x)$  and  $f_\alpha(x)$  has distinct roots. Thus  $\alpha$  is separable over  $F$ . Since  $\alpha$  was arbitrary,  $E/F$  is separable. Also for all  $\alpha \in E$ ,  $f_\alpha(x)$  splits in  $E$  so  $\text{Irred}(\alpha, F)$  splits in  $E$  which says  $E/F$  is normal. Thus  $E/F$  is Galois. Now  $[F(\alpha) : F] \leq \deg f_\alpha(x) = r \leq |G|$ . Since  $E/F$  is separable, the lemma tells us  $[E : F] \leq |G|$ . Now  $G \leq \text{Gal}(E/F)$  thus we have  $|G| \leq |\text{Gal}(E/F)| = [E : F] \leq |G|$ . So  $|G| = |\text{Gal}(E/F)| = [E : F]$  which implies  $G = \text{Gal}(E/F)$ .  $\square$

**Theorem 2.77 (Fundamental Thm of Galois Theory).** *Let  $E/F$  be a finite Galois Extension. Then there is a bijective correspondence between the intermediate fields of  $E/F$  and the subgroups of  $\text{Gal}(E/F)$  defined by  $L \mapsto \text{Gal}(E/L)$  and  $H \mapsto E_H$  for an intermediate field  $L$  and a subgroup  $H$ .*

*Proof.* By the previous lemma,  $E_{\text{Gal}(E/L)} = L$ . By Artin's Theorem, for  $H < \text{Gal}(E/F)$ ,  $E/E_H$  is Galois and  $\text{Gal}(E/E_H) = H$ .  $\square$

**Note.** The correspondence is inclusion reversing. That is, for intermediate fields

$$L_1 \subseteq L_2 \text{ we see } \text{Gal}(E/L_1) \supseteq \text{Gal}(E/L_2)$$

and for subgroups

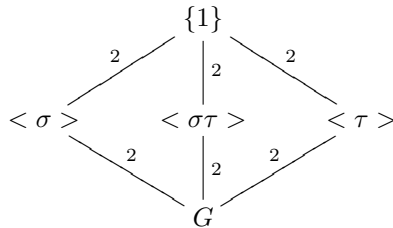
$$H_1 \supseteq H_2 \text{ we see } E_{H_1} \subseteq E_{H_2}.$$

Recall that Artin's Theorem says  $|\text{Gal}(E/L)| = [E : L]$  and for  $H < G = \text{Gal}(E/F)$ ,  $|H| = [E : E_H]$ , which implies  $[G : H] = [E_H : F]$ . Thus we can construct the following diagram:

$$\begin{array}{ccccc} E & \longleftrightarrow & \{1\} & \longleftrightarrow & E \\ \left| \begin{array}{c} [E:L] \\ \\ [L:F] \end{array} \right. & & \left| \begin{array}{c} |H| \\ \\ [G:H] \end{array} \right. & & \left| \begin{array}{c} \\ \\ [E_H:F] \end{array} \right. \\ L & \longleftrightarrow & H = \text{Gal}(E/L) & \longleftrightarrow & E_H \\ F & \longleftrightarrow & G = \text{Gal}(E/F) & \longleftrightarrow & E_G \end{array}$$

**Example.** Let  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Find primitive elements for all intermediate fields of  $E/\mathbb{Q}$ .

1. Compute  $G = \text{Gal}(E/\mathbb{Q})$ . We know  $[E : \mathbb{Q}] = 4$  and there are 4 obvious automorphisms:  $\sqrt{2} \mapsto \pm\sqrt{2}$  and  $\sqrt{3} \mapsto \pm\sqrt{3}$ . So that must be all of them. It is easy to check that  $G = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle = C_2 \times C_2$  where  $\sigma : E \rightarrow E$  sends  $\sqrt{2} \mapsto -\sqrt{2}$  and  $\tau : E \rightarrow E$  sends  $\sqrt{3} \mapsto -\sqrt{3}$ .
2. Create a subgroup lattice:

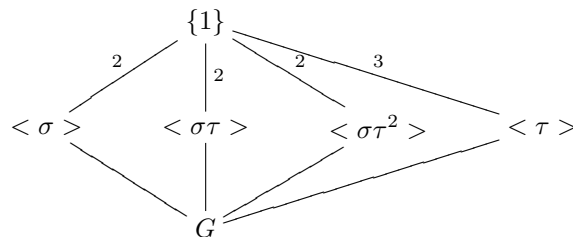


This tells us our Intermediate fields are  $E_{\langle \sigma \rangle}, E_{\langle \sigma\tau \rangle}, E_{\langle \tau \rangle}$ , all of which have degree 2 over  $\mathbb{Q}$ . Now,  $\sqrt{3}$  is fixed by  $\sigma$ ,  $\sqrt{2}$  by  $\tau$ , and  $\sqrt{6}$  by  $\sigma\tau$ . So

$$E_{\langle \sigma \rangle} = \mathbb{Q}(\sqrt{3}), E_{\langle \sigma\tau \rangle} = \mathbb{Q}(\sqrt{6}), E_{\langle \tau \rangle} = \mathbb{Q}(\sqrt{2})$$

and of course  $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$  (this element is not fixed by any of the above automorphisms.)

**Example.** Let  $E = \mathbb{Q}(\omega \sqrt[6]{3})$ ,  $\omega = e^{2\pi i/12}$ . Then  $E$  is the splitting for  $x^6 + 3$ . Recall from before that  $\text{Gal}(E/\mathbb{Q}) = S_3$  and was generated by  $\sigma : E \rightarrow E$  defined by  $\omega \sqrt[6]{3} \mapsto \omega^3 \sqrt[6]{3}$  and  $\tau : E \rightarrow E$  defined by  $\omega \sqrt[6]{3} \mapsto \omega^5 \sqrt[6]{3}$ . Now, we can again make our subgroup lattice:



- We see  $\tau$  fixes  $\omega^2 = e^{\pi i/3}$ , an element of degree 2 over  $\mathbb{Q}$  (the irreducible polynomial is  $x^2 + x + 1$ .) So  $E_{\langle \tau \rangle} = \mathbb{Q}(\omega^2)$ .
- Since  $\sigma^2 = 1$ , we see  $\omega \sqrt[6]{3} \sigma(\omega \sqrt[6]{3}) = \omega \sqrt[6]{3} \omega^3 \sqrt[6]{3} = \omega^4 \sqrt[6]{3}$  is fixed by  $\sigma$  and not in  $\mathbb{Q}$ . Thus  $E_{\langle \sigma \rangle} = \mathbb{Q}(\omega^4 \sqrt[6]{3})$ .
- We expect the other roots of  $x^3 - 3$  to be fixed by our other two intermediate fields.
- Since  $(\sigma\tau)^2 = 1$ , we see  $\omega \sqrt[6]{3} \sigma\tau(\omega \sqrt[6]{3}) = \sqrt[6]{3}$  is fixed by  $\sigma\tau$ . So  $E_{\langle \sigma\tau \rangle} = \mathbb{Q}(\sqrt[6]{3})$ .
- Similarly, we see  $E_{\langle \sigma\tau^2 \rangle} = \mathbb{Q}(\omega^8 \sqrt[6]{3})$ .

**Definition 2.78.** Let  $F$  be a field and  $\alpha \in \overline{F}$ . Let  $\sigma_1, \dots, \sigma_s$  be the distinct embeddings of  $F(\alpha) \rightarrow \overline{F}$  fixing  $F$ . Then  $\sigma_1(\alpha), \dots, \sigma_s(\alpha)$  are called the  $F$ -**conjugates** of  $\alpha$ , that is, the  $F$ -conjugates of  $\alpha$  are the distinct roots of  $\text{Irred}(\alpha, F)$ .

**Remark.** Suppose  $\alpha$  is separable over  $F$  and  $\text{Irred}(\alpha, F) = \prod_{i=1}^s (x - \sigma_i(\alpha)) = x^n + c_{n-1}x^{n-1} + \dots + c_0$ . Then  $\prod \sigma_i(\alpha) = c_0$  and  $\sum \sigma_i(\alpha) = -c_{n-1}$ . Thus they are in  $F$ .

**Proposition 2.79.** Let  $E/F$  be a finite Galois extension. Say  $E = F(\alpha)$ . Then

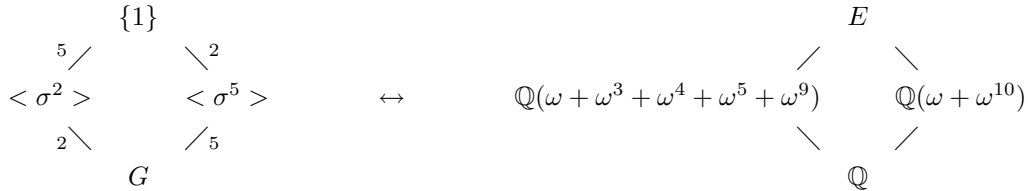
1.  $\text{Irred}(\alpha, E_H) = \prod_{h \in H} (x - h(\alpha)) = x^n - c_1 x^{n-1} + \dots + c_n$ .
2.  $E_H = F(c_1, \dots, c_n)$ .



*Proof.* 1. Let  $f(x) = \prod(x - h(\alpha))$ . If  $h' \in H$ , then  $f^{h'}(x) = \prod(x - h'h(\alpha)) = f(x)$  as  $h' \in H$ . Thus  $f(x) \in E_H[x]$ . Note that  $\deg f = |H|$  and  $\deg \text{Irred}(\alpha, E_H) = [E_H(\alpha) : E_H] = [E : H] = |H| = \deg f$ . Since  $f(\alpha) = 0$  ( $1 \in H$ ) and  $f$  is monic,  $f = \text{Irred}(\alpha, E_H)$ .

2. Let  $L = F(c_1, \dots, c_n) \subseteq E_H$  (as the  $c_i$ 's are fixed by  $H$ ). Then  $f(x) \in L[x]$ ,  $f$  is irreducible, and  $f(\alpha) = 0$ . Thus  $f = \text{Irred}(\alpha, L)$ . So  $[E : L] = [E : E_H]$  which implies  $L = E_H$ .  $\square$

**Example.** Let  $\omega$  be a primitive 11th root of unity and  $E = \mathbb{Q}(\omega)$ . We've proved  $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_{11}^* = C_{10}$ . Say  $\text{Gal}(E/\mathbb{Q}) = \langle \sigma \rangle$  where  $\sigma : E \rightarrow E$  is such that  $\omega \mapsto \omega^2$ .



- $\omega + \sigma^5(\omega) = \omega + \omega^{10} \notin \mathbb{Q}$  as otherwise  $\omega$  would be a root of both  $x^{10} + x - q$  for some  $q \in \mathbb{Q}$  and  $x^{10} + x^9 + \dots + 1$ , a contradiction as the minimal polynomial is unique.
- $\omega + \sigma^2(\omega) + \sigma^4(\omega) + \sigma^6(\omega) + \sigma^8(\omega) = \omega + \omega^4 + \omega^5 + \omega^9 + \omega^3 \notin \mathbb{Q}$  as then  $[\mathbb{Q}(\omega) : \mathbb{Q}] \leq 9$ , a contradiction.

**Theorem 2.80.** Let  $E/F$  be a finite Galois extension and  $G = \text{Gal}(E/F)$ . Let  $L$  be an intermediate field and  $H = \text{Gal}(E/L)$ . Then

1.  $L/F$  is normal if and only if  $H$  is normal
2. If  $H \triangleleft G$ , then  $\text{Gal}(L/F) \cong G/H$ .

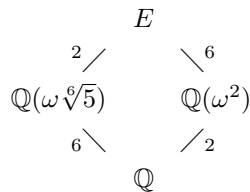
*Proof.*  $\Rightarrow$ : Define  $\phi : G \rightarrow \text{Gal}(L/F)$  by  $\sigma \mapsto \sigma|_L$ . This is well-defined as  $L/F$  is normal. Furthermore,  $\phi$  is surjective as for  $\pi \in \text{Gal}(L/F)$ , we can extend  $\pi$  to an element  $\sigma \in G$ . Thus  $\sigma|_L = \pi$  and thus  $\text{Gal}(L/F) \cong G/\ker \phi$ . Now  $\sigma \in \ker \phi$  if and only if  $\sigma|_L = 1$  if and only if  $\sigma$  fixes  $L$  if and only if  $\sigma \in H$ . Thus  $H \triangleleft G$  and  $\text{Gal}(L/F) \cong G/H$ .

$\Leftarrow$ : Suppose  $\sigma : L \rightarrow \bar{F}$  fixes  $F$ . Need to show  $\sigma(L) \subseteq L$ . Let  $\alpha \in L$ . Extend  $\sigma$  to  $\tau : E \rightarrow \bar{F}$ . Then  $\tau \in G$  as  $E/F$  is normal. It is enough to show  $\tau(\alpha) \in L = E_H$ . Let  $h \in H$ . As  $H \triangleleft G$ ,  $\tau^{-1}h\tau \in H$ . Therefore  $\tau^{-1}h\tau(\alpha) = \alpha$ , which implies  $h\tau(\alpha) = \tau(\alpha)$ . Thus  $h$  fixes  $\tau(\alpha)$ . Since  $h$  is arbitrary,  $\tau(\alpha) \in E_H = L$ . Thus  $\sigma$  is an automorphism of  $L$  and  $L/F$  is normal.  $\square$

**Definition 2.81.** Let  $E/F$  be a Galois extension. Say  $E/F$  is **abelian/cyclic/solvable** if  $\text{Gal}(E/F)$  is abelian/cyclic/solvable.

**Example.** Cyclotomic Extensions are abelian.

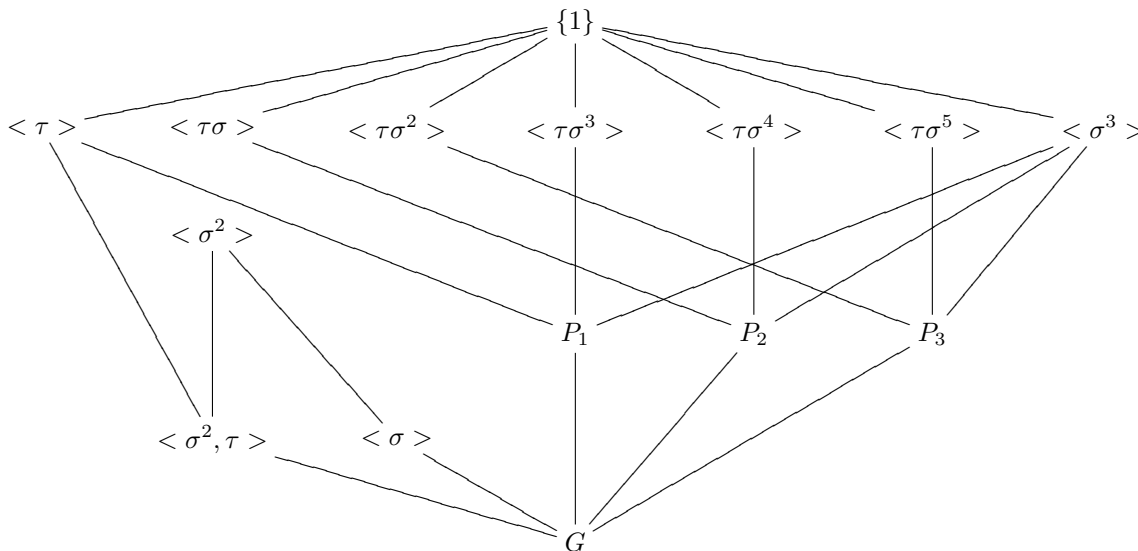
**Example.** Let  $E$  be the splitting field of  $x^6 + 5$  over  $\mathbb{Q}$ . Recall  $[E : \mathbb{Q}] = 12$  and  $E = \mathbb{Q}(\omega^2, \omega^{\sqrt[6]{5}})$  for  $\omega = e^{2\pi i/12}$ .



As  $\text{Irred}(\omega^{\sqrt[6]{5}}, \mathbb{Q}(\omega^2)) = x^6 + 5$ , we can define  $\sigma : E \rightarrow E$  such that  $\left\{ \begin{array}{l} \omega^{\sqrt[6]{5}} \mapsto \omega^3 \sqrt[6]{5} \\ \omega^2 \mapsto \omega^2 \end{array} \right\}$ . Similarly, we can define  $\tau : E \rightarrow E$  by  $\left\{ \begin{array}{l} \omega^{\sqrt[6]{5}} \mapsto \omega^{\sqrt[6]{5}} \\ \omega^2 \mapsto \omega^{10} \end{array} \right\}$ . Note that  $\sigma^i : \omega^{\sqrt[6]{5}} \mapsto \omega^{2i+1} \sqrt[6]{5}$  as  $\sigma$  fixes  $\omega^2$ . So  $|\sigma| = 6$  and clearly  $|\tau| = 2$ . Since  $\tau \notin \langle \sigma \rangle$ ,

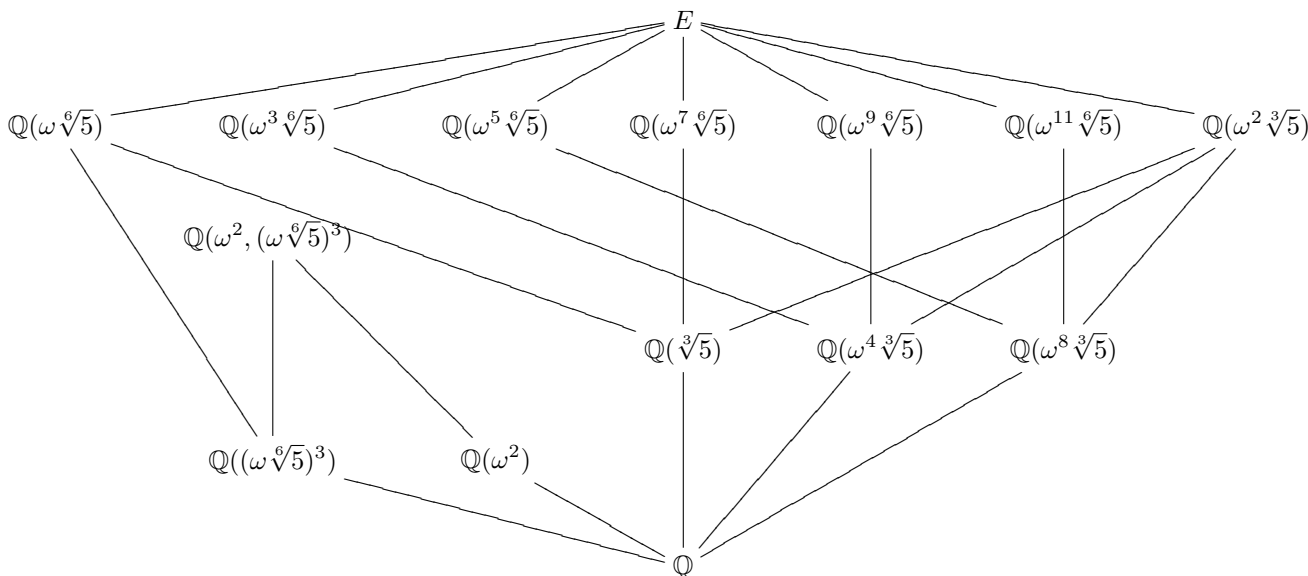
$G = \langle \sigma, \tau \rangle$ . Note  $\sigma\tau(\omega^{\sqrt[6]{5}}) = \omega^3 \sqrt[6]{5}$  but  $\tau\sigma(\omega^{\sqrt[6]{5}}) = \tau(\omega^3 \sqrt[6]{5}) = \tau(\omega^2)\tau(\omega^{\sqrt[6]{5}}) = \omega^{10}\omega^{\sqrt[6]{5}} = \omega^{11} \sqrt[6]{5}$ . Thus  $\tau\sigma \neq \sigma\tau$ . Note  $\tau\sigma\tau \in \langle \sigma \rangle$  and by order arguments,  $\tau\sigma\tau = \sigma^{-1} = \sigma^5$ . So  $G = D_{12}$ . Now we want to find the subgroups of  $D_{12}$ .

- 7 subgroups of order 2:  $\langle \sigma^3 \rangle, \langle \tau \rangle, \langle \tau\sigma \rangle, \langle \tau\sigma^2 \rangle, \langle \tau\sigma^3 \rangle, \langle \tau\sigma^4 \rangle, \langle \tau\sigma^5 \rangle$  (All the subgroups generated by the elements of order 2.)
- 1 subgroup of order 3:  $\langle \sigma^2 \rangle$  (since either the Sylow 3 or Sylow 4 subgroup is normal by Sylows Theorems but the Sylow 4 subgroup can not be normal as then we'd only have 3 order 2 elements, not 7)
- 3 subgroups of order 4:  $P_1 = \langle \sigma^3, \tau \rangle, P_2 = \langle \sigma^3, \tau\sigma \rangle, P_3 = \langle \sigma^3, \tau\sigma^2 \rangle$  (by Sylow's Theorems)
- 2 subgroups order 6:  $\langle \sigma \rangle, \langle \sigma^2, \tau \rangle$ .



To translate this into field extensions, note:

- Degree 6 extensions: Roots of  $x^6 + 5$  correspond to  $E_{\langle \tau\sigma^i \rangle}$  and  $E_{\langle \sigma^3 \rangle} = \mathbb{Q}(\omega^2, \sqrt[6]{5})$ .
- Degree 4 extension: We've seen this is  $\mathbb{Q}(i\sqrt{3}, i\sqrt{5}) = \mathbb{Q}(\omega^2, (\omega^{\sqrt[6]{5}})^3)$ .
- Degree 2 extensions: We know one is  $E_{\langle \sigma \rangle} = \mathbb{Q}(\omega^2)$ . We expect the other to be  $E_{\langle \sigma^2, \tau \rangle} = \mathbb{Q}((\omega^{\sqrt[6]{5}})^3)$ . In fact it is as  $\sigma^2((\omega^{\sqrt[6]{5}})^3) = (\sigma^5 \sqrt[6]{5})^3 = \omega^3 \sqrt{5} = (\sqrt[6]{5})^3$  and  $\tau((\omega^{\sqrt[6]{5}})^3) = (\omega^{\sqrt[6]{5}})^3$ .
- Degree 3 extensions: Roots of  $x^3 + 5$ .



**Theorem 2.82.** Let  $F$  be a finite field and  $E/F$  a finite extension. Then  $E/F$  is cyclic.

*Proof.* Say  $\text{char } F = p$ . Then  $\mathbb{Z}_p \subseteq F$ . Since  $\text{Gal}(E/F) \subseteq \text{Gal}(E/\mathbb{Z}_p)$ , it is enough to show  $\text{Gal}(E/\mathbb{Z}_p)$  is cyclic. Say  $[E : \mathbb{Z}_p] = n$ . Then  $|E| = p^n$ . Let  $\sigma : E \rightarrow E$  be the Frobenius map. The  $\sigma \in \text{Gal}(E/\mathbb{Z}_p)$ .

Claim:  $\text{Gal}(E/\mathbb{Z}_p) = \langle \sigma \rangle$ .

*Proof:* We want to show  $|\sigma| = n$ . Suppose  $\sigma^i = 1$  for some  $1 \leq i < n$ . Then  $a = \sigma^i(a) = a^{p^i}$  for all  $a \in E$ . Then  $x^{p^i} - x$  has  $|E| = p^n$  roots, contradiction as  $p^n > p^i$ . Thus  $|\sigma| = n$ . □

**Corollary 2.83.** Let  $E$  be a field with  $p^n$  elements. Then  $E$  contains a subfield with  $p^m$  elements if and only if  $m|n$ . Equivalently,  $x^{p^m} - x$  splits in  $E$  if and only if  $m|n$ .

*Proof.* Let  $G = \text{Gal}(E/\mathbb{Z}_p)$ . Then  $n = |G| = [E : \mathbb{Z}_p]$ . So  $E$  contains a subfield  $F$  with order  $p^m$  if and only if there exists  $F \subseteq E$  with  $[F : \mathbb{Z}_p] = m$  if and only if there exists  $F \subseteq E$  with  $[E : F] = \frac{n}{m}$  if and only if there exists a subgroup  $H \subseteq G$  such that  $|H| = \frac{n}{m}$  if and only if  $m|n$  as  $G$  is cyclic. □

**Remark.** Let  $E$  be the splitting field of a degree  $n$  separable irreducible polynomial  $f \in F[x]$ . Then  $E/F$  is Galois and  $\text{Gal}(E/F) \cong$  a subgroup of  $S_n$ .

*Proof.* Let  $E = F(\alpha_1, \dots, \alpha_n)$  where  $\alpha_1, \dots, \alpha_n$  are the roots of  $f(x)$ . Define  $\phi : \text{Gal}(E/F) \rightarrow \text{Perm}(\Gamma)$  such that  $\sigma \mapsto \sigma_\Gamma$  where  $\Gamma = \{\alpha_1, \dots, \alpha_n\}$ . Then  $\phi$  is injective as  $\sigma$  is determined by  $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ . □

**Example.** Consider  $x^3 - 2 \in \mathbb{Q}(\omega)[x]$  where  $\omega = e^{2\pi i/3}$ . This is irreducible as  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  and  $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$  and  $\text{gcd}(2, 3) = 1$ . Then  $|\text{Gal}(E/\mathbb{Q}(\omega))| = 3$ .

Let  $x_1, \dots, x_n$  be independent indeterminants over a field  $F$ . Let  $E = F(x_1, \dots, x_n)$ . Let  $\sigma \in S_n$ . Then there exists an automorphism of  $E$  induced by  $\sigma$ , say  $\tilde{\sigma} : E \rightarrow E$  defined by  $\frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \mapsto \frac{f(\sigma(x_1), \dots, \sigma(x_n))}{g(\sigma(x_1), \dots, \sigma(x_n))}$ .

**Example.** Let  $n = 3$  and  $\sigma = (123)$ . Then

$$\tilde{\sigma} \left( \frac{x_1^2 + 3x_1x_3 + x_2^2}{x_1x_2 - 2x_1^5} \right) = \frac{x_2^2 + 3x_2x_1 + x_3^2}{x_2x_3 - 2x_2^5}.$$

For simplification, we will identify  $\tilde{\sigma}$  with  $\sigma$ .

Let  $L = E_{S_n}$ . By Artin's Theorem,  $E/L$  is Galois and  $\text{Gal}(E/L) \cong S_n$ . We call  $L$  the **field of symmetric rational functions**. Now, any finite group is a subgroup of a group of permutations. So  $H \leq S_n$  will correspond to an intermediate field of  $E/L$ .

**Example.** Let  $n = 3, F \subseteq L$ . Let  $t$  be an indeterminant over  $E$  and consider  $f(t) = \prod_{i=1}^n (t - x_i) \in E[t]$ . For all  $\sigma \in S_n$ , we see  $f^\sigma(t) = f(t)$ . Thus  $f(t) \in L[t]$ . Then, if  $f = t^n - s_1t^{n-1} + s_2t^{n-2} - \dots + (-1)^ns_n$ , we see  $s_i \in L$  for all  $i$ . Call  $\{s_i\}$  the **elementary symmetric functions in  $x_1, \dots, x_n$** .

**Theorem 2.84.** With the above notation,  $L = E_{S_n} = F(s_1, \dots, s_n)$ .

*Proof.* Note  $f(t) \in F(s_1, \dots, s_n)[t]$ . Then  $E = F(s_1, \dots, s_n)(x_1, \dots, x_n)$  is the splitting field of  $f(t)$  over  $F(s_1, \dots, s_n)$ . But  $\deg f = n$ , so  $[E : F(s_1, \dots, s_n)] \leq n!$ . But  $[E : F(s_1, \dots, s_n)] \geq [E : L] = n!$ . Thus  $E = L$ . □

**Inverse Galois Problem:** Is every finite group the Galois group of a Galois extension of  $\mathbb{Q}$ ?

**Fact.** For all  $n \in \mathbb{Z}$  such that  $n > 0$ , there exist infinitely many primes  $p$  such that  $p \equiv 1 \pmod n$ .

**Theorem 2.85.** Let  $G$  be a finite abelian group. Then there exists a primitive  $m$ th root of unity  $\omega$  and a field  $E \subseteq \mathbb{Q}(\omega)$  such that  $\text{Gal}(E/\mathbb{Q}) \cong G$ .

*Proof.* Let  $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ . Let  $p_1, \dots, p_k$  be distinct primes such that  $p_i \equiv 1 \pmod{n_i}$ . (Note we use the claim here in the case of  $n_i = n_j$ .) Let  $m = p_1 \cdots p_k$ . Let  $\omega$  be a primitive  $m$ th root of unity. Then  $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_m^* = \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_k}^* \cong C_{p_1-1} \times \cdots \times C_{p_k-1}$ . Since  $n_i | p_i - 1$ , let  $H_i \leq C_{p_i-1}$  such that  $|H_i| = \frac{p_i-1}{n_i}$ . Then  $H_1 \times \cdots \times H_k$  is a normal subgroup of  $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ . Let  $E$  be the fixed field for  $H_1 \times \cdots \times H_k$ . Then  $E/\mathbb{Q}$  is normal and  $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_k}^*/H_1 \times \cdots \times H_k \cong C_{n_1} \times \cdots \times C_{n_k} \cong G$ .  $\square$

## 2.9 Norm and Trace

**Definition 2.86.** Let  $E/F$  be a finite extension. Let  $\sigma_1, \dots, \sigma_r$  be the distinct embeddings of  $E \rightarrow \bar{F}$  which fix  $F$ . For  $\alpha \in E$ , define  $N_F^E(\alpha) = (\sigma_1(\alpha) \cdots \sigma_r(\alpha))^{[E:F]}$  as the **norm** of  $\alpha$  and  $Tr_F^E(\alpha) = (\sigma_1(\alpha) + \cdots + \sigma_r(\alpha))^{[E:F]}$  as the **trace** of  $\alpha$ .

**Examples.**

1. If  $E = \mathbb{Q}(\sqrt{2})$ . Then  $1 : E \rightarrow E$  and  $\sigma : E \rightarrow E$  defined by  $\sqrt{2} \mapsto -\sqrt{2}$  are the only 2 embeddings. So  $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$  and  $Tr(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a$ .
2. Let  $E = \mathbb{Q}(\sqrt[3]{2})$ . Then there are three embeddings:  $1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \tau : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$ , where  $\omega = e^{2\pi i/3}$ . Then  $N_{\mathbb{Q}}^E(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$  and  $Tr_{\mathbb{Q}}^E(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a$ .
3. Let  $F = \mathbb{Z}_p(t)$  and  $E$  the splitting field of  $f(x) = x^p - t$  over  $F$ . Then  $E = F(\alpha)$  where  $\alpha^p = t$ . Clearly,  $\alpha$  is p.i. over  $F$  which implies  $E/F$  is p.i. and  $[E : F] = p$ . So  $[E : F]_S = 1$  and  $[E : F]_i = p$ . Then we have only one embedding—the identity. So  $N_F^E(\beta) = \beta^p$  and  $Tr_F^E(\beta) = p\beta = 0$  (since  $char F = p$ .)

**Lemma 2.87.** If  $E/F$  is finite and separable, then  $N_F^E(\alpha), Tr_F^E(\alpha) \in F$  for all  $\alpha \in E$ .

*Proof.* Let  $L$  be the normal closure of  $E/F$ . Then  $L/F$  is finite and Galois. Let  $\sigma_1, \dots, \sigma_r$  be the distinct embeddings of  $E \rightarrow \bar{F}$  which fix  $F$ . Let  $\phi \in G = Gal(L/F)$ . Then  $\phi\sigma_i : E \rightarrow L$  for all  $i$ . Further,  $\phi\sigma_i$  are distinct as  $\phi$  is injective. So  $\{\phi\sigma_1, \dots, \phi\sigma_r\} = \{\sigma_1, \dots, \sigma_r\}$  for all  $\phi \in F$ . Thus  $\phi(N_F^E(\alpha)) = \phi(\sigma_1(\alpha) \cdots \sigma_r(\alpha)) = \phi\sigma_1(\alpha) \cdots \phi\sigma_r(\alpha) = N_F^E(\alpha)$ . Since this holds for all  $\phi \in G$ , we see  $N_F^E(\alpha) \subseteq L_G = F$ . Similarly for  $Tr_F^E(\alpha)$ .  $\square$

**Proposition 2.88.** If  $E/F$  is finite, then  $N_F^E(\alpha), Tr_F^E(\alpha) \in F$  for all  $\alpha \in E$ .

*Proof.* If  $E/F$  is inseparable, then  $[E : F]_i = p^n$ . So  $Tr_F^E(\alpha) = p^n(\cdots) = 0$  as  $char F = p$ . Let  $L$  be the separable closure of  $F$  in  $E$ . Then  $E/L$  is p.i. and  $L/F$  is separable (by HW4#1). Therefore,  $[E : F]_S = [E : L]_S [L : F]_S = [L : F]_S = [L : F]$ . Let  $\sigma_1, \dots, \sigma_r$  be the distinct embeddings of  $L \rightarrow \bar{F}$  fixing  $F$ . Then  $r = [L : F]_S$ . Extend  $\sigma_1, \dots, \sigma_r$  to  $\tau_1, \dots, \tau_r : E \rightarrow \bar{F}$ . Then  $\{\tau_1, \dots, \tau_r\}$  is the set of distinct embeddings of  $E \rightarrow \bar{F}$  fixing  $F$ . Let  $\alpha \in E$ . Then  $p^m = [L(\alpha) : L]_i \leq [E : L]_i = p^n$ . So  $\alpha^{p^n} \in L$  since  $\alpha^{[L(\alpha):L]_i} \in L$ . By the lemma, for all  $\beta \in L$ ,  $N_F^L(\beta) \in F$  as  $L/F$  is separable. Now  $N_F^E(\alpha) = (\tau_1(\alpha) \cdots \tau_r(\alpha))^{[E:F]_i = [E:L]_i} = \tau_1(\alpha^{[E:L]_i}) \cdots \tau_r(\alpha^{[E:L]_i}) = \sigma_1(\alpha^{[E:L]_i}) \cdots \sigma_r(\alpha^{[E:L]_i}) \in F$  by the previous sentence (take  $\beta = \alpha^{[E:L]_i}$ ).  $\square$

**Proposition 2.89.** Let  $E/F$  be a finite extension. Let  $\alpha, \beta \in E$ . Then

1.  $N_F^E(\alpha\beta) = N_F^E(\alpha)N_F^E(\beta)$  and  $Tr_F^E(\alpha + \beta) = Tr_F^E(\alpha) + Tr_F^E(\beta)$ .
2. If  $\alpha \in F$ , then  $N_F^E(\alpha) = \alpha^{[E:F]}$  and  $Tr_F^E(\alpha) = \alpha[E : F]$ .
3. If  $K$  is an intermediate field, then  $N_F^E = N_F^K \circ N_K^E$  and  $Tr_F^E = Tr_F^K \circ Tr_K^E$ .

*Proof.* 1. Follows from the definition as  $\sigma_i$  are homomorphisms.

2. Let  $\alpha \in F$ . Then  $N_F^E(\alpha) = (\sigma_1(\alpha) \cdots \sigma_r(\alpha))^{[E:F]_i} = (\alpha^r)^{[E:F]_i} = \alpha^{[E:F]}$  as  $r = [E : F]_S$ .

3. Let  $\sigma_1, \dots, \sigma_r$  be the distinct embeddings of  $K \rightarrow \overline{F}$  fixing  $F$ . Extend these to  $\tau_1, \dots, \tau_r : E \rightarrow \overline{F}$ . Let  $\phi_1, \dots, \phi_t$  be the distinct embeddings of  $E \rightarrow \overline{F}$  fixing  $K$ . Then  $\{\tau_i \phi_j\}_{i,j}$  are the distinct embeddings of  $E \rightarrow \overline{F}$  fixing  $F$ . Then

$$N_F^K N_K^E(\alpha) = N_F^K \left( \left( \prod_j \phi_j(\alpha) \right)^{[E:K]_i} \right) = \left( \prod_i \tau_i \left( \prod_j \phi_j(\alpha) \right)^{[E:K]_i} \right)^{[K:F]_i} = \left( \prod_{i,j} \tau_i \phi_j(\alpha) \right)^{[E:F]_i} = N_F^E(\alpha).$$

Similarly for the trace. □

### Remarks.

1.  $N_F^E : E^* \rightarrow F^*$  is a group homomorphism and  $Tr_F^E : (E, +) \rightarrow (F, +)$  is an additive group homomorphism. In fact,  $Tr_F^E : E \rightarrow F$  is a linear functional of  $E$  as an  $F$ -VS.

*Proof.* Let  $c \in F, \alpha \in E$ . Then

$$Tr_F^E(c\alpha) = [E : F]_i \left( \sum \sigma_i(c\alpha) \right) = [E : F]_i \left( c \sum \sigma_i(\alpha) \right) = c Tr_F^E(\alpha)$$

as  $\sigma_i$  fixes  $c \in F$ . We have already seen the trace is additive. □

2. If  $\text{char } F = 0$ , then  $Tr_F^E(c) = [E : F]c \neq 0$ . If  $\text{char } F = p$  and  $[E : F]_i > 1$ , we have already seen  $Tr_F^E(\alpha) = [E : F]_i(--) = p^i(--) = 0$ . So  $Tr_F^E$  degenerates. It's a little harder to see, but if  $\text{char } F = p$  and  $[E : F]_i = 1$ , then the trace is non-degenerate. We will prove this.

**Lemma 2.90.** *Let  $E/F$  be a field extension,  $L$  a field such that  $F \subseteq L$ , and  $\sigma_1, \dots, \sigma_n$  the distinct field embeddings of  $E \rightarrow L$  which fix  $F$ . Then  $\sigma_1, \dots, \sigma_n$  are linearly independent over  $F$ .*

*Proof.* We will induct on  $n$ . Let  $n = 1$ . Suppose  $a\sigma_1 = 0$ , where  $\sigma_1 \neq 0$ . Let  $\alpha \in E \setminus \{0\}$ . Then  $\sigma_1(\alpha) \neq 0$ . Since we are in a field,  $a\sigma_1(\alpha) = 0$  implies  $a = 0$ . Let  $n > 1$ . Suppose  $(*) a_1\sigma_1 + \dots + a_n\sigma_n = 0$  for some  $\sigma_1, \dots, \sigma_n$  not all zero. If any of these terms are 0, we are done by induction. So assume  $a_i \neq 0$  for all  $i$ . Let  $\beta \in E$  such that  $\sigma_1(\beta) \neq \sigma_2(\beta)$ . For  $\alpha \in E$ , we see  $a_1\sigma_1(\alpha\beta) + \dots + a_n\sigma_n(\alpha\beta) = 0$  which implies  $a_1\sigma_1(\beta)\sigma_1(\alpha) + \dots + a_n\sigma_n(\beta)\sigma_n(\alpha) = 0$  for all  $\alpha \in E$ . This implies  $a_1\sigma_1(\beta)\sigma_1 + \dots + a_n\sigma_n(\beta)\sigma_n = 0$ . Now divide by  $\sigma_1(\beta)$  and subtract from  $(*)$ . Then  $a_2 \left(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\right) \sigma_2 + \dots + a_n \left(1 - \frac{\sigma_n(\beta)}{\sigma_1(\beta)}\right) \sigma_n = 0$ . By induction, since  $a_i \neq 0$ , we see  $1 = \frac{\sigma_i(\beta)}{\sigma_1(\beta)}$  which implies  $\sigma_1(\beta) = \sigma_i(\beta)$ , contradiction. □

**Corollary 2.91.** *If  $E/F$  is a finite separable extension, then  $Tr_F^E \neq 0$ . So  $Tr_F^E$  is nondegenerate for separable extensions.*

**Theorem 2.92 (Hilbert's Satz 90).** *Let  $E/F$  be a finite cyclic extension. Let  $\langle \sigma \rangle = \text{Gal}(E/F)$  and  $\beta \in E$ . Then  $N_F^E(\beta) = 1$  if and only if  $\beta = \frac{\alpha}{\sigma(\alpha)}$  for some  $\alpha \in E$ .*

*Proof.* Let  $|\sigma| = n$ .

( $\Leftarrow$ ): Then  $N_F^E(\beta) = \prod_0^{n-1} \sigma^i(\beta) = \prod_0^{n-1} \sigma^i \left( \frac{\alpha}{\sigma(\alpha)} \right) = \prod_0^{n-1} \frac{\sigma^i(\alpha)}{\sigma^{i+1}(\alpha)} = 1$  as  $\sigma^n = 1$ .

( $\Rightarrow$ ): Suppose  $N(\beta) = 1$ . By the lemma,  $\{1, \sigma, \dots, \sigma^{n-1}\}$  are linearly independent over  $F$ . Let

$$g = 1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \dots + (\beta\sigma(\beta) \dots \sigma^{n-2}(\beta))\sigma^{n-1} \neq 0.$$

Then there exists  $u \in E$  such that  $g(u) \neq 0$ . Let  $\alpha = g(u)$ . Then

$$\begin{aligned} \beta\sigma(\alpha) &= \beta\sigma(g(u)) \\ &= \beta\sigma(u + \beta\sigma(u) + (\beta\sigma(\beta))\sigma^2(u) + \dots + (\beta\sigma(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}(u)) \\ &= \beta\sigma(u) + \beta\sigma(\beta)\sigma^2(u) + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3(u) + \dots + \underbrace{(\beta\sigma(\beta) \cdots \sigma^{n-1}(\beta))}_{=N(\beta)=1} \underbrace{\sigma^n(u)}_u \\ &= g(u) = \alpha. \end{aligned}$$

Thus  $\beta = \frac{\alpha}{\sigma(\alpha)}$ . □

**Remark.** Let  $F$  be a field,  $n \geq 1$ . Then the roots of  $x^n - 1$  form a finite subgroup  $U_n$  of  $(\overline{F})^*$ . Thus  $U_n$  is a cyclic group, say  $U_n = \langle \omega \rangle$ . If  $\text{char } F \nmid n$ , then  $x^n - 1$  has  $n$  distinct roots. Thus  $|U_n| = n$ . Any generator for  $U_n$  is called a primitive  $n^{\text{th}}$  root of unity.

**Theorem 2.93.** Let  $F$  be a field,  $n \geq 1$  such that  $\text{char } F \nmid n$ . Assume  $F$  contains a primitive  $n^{\text{th}}$  root of unity. Then  $E/F$  is cyclic of  $\text{deg } |n|$  if and only if  $E = F(\alpha)$  where  $\alpha^n \in F$ .

*Proof.* ( $\Rightarrow$ ): Let  $[E : F] = d$ . Then, since  $d|n$ , there is a primitive  $d^{\text{th}}$  root of unity, call it  $\xi \in F$ . Then  $\xi^{-1} \in F$  and  $N_F^E(\xi^{-1}) = (\xi^{-1})^{[E:F]} = 1$ . So there exists  $\alpha \in E$  such that  $\xi^{-1} = \frac{\alpha}{\sigma(\alpha)}$ , where  $\langle \sigma \rangle = \text{Gal}(E/F)$ . Then  $\sigma(\alpha) = \xi\alpha$  which implies  $\sigma^i(\alpha) = \xi^i\alpha$  as  $\xi \in F$  implies  $\sigma$  fixes  $\xi$ . Since  $\sigma(\alpha), \dots, \sigma^d(\alpha)$  are distinct, we see  $[F(\alpha) : F]_S \geq d$ . Since  $[E : F] = d$  this says  $[E : F(\alpha)] = 1$  and thus  $E = F(\alpha)$ . Now notice  $\sigma(\alpha^d) = \sigma(\alpha)^d = (\xi\alpha)^d = \alpha^d$ . So  $\alpha^d \in E_{\langle \sigma \rangle} = F$  and since  $d|n$ ,  $\alpha^n \in F$ .

( $\Leftarrow$ ): Let  $a = \alpha^n \in F$ . Then  $\alpha$  is a root of  $x^n - a \in F[x]$ . Let  $\omega \in F$  be a primitive  $n^{\text{th}}$  root of unity. Then

$$x^n - a = \prod_{i=0}^{n-1} (x - \omega^i \alpha) \in E[x].$$

So  $E$  is the splitting field of  $x^n - a$  which implies  $E/F$  is normal. Since  $\text{char } F \nmid n$ , the  $\omega^i$  are distinct and thus  $x^n - a$  is separable. So  $E/F$  is Galois. Let  $d = [E : F]$ . Let  $f(x) = \text{Irred}(\alpha, F)$ . Then  $f(x) | x^n - a$ . So  $f(x) = \prod_{\ell=0}^{d-1} (x - \omega^{i_\ell} \alpha)$  where  $0 \leq i_\ell \leq n-1$ . Therefore, the  $d$  elements of  $\text{Gal}(E/F)$  are  $\sigma_{i_\ell} : E \rightarrow E$  defined by  $\alpha \mapsto \omega^{i_\ell} \alpha$ . Define  $\phi : \text{Gal}(E/F) \rightarrow \langle \omega \rangle$  by  $\sigma_{i_\ell} \mapsto \omega^{i_\ell}$ . This is a homomorphism as  $\sigma_{i_\ell} \sigma_{i_j}(\alpha) = \omega^{i_j} \sigma_{i_\ell}(\alpha) = \omega^{i_j+i_\ell}(\alpha)$  and so  $\phi(\sigma_{i_\ell} \sigma_{i_j}) = \phi(\sigma_{i_\ell}) \phi(\sigma_{i_j})$ . This is injective as the  $\omega^{i_j}$  are distinct. So  $\text{Gal}(E/F)$  is isomorphic to a subgroup  $H$  of  $\langle \omega \rangle$ . Clearly,  $H$  is cyclic and has order  $d$ . □

## 2.10 Can we find polynomials whose Galois Group is $S_n$ ?

**Theorem 2.94.** Let  $f(x) \in \mathbb{Z}[x]$  be monic of degree  $n$ , with  $n$  distinct roots. Let  $p$  be prime and  $\overline{f}(x) \in \mathbb{Z}_p[x]$  where  $\overline{f}(x)$  is obtained by reducing the coefficients of  $f(x)$  modulo  $p$ . Let  $\alpha_1, \dots, \alpha_n$  be the roots of  $f(x)$  and  $u_1, \dots, u_n$  the roots of  $\overline{f}(x)$  (assume  $u_1, \dots, u_n$  are also distinct.) After possibly reordering  $u_1, \dots, u_n$ , there exists an injective group homomorphism  $\text{Gal}_{\mathbb{Z}_p}(\overline{f}) \rightarrow \text{Gal}_{\mathbb{Q}}(f)$  defined by  $\overline{\sigma}(u_i) = u_j$  if and only if  $\sigma(\alpha_i) = \alpha_j$ .

**Definition 2.95.** A subgroup  $H \leq S_n$  is called **transitive** if for all  $i \neq j \in [n]$ , there exists  $\sigma \in H$  such that  $\sigma(i) = j$ .

**Proposition 2.96.** Suppose  $\overline{f}(x)$  is irreducible in  $\mathbb{Z}_p[x]$ . Then

1.  $\text{Gal}_{\mathbb{Z}_p}(\overline{f})$  is transitive and hence  $\text{Gal}_{\mathbb{Q}}(f)$  is transitive.
2.  $\text{Gal}_{\mathbb{Q}}(f)$  contains an  $n$ -cycle.

*Proof.* 1. As  $\overline{f}(x)$  is irreducible, there exists a map  $\phi : \mathbb{Z}_p(\alpha_i) \rightarrow \mathbb{Z}_p(\alpha_j)$  sending  $\alpha_i \mapsto \alpha_j$ . Extend  $\phi$  to the splitting field. Then  $\phi : \text{Gal}_{\mathbb{Z}_p}(\overline{f}) \rightarrow \text{Gal}_{\mathbb{Z}_p}(\overline{f})$ .

2. As  $\mathbb{Z}_p$  is a finite field,  $Gal_{\mathbb{Z}_p}(\bar{f})$  is cyclic of order  $n$ . Let  $\langle \sigma \rangle = Gal_{\mathbb{Z}_p}(\bar{f})$ . Say  $\sigma = \pi_1 \cdots \pi_k$ , where  $\pi_i$  are disjoint. Of course,  $\langle \sigma \rangle$  is transitive so we must have  $\sigma = \pi_1$ . Thus  $\pi_1$  is an  $n$ -cycle.  $\square$

**Theorem 2.97.** Let  $n \geq 4$  and  $f_1, f_2, f_3 \in \mathbb{Z}[x]$  be monic polynomials of degree  $n$  such that

1.  $\bar{f}_1 \in \mathbb{Z}_2[x]$  is irreducible.
2.  $\bar{f}_2 \in \mathbb{Z}_3[x]$  is such that  $\bar{f}_2 = \bar{g}_1 \bar{h}_1$  where  $\bar{g}_1$  is irreducible of degree  $n-1$ .
3.  $\bar{f}_3 = \bar{g}_2 \bar{h}_2 \in \mathbb{Z}_5[x]$  where  $\bar{g}$  is irreducible of degree 2 and  $\bar{h}$  is a product of irreducible factors of odd degree. [Note: we may need that the roots are distinct here...]

Let  $f = -15f_1 + 10f_2 + 6f_3$ . Then  $f$  is monic of degree  $n$  and  $Gal_{\mathbb{Q}}(f) \cong S_n$ .

*Proof.* The key here is to note that  $S_n$  is generated by an  $n-1$  cycle and a transposition. By 2, we see  $Gal_{\mathbb{Q}}(f)$  contains an  $n-1$  cycle. Now, we will show that the construction in 3 gives us a transposition. Let  $f(x) = g(x)h_1(x) \cdots h_k(x)$ , where  $g, h_i$  are irreducible,  $\deg g = 2$  and  $\deg h_i$  is odd for all  $i$ . Consider  $G = Gal_{\mathbb{Z}_p}(f)$  as a subgroup of  $S_n$ . Let  $\alpha_1, \alpha_2 \in \bar{\mathbb{Z}}_p$  be the roots of  $g(x)$  and  $\alpha_3, \dots, \alpha_n$  the roots of  $h_1, \dots, h_k$ . Let  $F = \bar{\mathbb{Z}}_p(\alpha_1, \alpha_2)$  and  $L = \bar{\mathbb{Z}}_p(\alpha_3, \dots, \alpha_n)$ . Then  $E = FL$  is the splitting field of  $f$ . If we show  $[E : L] = 2$ , then any nontrivial element of  $Gal(E/L)$  corresponds to a transposition (we swap  $\alpha_1$  and  $\alpha_2$  and leave all the other roots fixed). To do this, we need only show  $[L : \bar{\mathbb{Z}}_p]$  is odd. Induct on  $k$ . If  $k = 1$ , since every finite extension of a finite field is cyclic,  $L = \bar{\mathbb{Z}}_p(\alpha)$  where  $\alpha$  is a root of  $h_1$ . So  $[L : \bar{\mathbb{Z}}_p] = \deg h_1$  which is odd. So suppose  $k > 1$ . Let  $T$  be the splitting field for  $h_1, \dots, h_{k-1}$  and  $\alpha$  be a root of  $h_k$ . By the same reasoning as above,  $h_k$  splits in  $\bar{\mathbb{Z}}_p(\alpha)$ . So  $[\bar{\mathbb{Z}}_p(\alpha) : \bar{\mathbb{Z}}_p]$  is odd. By induction,  $[T : \bar{\mathbb{Z}}_p]$  is odd. Note that  $L/T$  and  $\bar{\mathbb{Z}}_p(\alpha)/\bar{\mathbb{Z}}_p$  are Galois (they are both splitting fields for  $h_k$ . Recall  $Gal(L/T) \leq Gal(\bar{\mathbb{Z}}_p(\alpha)/\bar{\mathbb{Z}}_p)$ . So  $[L : T] \mid [\bar{\mathbb{Z}}_p(\alpha) : \bar{\mathbb{Z}}_p]$ . So  $[L : T]$  odd implies  $[L : \bar{\mathbb{Z}}_p]$  is odd. Thus  $2 = [E : L]$  which says  $G$  contains a transposition. Now, by the previous theorem, since there exists an injection  $G \rightarrow Gal_{\mathbb{Q}}(f)$ , we see that  $Gal_{\mathbb{Q}}(f)$  contains a transposition.  $\square$

**Example.** Find a polynomial  $f(x) \in \mathbb{Q}[x]$  such that  $Gal_{\mathbb{Q}}(f) \cong S_4$ .

$$f_1 = x^4 + x + 1$$

$$f_2 = (x^3 + 2x + 2)(x) = x^4 + 2x^2 + 2x$$

$$f_3 = (x^2 + 2)(x)(x + 1) = x^4 + x^3 + 2x^2 + 2x$$

Then  $f = -15f_1 + 10f_2 + 6f_3 = x^4 + 6x^3 + 32x^2 + 17x - 15$  has Galois group  $S_4$  over  $\mathbb{Q}$  by the theorem. Note that  $f$  is irreducible as it is modulo 2.

## 2.11 Solvability by Radicals

Motivation:

- Let  $f(x) = ax^2 + bx + c \in F[x], a \neq 0$ . Then, if  $\text{char } F \neq 2$ , the roots of  $f(x) = \frac{-b \pm \alpha}{2a}$  where  $\alpha$  is a root of  $x^2 - (b^2 - 4ac)$ . Less specifically, we know the roots of  $f(x)$  lie in  $F(\alpha)$  for some  $\alpha \in \bar{F}$  such that  $\alpha^2 \in F$ .
- Let  $f(x) = ax^3 + bx^2 + cx + d \in F[x]$ . Then, if  $\text{char } F \neq 2, 3$ , we can reduce  $f$  to  $f(x) = x^3 + px + q \in F[x]$ . Cardano (1500s) found that the roots of  $f(x)$  lie in  $F(\omega, \delta, y_1, y_2)$  where  $\omega$  is a primitive  $3^{rd}$  root of unity,  $\delta$  is a

root of  $x^2 - (12p^3 - 81q^2)$ ,  $y_1$  is a root of  $x^2 + (\frac{27}{2}q + \frac{3}{2}\delta)$ , and  $y_2$  a root of  $x^3 + (\frac{27}{2}q - \frac{3}{2}\delta)$ .

$$\begin{array}{c} F(\omega, \delta, y_1, y_2) \\ | \\ y_2^2 \in F(\omega, \delta, y_1) \\ | \\ y_1^2 \in F(\omega, \delta) \\ | \\ \delta^2 \in F(\omega) \\ | \\ \omega^3 \in F \end{array}$$

**Definition 2.98.** A finite extension  $E/F$  is called **radical** if  $E = F(\alpha_1, \dots, \alpha_n)$  such that for all  $i = 1, \dots, n$  there exists  $m_i$  such that  $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ . A polynomial  $f(x) \in F[x]$  is **solvable by radicals** over  $F$  if  $f(x)$  splits in some radical extension of  $F$ .

**Theorem 2.99.** Let  $f(x) \in F[x]$  be a separable polynomial. Let  $E$  be the splitting field for  $f(x)$  over  $F$ . Suppose  $\text{char } F \nmid [E : F]$ . If  $\text{Gal}(E/F)$  is solvable, then  $f(x)$  is solvable by radicals over  $F$ .

*Proof.* Let  $n = [E : F]$  and  $\omega$  be a primitive  $n^{\text{th}}$  root of unity. Let  $L = F(\omega)$ . By HW3#1,  $EL/L$  is Galois and  $\text{Gal}(EL/L)$  is isomorphic to a subgroup of  $\text{Gal}(E/F)$ . Since subgroups of solvable groups are solvable,  $\text{Gal}(EL/L)$  is solvable. Now  $EL$  is the splitting field of  $f(x)$  over  $L$ . Note that

$$\begin{aligned} f(x) \text{ is solvable by radicals over } L &\Leftrightarrow EL \text{ lives in a radical extension of } L \\ &\Leftrightarrow EL \text{ lives in a radical extension of } F (\text{since } L = F(\omega) \text{ and } \omega^n \in F) \\ &\Leftrightarrow E \text{ lives in a radical extension of } F \\ &\Leftrightarrow f(x) \text{ is solvable by radicals over } F. \end{aligned}$$

So WLOG, we may assume  $\omega \in F$ . Let  $G = \text{Gal}(E/F)$ . Since  $G$  is solvable, there exists a normal series  $\{1\} = G_t \triangleleft G_{t-1} \triangleleft \dots \triangleleft G_0 = G$  such that  $G_i/G_{i+1} \cong C_{n_i}$  (we know the factor groups are abelian, if not cyclic then just take smaller subgroups so that they are), where  $n_i | n = |G|$ . Let  $E_i$  be the corresponding intermediate field of  $G_i$  with  $E = E_t$  and  $E_0 = F$ . Note that  $E_{i+1}/E_i$  is Galois for all  $i$  and  $\text{Gal}(E_{i+1}/E_i) \cong G_i/G_{i+1} \cong C_{n_i}$  and since  $F$  contains a primitive  $n_i^{\text{th}}$  root of unity (it contains a primitive  $n^{\text{th}}$  root of unity and  $n_i | n$ ). Then by the previous theorem,  $E_{i+1} = E_i(\alpha_i)$  where  $\alpha_i^{n_i} \in E_i$ . Therefore,  $E$  is a radical extension of  $F$  and so  $f$  is solvable by radicals over  $F$ .  $\square$

**Lemma 2.100.** Suppose  $E/F$  is a radical extension. Let  $L$  be the normal closure of  $E/F$ . Then  $L/F$  is radical.

*Proof.* Let  $E = F(u_1, \dots, u_n)$  where  $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$  for  $i = 1, \dots, n$ . Let  $\sigma_1, \dots, \sigma_s$  be the distinct embeddings of  $E \rightarrow \bar{F}$  which fix  $F$ . Then  $L = F(\{\sigma_i(u_j)\}_{i,j})$  (as this gives all of the roots of  $\{\text{Irred}(u_i, F)\}_i$ ). Note that  $\sigma_i(u_j)^{m_j} = \sigma_i(u_j^{m_j}) \in \sigma_i(F(u_1, \dots, u_{j-1})) = F(\sigma_i(u_1), \dots, \sigma_i(u_{j-1}))$ .  $\square$

**Lemma 2.101.** Let  $L/K$  be a Galois, radical extension. Then  $\text{Gal}(L/K)$  is solvable.

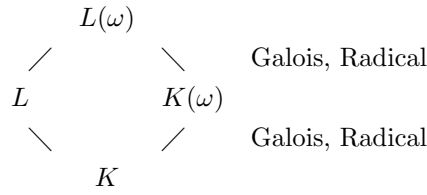
*Proof.* Say  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = L$  where  $K_i = K_{i-1}(u_i)$  and  $u_i^{m_i} \in K_{i-1}$ .

Claim:  $\text{char } K \nmid m_i$  for all  $i$ .

*Proof:* Suppose  $m_i = p^t \ell$  where  $p = \text{char } K$  and  $p \nmid \ell$ . Then  $(u_i^\ell)^{p^t} = u_i^{m_i} \in K_{i-1}$ . This says  $u_i^\ell$  is p.i. over  $K_{i-1}$ . But  $L/K$  Galois says  $L/K_{i-1}$  is separable. Thus we must have  $u_i^\ell \in K_{i-1}$ . So we can simply replace  $m_i$  with  $\ell$  and since  $p \nmid \ell$ , done.



Let  $m = m_1 \cdots m_n$ . Then  $u_i^m \in K_{i-1}$  and  $\text{char } K \nmid m$ . Let  $\omega$  be a primitive  $m^{\text{th}}$  root of unity.



By the picture,  $L(\omega)/K$  is radical and Galois (as  $L(\omega) = LK(\omega)$  where  $L, K(\omega)$  are Galois). Now, since  $L/K$  is normal,

$$\text{Gal}(L/K) \cong \text{Gal}(L(\omega)/K) / \text{Gal}(L(\omega)/L).$$

Since quotient groups of solvable groups are solvable, it is enough to show  $\text{Gal}(L(\omega)/K)$  is solvable. Also

$$\mathbb{Z}_m^* \cong \text{Gal}(K(\omega)/K) \cong \text{Gal}(L(\omega)/K) / \text{Gal}(L(\omega)/K(\omega)).$$

Recall that  $\text{Gal}(L(\omega)/K)$  is solvable if and only if  $\text{Gal}(K(\omega)/K)$  and  $\text{Gal}(L(\omega)/K(\omega))$  are solvable. Since  $\text{Gal}(K(\omega)/K)$  is abelian, it is solvable. So we need only show  $\text{Gal}(L(\omega)/K(\omega))$  is solvable. Note that we have shown that  $\text{Gal}(L/K)$  is solvable if  $\text{Gal}(L(\omega)/K(\omega))$  is solvable. Thus, we may assume  $K$  contains a primitive  $m^{\text{th}}$  root of unity. By the theorem on cyclic extensions,  $K_i/K_{i-1}$  is cyclic. Let  $H_{i-1} = \text{Gal}(L/K_{i-1})$  and  $H_i = \text{Gal}(L/K_i)$ . As  $K_i/K_{i-1}$  is normal,  $H_i \triangleleft H_{i-1}$  and  $H_{i-1}/H_i \cong \text{Gal}(K_i/K_{i-1})$  is cyclic. So  $\{1\} = H_n \triangleleft H_{n-1} \triangleleft \cdots \triangleleft H_0 = \text{Gal}(L/K)$  is a solvable series. Thus  $G$  is solvable.  $\square$

**Theorem 2.102.** *Let  $F$  be a field and  $f(x) \in F[x]$  a separable polynomial. If  $f(x)$  is solvable by radicals over  $F$ , then  $\text{Gal}_F(f(x))$  is solvable.*

*Proof.* Let  $E$  be the splitting field for  $f(x)$  over  $F$ . Then  $E \subseteq L$  for some radical extension  $L$  over  $F$ . WLOG, assume  $L/F$  is normal (can do by the first lemma). Define  $\phi : \text{Aut}(L/F) \rightarrow \text{Gal}(E/F)$  by  $\sigma \mapsto \sigma|_E$ . Since  $E/F$  is normal,  $\phi$  is well-defined. Also  $\phi$  is surjective as  $L/F$  is normal (given  $\rho \in \text{Gal}(E/F)$ , we can extend it to  $L$  and it will be an automorphism of  $L$ ). Hence

$$\text{Gal}(E/F) \cong \text{Aut}(L/F) / \ker \phi.$$

Since quotients of solvable groups are solvable, it is enough to prove  $\text{Aut}(L/F)$  is solvable. Note  $|\text{Aut}(L/F)| = [L : F]_S \leq [L : F] < \infty$  (as radical extensions are by definition finite). Let  $G = \text{Aut}(L/F)$  and  $K = E_G$ . By Artin's Theorem,  $L/K$  is Galois and  $G = \text{Gal}(L/K)$ . Note that  $F \subseteq K$  and  $L/K$  is radical. Thus by the second lemma, we're done.  $\square$

**Definition 2.103.** *Let  $F$  be a field and  $t_1, \dots, t_n$  indeterminants over  $F$ . Then the **general equation of degree  $n$**  over  $F$  is  $f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} + \dots + (-1)^nt_n \in F(t_1, \dots, t_n)[x]$ .*

**Theorem 2.104.** *Let  $L = F(t_1, \dots, t_n)$  and  $f(x)$  as above. Then  $\text{Gal}_L(f) \cong S_n$ .*

*Proof.* Let  $E$  be the splitting field for  $f(x)$  over  $L$ . Say  $f(x) = \prod_{i=1}^n (x - y_i) \in E[x]$ . Then  $E = L(y_1, \dots, y_n) = F(y_1, \dots, y_n)$ . Thus  $t_i = s_i(y_1, \dots, y_n)$ , where  $s_i \in L[x_1, \dots, x_n]$  is the  $i^{\text{th}}$  elementary symmetric function. Define a field homomorphism  $\sigma : L \rightarrow F(s_1, \dots, s_n) \subseteq F(x_1, \dots, x_n)$  by  $t_i \mapsto s_i$  and fixes  $F$ . Then  $\sigma$  is clearly surjective.

Claim:  $\sigma$  is an isomorphism

*Proof:* Define  $\tau : F(x_1, \dots, x_n) \rightarrow E = F(y_1, \dots, y_n)$  by  $x_i \mapsto y_i$ . Then  $\tau(s_i) = t_i$  as  $t_i = s_i(y_1, \dots, y_n)$  and  $\tau\sigma\left(\frac{p(t_1, \dots, t_n)}{q(t_1, \dots, t_n)}\right) = \tau\left(\frac{p(s_1, \dots, s_n)}{q(s_1, \dots, s_n)}\right) = \frac{p(t_1, \dots, t_n)}{q(t_1, \dots, t_n)}$ . So  $\sigma$  is injective and thus an isomorphism.

Note that  $f^\sigma(x) = x^n - s_1x^{n-1} + \dots + (-1)^n s_n$  and has splitting field  $F(x_1, \dots, x_n)$  (where the  $x_i$ 's are such that  $f^\sigma(x) = \prod_{i=1}^n (x - x_i)$ —from our definition of the elementary symmetric functions).

$$\begin{array}{ccc} & F(y_1, \dots, y_n) & \xrightarrow{\phi} & F(x_1, \dots, x_n) \\ \text{splitting field of } f(x) \rightarrow & | & & | \leftarrow \text{splitting field of } f^\sigma(x) \\ & F(t_1, \dots, t_n) & \xrightarrow{\cong} & F(s_1, \dots, s_n) \end{array}$$

By the theorem on the uniqueness of splitting fields, there exists an isomorphism  $\phi : F(y_1, \dots, y_n) \rightarrow F(x_1, \dots, x_n)$  where  $\phi|_L = \sigma$ . Hence  $\text{Gal}_L(f) \cong \text{Gal}_{F(s_1, \dots, s_n)}(f^\sigma) \cong S_n$ , as we saw earlier with the symmetric functions, using Artin's Theorem.  $\square$

Recall:  $S_n$  is solvable if and only if  $n \leq 4$ .

**Corollary 2.105.** *If  $n \leq 4$  and  $\text{char } F \nmid |S_n| = n!$ , then the general equation of degree  $n$  over  $F$  is solvable by radicals.*

**Corollary 2.106 (Abel's Theorem).** *If  $n \geq 5$ , then the general equation of degree  $n$  over  $F$  is not solvable by radicals.*

**Fact.** If  $p$  is prime, then  $S_p$  is generated by any transposition and any  $p$ -cycle.

**Lemma 2.107.** *Let  $f(x) \in \mathbb{Q}[x]$  be irreducible of prime degree  $p$  and suppose  $f$  has exactly  $p - 2$  real roots. Then  $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$ .*

*Proof.* Let  $E = \mathbb{Q}(\alpha_1, \dots, \alpha_p)$  where  $\alpha_1, \dots, \alpha_p$  are roots of  $f(x)$  with  $\alpha_1, \alpha_2 \notin \mathbb{R}$ . Let  $G = \text{Gal}(E/\mathbb{Q}) \subseteq S_p$ . Since  $f(x)$  is irreducible,  $p \mid |G|$ . Since  $p$  is prime, the only elements of  $S_p$  of order  $p$  are the  $p$ -cycles. Thus  $G$  contains a  $p$ -cycle. Let  $\sigma$  be complex conjugation restricted to  $E$ . Then  $\sigma$  transposes  $\alpha_1$  and  $\alpha_2$  and fixes  $\alpha_3, \dots, \alpha_n$ . So  $\sigma \in G$  is a transposition. Done by fact.  $\square$

**Example.** Let  $f(x) = x^5 - 2x^3 - 8x - 2 \in \mathbb{Q}[x]$ . This is irreducible by Eisenstein. Using Calculus to find the critical numbers and looking at the end behavior, we see  $f(x)$  crosses the  $x$ -axis 3 times. Thus  $f(x)$  has 3 real roots. By the lemma,  $\text{Gal}_{\mathbb{Q}}(f) \cong S_5$ . Thus  $f$  is not solvable by radicals.

## 2.12 Transcendental Extension

**Definition 2.108.** *Let  $E/F$  be a field extension and  $S \subseteq E$ . Then  $S$  is **algebraically dependent** over  $F$  if there exists  $s_1, \dots, s_n \in S$  and  $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n] \setminus \{0\}$  such that  $f(s_1, \dots, s_n) = 0$ . Otherwise, we say  $S$  is **algebraically independent** over  $F$ .*

**Remarks.**

1.  $\emptyset$  is algebraically independent over any field.
2.  $\{u\}$  is algebraically independent if and only if  $u$  is transcendental over  $F$ .
3.  $\{s_1, \dots, s_n\}$  is algebraically independent over  $F$  if and only if  $F[s_1, \dots, s_n] \cong F[x_1, \dots, x_n]$ , where  $x_1, \dots, x_n$  are variables.

**Lemma 2.109.** *Let  $E/F$  be a field extension and  $S \subseteq E$  an algebraically independent set over  $F$ . Let  $u \in E$ . Then  $S \cup \{u\}$  is algebraically independent if and only if  $u$  is transcendental over  $F(S)$ .*

*Proof.* ( $\Leftarrow$ ) It is enough to show  $\{s_1, \dots, s_n, u\}$  is algebraically independent for  $s_1, \dots, s_n \in S$ . Suppose  $f(x_1, \dots, x_{n+1}) \in F[x_1, \dots, x_{n+1}]$  and  $f(s_1, \dots, s_n, u) = 0$ . Let  $g(x_{n+1}) = f(s_1, \dots, s_n, x_{n+1}) \in F(S)[x_{n+1}]$ . Note  $g(u) = 0$ . Since  $u$  is transcendental over  $F(S)$ , we must have  $g(x_{n+1}) = 0$ . Write

$$f(x_1, \dots, x_{n+1}) = h_r(x_1, \dots, x_n)x_{n+1}^r + \dots + h_0(x_1, \dots, x_n).$$

Then  $0 = g(x_{n+1})$  says  $h_i(s_1, \dots, s_n) = 0$  for all  $i$ . Since  $\{s_1, \dots, s_n\}$  are algebraically independent, we must have  $h_i(x_1, \dots, x_n) = 0$  for all  $i$ . Thus  $f(x_1, \dots, x_{n+1}) = 0$ .

( $\Rightarrow$ ) Suppose  $u$  is algebraic over  $F(S)$ . Then  $u$  is algebraic over a finite subset of  $S$ . So WLOG,  $S$  is finite. Then there exists  $f(x) \in F(S)[x] \setminus \{0\}$  such that  $f(u) = 0$ . Say

$$f(x) = \frac{g_r(s_1, \dots, s_n)}{h_r(s_1, \dots, s_n)}x^r + \dots + \frac{g_0(s_1, \dots, s_n)}{h_0(s_1, \dots, s_n)},$$

where  $g_i(x_1, \dots, x_n), h_i(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ . Multiply  $f$  by  $h_0 \cdots h_r$  to clear denominators and still get a polynomial that  $u$  satisfies. So WLOG,  $h_i = 1$ . Let  $\ell(x_1, \dots, x_n, x) = g_r(x_1, \dots, x_n)x^r + \dots + g_0(x_1, \dots, x_n)$ . Note that  $\ell(s_1, \dots, s_n, u) = 0$ . Since  $S \cup \{u\}$  is algebraically independent,  $\ell(x_1, \dots, x_n, x) = 0$ , a contradiction as  $f(x) \neq 0$ . Thus  $u$  is transcendental over  $F(S)$ .  $\square$

**Definition 2.110.** Let  $E/F$  be a field extension. A set  $S \subseteq E$  is called a **transcendence base** for  $E/F$  if  $S$  is algebraically independent over  $F$  and  $E/F(S)$  is algebraic.

**Theorem 2.111.** Let  $E/F$  be a field extension and  $L \subseteq E$  an algebraically independent set over  $F$ . Then there exists a transcendence base  $S$  for  $E/F$  such that  $L \subseteq S$ .

*Proof.* Let  $\Gamma = \{T \mid L \subseteq T \subseteq E \text{ and } T \text{ is algebraically independent over } F\}$ . Note  $L \in \Gamma$  so  $\Gamma \neq \emptyset$ . Let  $\mathcal{C}$  be any totally ordered subset of  $\Gamma$ . Then  $T_0 = \cup_{t \in \mathcal{C}} T \in \Gamma$  is an upper bound. By Zorn's Lemma, there exists a maximal set  $S \in \Gamma$ . Then  $S$  is algebraically independent by definition of  $\Gamma$  and  $E/F(S)$  is algebraic by the lemma and maximality of  $S$ .  $\square$

**Example.** Let  $X, Y$  be indeterminants over  $F$ . Then  $\{X, Y\}$  is a transcendence base for  $F(X, Y)/F$ . Also  $\{X^2, Y^2\}$  is a transcendence base.

**Theorem 2.112.** Let  $E/F$  be a field extension. Then any two transcendence bases for  $E/F$  have the same cardinality.

*Proof.* We'll prove this in the case that  $E/F$  has a finite transcendence base  $S = \{s_1, \dots, s_n\}$ . Let  $T$  be a transcendence base for  $E/F$ .

Claim: There exists  $t_1 \in T$  such that  $\{t_1, s_2, \dots, s_n\}$  is algebraically independent over  $E/F$ .

Proof: Suppose not. Therefore  $F(T)$  is algebraic over  $F(s_2, \dots, s_n)$ . But  $E/F(T)$  is algebraic, which implies  $E/F(s_2, \dots, s_n)$  is, so  $s_1 \in E$  is algebraic over  $F(s_2, \dots, s_n)$ , a contradiction.

Claim: The set  $\{t_1, s_2, \dots, s_n\}$  is a transcendence base of  $E/F$ .

Proof: Suppose  $s_1$  is transcendental over  $F(\{t_1, s_2, \dots, s_n\})$ . Then  $\{t_1, s_1, \dots, s_n\}$  is algebraically independent, but  $t_1$  is algebraic over  $F(\{s_1, \dots, s_n\})$ , a contradiction. Thus  $s_1$  is algebraic over  $F(\{t_1, s_2, \dots, s_n\})$  which implies  $F(\{t_1, s_1, \dots, s_n\})$  is algebraic over  $F(\{t_1, s_2, \dots, s_n\})$ . But  $E$  is algebraic over  $F(\{t_1, s_1, \dots, s_n\})$  (as it is over  $F(\{s_1, \dots, s_n\})$ ) and thus  $E$  is algebraic over  $F(\{t_1, s_2, \dots, s_n\})$ .

Repeating this process, replace  $s_2, \dots, s_n$  by  $t_2, \dots, t_n \in T$  to obtain a transcendence base  $\{t_1, \dots, t_n\}$  for  $E/F$ . Since  $T$  is algebraically independent,  $T = \{t_1, \dots, t_n\}$ .  $\square$

**Definition 2.113.** The **transcendence degree** of  $E/F$  is the cardinality of any transcendence base for  $E/F$ .

**Note.** The transcendence degree of  $E/F$  is 0 if and only if  $E/F$  is algebraic.

**Theorem 2.114.** Suppose  $K \subseteq F \subseteq E$  are fields. The  $\text{tr deg } E/K = \text{tr deg } E/F + \text{tr deg } F/K$ .

*Proof.* Let  $S, T$  be transcendence bases for  $E/F$  and  $F/K$  respectively. Since  $T \subseteq F$  and  $S \subseteq E \setminus F$ , we see  $S \cap T = \emptyset$ . Then it is enough to show  $S \cup T$  is a transcendence base for  $E/K$ .

Claim 1:  $E$  is algebraic over  $K(S \cup T)$ .

Proof: We know that  $F$  is algebraic over  $K(T)$ . So  $F(S)$  is algebraic over  $K(T)(S) = K(S \cup T)$ . As  $E$  is algebraic over  $F(S)$ ,  $E$  is algebraic over  $K(S \cup T)$ .

Claim 2:  $S \cup T$  is algebraically independent over  $K$ .

Proof: Let  $f(x_1, \dots, x_m, y_1, \dots, y_n) \in K[x_1, \dots, x_m, y_1, \dots, y_n]$  such that  $f(s_1, \dots, s_m, t_1, \dots, t_n) = 0$ . We want to show  $f = 0$ . Say  $f = \sum g_i(y_1, \dots, y_n)h_i(x_1, \dots, x_m)$  where  $g_i \in K[y_1, \dots, y_n]$  and the  $h_i$  are distinct monomials in the  $x$ 's. Let  $\ell(x_1, \dots, x_m) = f(x_1, \dots, x_m, t_1, \dots, t_n) \in K(T)[x] \subseteq F[x_1, \dots, x_m]$ . That  $\ell(s_1, \dots, s_m) = 0$ . As  $S$  is algebraically independence over  $F$ , we know  $\ell = 0$ . So  $f(x_1, \dots, x_m, t_1, \dots, t_n) = 0$ . Since the  $h_i(x_1, \dots, x_m)$  are linearly independent over  $F[x]$  (as they are distinct monomials), we must have that  $g_i(t_1, \dots, t_n) = 0$  for all  $i$ . Since  $T$  is algebraically independent over  $K$ ,  $g_i(y_1, \dots, y_n) = 0$ . Thus  $f = 0$ . □

### 3 Rings and Modules

We will take all rings to have identity, but not necessarily be commutative.

**Definition 3.1.** Let  $G$  be a group,  $k$  a field. Let  $B$  be a  $k$ -vector space with basis  $\{e_g\}_{g \in G}$ . Then  $V$  is a **group ring** with elements of the form  $\sum_{g \in G} c_g e_g$  where all but finitely many terms are zero. Define multiplication in  $V$  by  $(\sum c_g e_g)(\sum d_{g'} e_{g'}) = \sum c_g d_{g'} e_{gg'}$ .

**Remarks.** Under this definition,  $V$  is a ring with identity element  $e_1$ . For convenience, we will write  $g$  for  $e_g$  and  $K[G]$  for the ring  $V$ . Note that  $K[G]$  is commutative if and only if  $G$  is abelian.

**Example.** Let  $G = C_n = \langle g \rangle$  and  $K$  be any field. Then  $K[C_n] = \{\sum_{i=0}^{n-1} c_i g^i \mid c_i \in K\}$ . Define a ring homomorphism  $K[x] \rightarrow K[C_n]$  such that  $k \mapsto k$  and  $x \mapsto g$ . Clearly, this is surjective. As  $g^n = 1$ , we see  $x^n - 1 \in \ker \phi$ . So we have an induced map  $K[x]/(x^n - 1) \rightarrow K[C_n]$ . Since both of these have dimension  $n$ , we see that they are isomorphic.

**Definition 3.2.** A **division ring** is a ring in which every nonzero element is a unit.

**Examples.**

1. Any field is a division ring.
2. Consider the ring homomorphism  $\mathbb{R} \rightarrow M_2(\mathbb{C})$  defined by  $r \mapsto rI$ . In this way, we can consider  $\mathbb{R}$  as a subring of  $M_2(\mathbb{C})$ . Let  $\mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ ,  $\mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ ,  $\mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ . Then  $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$  are linearly independent over  $\mathbb{R}$ . Let  $H = \mathbb{R} \cdot 1 + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} \subseteq M_2(\mathbb{C})$ . Then  $H$  has dimension 4. Note that  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ,  $\mathbf{ij} = \mathbf{j} = -\mathbf{ji}$ ,  $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ ,  $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$ . Thus  $H$  is closed under multiplication and has identity. Since  $H$  is a vector space, it's an additive group. Thus  $H$  is a noncommutative subring of  $M_2(\mathbb{C})$ , called the ring of (real) quaternions. Let  $\alpha = r_0 + r_1\mathbf{i} + r_2\mathbf{j} + r_3\mathbf{k}$  and  $\bar{\alpha} = r_0 - r_1\mathbf{i} - r_2\mathbf{j} - r_3\mathbf{k}$ . One can check  $\alpha\bar{\alpha} = \bar{\alpha}\alpha = r_0^2 + r_1^2 + r_2^2 + r_3^2 =: |\alpha|^2$ . Note  $\alpha = 0$  if and only if  $|\alpha| = 0$ . So if  $\alpha \neq 0$ ,  $\alpha^{-1} = \frac{\bar{\alpha}}{|\alpha|^2}$ . Thus  $H$  is a division ring (but not a field!).

**Definition 3.3.** Let  $R$  be a ring. A **left (respectively, right)  $R$ -module** is an abelian group  $(M, +)$  together with a map  $R \times M \rightarrow M$  defined by  $(r, m) \mapsto rm$  such that

1.  $r(m + n) = rm + rn$
2.  $(r + s)m = rm + sm$
3.  $r(sm) = (rs)m$
4.  $1m = m$

**Notes.** Not everyone requires (4). In this case,  $R$  is called a **unital module**. Also, we will assume  $1 \mapsto 1$  in a ring homomorphism.

**Definition 3.4.** Let  $f : R \rightarrow S$  be a ring homomorphism such that  $f(R) \subseteq Z(S)$ . Then  $S$  is called an  $R$ -**algebra**.

**Note.** The  $\ker f$  is a two-sided ideal. Thus  $\bar{f} : R/\ker f \rightarrow S$  is injective. Thus  $R/\ker f$  is commutative and  $R/\ker f \subseteq Z(S)$ .

**Examples.** Assume  $R$  is a commutative ring.

1. Let  $R[x_1, \dots, x_n]$  be the polynomial ring in  $x_1, \dots, x_n$  and  $I$  an ideal of  $R[x_1, \dots, x_n]$ . Then  $f : R \rightarrow R[x_1, \dots, x_n]/I$  defined by  $r \mapsto \bar{r} = r + I$  is a ring homomorphism. Thus  $R[x_1, \dots, x_n]/I$  is an  $R$ -algebra.
2. Define  $f : R \rightarrow M_n(R)$  by  $r \mapsto rI$ . This is a ring homomorphism, so  $M_n(R)$  is an  $R$ -algebra.
3. Let  $G$  be a group. Define  $f : R \rightarrow R[G]$  by  $r \mapsto re_1$ . This is a ring homomorphism, so  $R[G]$  is an  $R$ -algebra.
4. Let  $C(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous}\}$ . Then  $f : \mathbb{R} \rightarrow C(\mathbb{R})$  defined by  $r \mapsto f_r(x) = r$  is a ring homomorphism. Thus  $C(\mathbb{R})$  is an  $\mathbb{R}$ -algebra.

**Definition 3.5.** Let  $S$  be a ring,  $A \subseteq Z(S)$  a subring,  $T$  a subset of  $S$ . Say  $S$  is **generated** over  $A$  by  $T$  if every element of  $S$  is a finite sum of elements of the form  $at_1^{n_1} \cdots t_k^{n_k}$ , where  $a \in A, t_i \in T, n_i \geq 0$ . We write  $S = A[T]$ . If  $S = A[T]$  for some finite subset  $T$  of  $S$ , then  $S$  is **finitely generated over  $A$  as a ring**. If  $f : R \rightarrow S$  is a ring homomorphism with  $f(R) \subseteq Z(S)$ , then  $S$  is a **finitely generated  $R$ -algebra** if  $S$  is finitely generated over  $f(R)$  as a ring.

**Notes.**

- If  $E/K$  is a finitely generated field extension and  $F$  is an intermediate field, then  $F/K$  is a finitely generated field extension (HW).
- This is NOT true for algebras. For example,  $K[x, y]$  is finitely generated as a  $K$ -algebra, but  $K[x, xy, xy^2, \dots]$  is not finitely generated as a  $K$ -algebra.

**Examples.** Let  $R$  be a commutative ring.

1.  $S = R[x_1, \dots, x_n]/I$  is a finitely generated  $R$ -algebra where  $T = \{\bar{x}_1, \dots, \bar{x}_n\}$ . Using the above notation, we can say  $S = R[\bar{x}_1, \dots, \bar{x}_n]$ .  
**Claim.** Let  $S$  be a finitely generated  $A$ -algebra which is commutative. Say  $S = A[T]$  where  $T = \{t_1, \dots, t_n\}$ . Define  $\phi : A[x_1, \dots, x_n] \rightarrow S$  by  $f(x_1, \dots, x_n) \mapsto f(t_1, \dots, t_n)$ . Because the  $t_i$ 's commute,  $\phi$  is an onto ring homomorphism. So  $S \cong A[x_1, \dots, x_n]/I$ .
2.  $S = M_n(R)$ . Let  $E_{ij}$  be the  $n \times n$  matrix with a 1 in the  $i, j^{\text{th}}$  entry and zeros everywhere else. Then for  $A = (a_{ij}) \in S$ , we see  $A = \sum a_{ij} E_{ij}$ . Thus  $S$  is generated by  $E_{ij}$ . So  $S = R[\{E_{ij}\}]$ .
3.  $R[G]$  is a finitely generated  $R$ -algebra if and only if  $G$  is a finitely generated group. For one direction, we see if  $G = \langle g_1, \dots, g_n \rangle$ , then  $R[G] = R[g_1, \dots, g_n]$ .
4.  $C(\mathbb{R})$  is not a finitely generated  $R$ -algebra.

Let  $A$  be a ring. By an  $A$ -module, we mean a left  $A$ -module, unless when explicitly stated otherwise.

**Remark.** Let  $f : R \rightarrow S$  be a ring homomorphism. Any  $S$ -module  $M$  is an  $R$ -module via the action  $r \cdot m := f(r)m$ . In particular,  $S$  is an  $R$ -module.

**Definition 3.6.** Let  $M$  be an  $R$ -module and  $T \subseteq M$ . Say  $T$  **generates**  $M$  as an  $R$ -module if every element of  $M$  can be expressed as  $\sum_1^n r_i t_i$ , for  $t_i \in T, r_i \in R$ , that is,  $M = RT = R$ -submodule of  $M$  generated by  $T$ . We say  $M$  is **finitely generated as an  $R$ -module** if  $M = RT$  for some finite subset  $T$  of  $M$ . In practice, if  $T = \{t_1, \dots, t_n\}$ , we will write  $M = Rt_1 + \dots + Rt_n$ . Sometimes, this is stated as “ $M$  is a finite  $R$ -module” even though  $M$  is not necessarily finite.

**Examples.** Let  $R$  be a commutative ring.

1.  $R[x_1, \dots, x_n]/I$  need not be a finitely generated  $R$ -module. For example  $k[x, y]/(xy)$  is not a finitely generated  $k$ -module.
2.  $M_n(R)$  is a finitely generated  $R$ -module ( $M_n(R) = \sum RE_{ij}$ ).
3.  $R[G]$  is a finitely generated  $R$ -module if and only if  $|G| < \infty$ .

### 3.1 Free Modules and Bases

**Definition 3.7.** Let  $M$  be an  $A$ -module,  $T \subseteq M$ . Say  $T$  is **linearly independent** over  $A$  if whenever  $\sum_1^n a_i t_i = 0$  where  $t_1, \dots, t_n \in T$  are distinct, then  $a_i = 0$  for all  $i$ .

**Example.** Let  $R = \mathbb{Z}_6$  and  $I = (\bar{2})$ . Then  $\bar{2}$  is a minimal generating set of  $I$  but  $\bar{3} \cdot \bar{2} = \bar{0}$ . So  $\{\bar{2}\}$  is not linearly independent over  $R$ .

**Definition 3.8.** A **basis**  $T$  for an  $A$ -module  $M$  is a generating set for  $M$  which is linearly independent over  $A$ .

**Proposition 3.9.** Let  $M$  be an  $A$ -module,  $S \subseteq M$ . TFAE

1.  $S$  is an  $A$ -basis for  $M$
2. For any  $A$ -module  $N$  and any set map  $j : S \rightarrow N$ , there exists a unique  $A$ -module homomorphism  $\tilde{j} : M \rightarrow N$  such that the following diagram commutes

$$\begin{array}{ccc} S & \longrightarrow & M \\ j \downarrow & \nearrow \exists! \tilde{j} & \\ N & & \end{array}$$

*Proof.* (1)  $\Rightarrow$  (2) Given  $j : S \rightarrow N$ , define  $\tilde{j} : M \rightarrow N$  by  $\tilde{j} : (\sum_{s \in S} a_s s) = \sum_{s \in S} a_s j(s)$  (where all but finitely many  $a_s$  are 0). Since  $S$  is a basis for  $M$ , every element of  $M$  can be written uniquely in the form  $\sum_{s \in S} a_s s$ . Thus  $\tilde{j}$  is a well-defined homomorphism. Also,  $\tilde{j}$  is clearly unique.

(2)  $\Rightarrow$  (1)  $S$  is linearly independent: Suppose  $\sum_{s \in S} a_s s = 0$ . For each  $t \in S$ , define  $j_t : S \rightarrow A$  by  $t \mapsto 1$  and  $s \mapsto 0$  for  $s \neq t$ . Then  $0 = \tilde{j}_t(0) = \tilde{j}_t(\sum a_s s) = \sum a_s j_t(s) = a_t$ . Since  $t$  was arbitrary, done.

$S$  generates  $M$ : Let  $M'$  be the  $A$ -submodule of  $M$  generated by  $S$ , that is  $M' = \{\sum_{s \in S} a_s s \mid a_s \in A, s \in S\}$ . Define  $j : S \rightarrow M/M'$  by  $s \mapsto 0 = s + M'$ . Consider  $\tilde{j} : M \rightarrow M/M'$  defined by  $m \mapsto m + M'$ . By the uniqueness of  $\tilde{j}$ , since the 0 map also make the diagram commute,  $\tilde{j} = 0$ , which implies  $m + M' = 0$  for all  $m \in M$ . Thus  $M = M'$ .

**Definition 3.10.** An  $A$ -module is called **free** if  $M$  has a basis.

**Remarks.**

1.  $M$  is a free  $A$ -module if and only if  $M \cong \otimes_{i \in I} A$ .

*Proof.* ( $\Leftarrow$ ): For all  $j \in I$ , let  $e_j \in \otimes_{i \in I} A$  where  $(e_j)_i = 0$  if  $i \neq j$  and 1 if  $i = j$ . Then  $\{e_j\}_{j \in I}$  forms a basis.

( $\Rightarrow$ ): Let  $S$  be a basis for  $M$ . Define  $\phi : \otimes_{s \in S} A \rightarrow M$  by  $e_s \mapsto s$ . Then  $\sum a_s e_s \mapsto \sum a_s s$ . Since  $S$  generates  $M$ , its onto. Since  $S$  is linearly independent, its injective. □

2. Every  $A$ -module is the homomorphic image of a free  $A$ -module.

*Proof.* Let  $M$  be an  $A$ -module. Define  $\otimes_{m \in M} A \rightarrow M$  by  $e_m \mapsto m$ . Then extend it to  $\sum a_m e_m \mapsto \sum a_m m$ . Then  $\phi$  is a surjective homomorphism. □

**Examples.**

1. The 0–module is always free.
2. Let  $R$  be a commutative ring,  $I \neq (0)$  an ideal. TFAE
  - (a)  $I$  is free
  - (b)  $I \cong R$
  - (c)  $I = Ra = (a)$  for some non-zero-divisor  $a \in R$ .

*Proof.* (a) $\Rightarrow$ (b): Let  $S$  be a basis for  $I$ . Suppose  $|S| > 1$ . Let  $s \neq t \in S$ . Since  $R$  is commutative,  $st + (-t)s = 0$ . Since  $s$  and  $t$  are linearly independent, the coefficients are 0. Thus  $s = t = 0$ . So  $|S| = 1$  which implies  $I \cong R$ .  $\square$

3. Let  $R = \mathbb{Z}[x]$  and  $I = (2, x)$ . Then  $I$  can be shown to be not principal, thus  $I$  is not free.
4. Let  $R = \mathbb{Z}[\sqrt{-5}]$  and  $I = (2, 1 + \sqrt{-5})$ . Then  $I$  is not principal, so  $I$  is not free. However,  $I \otimes J \cong R^2$  for some ideal  $J$ .
5. Let  $R$  be commutative. Then  $M_n(R)$  is a free  $R$ –module with basis  $\{E_{ij}\}$ .
6.  $R[G]$  is a free  $R$ –module with basis  $\{g\}_{g \in G}$ .

**Remark.** Let  $A$  be a ring,  $I$  a two-sided ideal. Let  $M$  be an  $A$ –module. Then  $M/IM$  is an  $A/I$ –module via  $(a + I)(m + IM) = am + IM$ .

**Lemma 3.11.** Let  $M$  be an  $A$ –module and  $I$  a two-sided ideal. If  $S$  is a basis for  $M$ , then  $\bar{S} = \{s + IM \mid s \in S\}$  is an  $A/I$  basis for  $M/IM$ .

*Proof.* Let  $\bar{m} \in M/IM$ . Then if  $\bar{m} = m + IM$ , we know  $m = \sum a_s s$ , which says  $\bar{m} = \sum \bar{a}_s \bar{s}$ . So  $\bar{S}$  generates  $M/IM$ . Suppose  $\sum \bar{a}_s \bar{s} = \bar{0}$ . Then  $\sum a_s s \in IM$  which implies  $\sum a_s s = \sum_{j=1}^n i_j m_j$  for  $i_j \in I, m_j \in M$ . Now  $m_j = \sum_{s \in S} b_{js} s$ . So,  $\sum a_s s = \sum_{j,s} i_j b_{js} s = \sum_s (\sum_j i_j b_{js}) s$  which implies  $a_s = \sum i_j b_{js} \in I$ . Thus  $\bar{a}_s = 0$ .  $\square$

**Lemma 3.12.** Let  $R$  be a division ring. Any  $R$ –module  $M$  has a basis and any two bases for  $M$  have the same cardinality.

**Proposition 3.13.** Let  $R$  be a commutative ring and  $M$  an  $R$ –module. Then any two bases have the same cardinality.

*Proof.* Let  $m$  be a maximal ideal of  $R$  (it exists by Zorn’s Lemma). Then  $R/m$  is a field. Let  $S_1, S_2$  be two  $R$ –bases for  $M$ . By the above two lemmas,  $\bar{S}_1, \bar{S}_2$  are  $R/m$ –bases for  $M/mM$  and  $\bar{S}_1, \bar{S}_2$  have the same cardinality (as  $R/m$  is a field).

Claim: For any basis  $S$  of  $M$ ,  $S$  and  $\bar{S}$  have the same cardinality.

*Proof:* We know the map  $S \rightarrow \bar{S}$  defined by  $s \mapsto \bar{s}$  is onto. Suppose  $\bar{s} = \bar{t}$  for  $s, t \in S$ . Then  $s - t \in mM$ . So  $s - t = \sum i_s s$  for  $i_s \in m$  by the proof of the first lemma. Comparing coefficients, this says  $1 \in m$ , a contradiction as  $m \neq R$ .

Thus  $S_1$  and  $S_2$  have the same cardinality.  $\square$

**Definition 3.14.** If  $R$  is commutative and  $F$  is a free  $R$ –module, then the **rank** of  $F$  is defined to be the cardinality of any basis for  $F$ . (Note: When  $R$  is a field, this is just the dimension).

**Definition 3.15.** Let  $M$  be an  $A$ –module. Define  $End_A M = \{f : M \rightarrow M \mid f \text{ is an } A\text{–module homomorphism}\}$ .

**Remarks.**

1.  $End_A M$  is a ring under addition and composition. We call it the **endomorphism ring** of  $M$ .

2. If  $A$  is commutative, then  $\phi : A \rightarrow \text{End}_A(M)$  defined by  $a \mapsto aI$  is a ring homomorphism.

[Note: If  $A$  is not commutative, then for  $r \notin Z(A)$ , we have  $rI \notin \text{End}_A(M)$  as  $f(r'm) \neq r'f(m)$ .]

Thus if  $A$  is commutative, then  $\text{End}_A(M)$  is an  $A$ -algebra, and in particular an  $A$ -module.

3. If  $A$  is commutative and  $F$  is a free  $A$ -module of rank  $n$ , then  $\text{End}_A(F) \cong M_n(A)$  (as a homomorphism is determined by where it sends the basis elements).

**Example.** Let  $A$  be a commutative ring,  $F$  a free  $A$ -module with basis  $\mathbb{N}$ , that is  $F \cong \bigotimes_{i=1}^{\infty} A$ . Let  $\{e_i | i = 0, 1, \dots\}$  be a basis for  $F$  and  $R = \text{End}_A(F)$ . Then  $R \cong R^n$  for all  $n \geq 1$ .

*Proof.* Define  $f_1, f_2 : F \rightarrow F$  by  $f_1(e_{2i}) = e_i, f_1(e_{2i+1}) = 0$  and  $f_2(e_{2i}) = 0, f_2(e_{2i+1}) = e_i$  for  $i \geq 0$ . Then  $f_1, f_2 \in \text{End}_A(F) = R$ .

Claim:  $\{f_1, f_2\}$  is an  $R$ -basis for  $R$ .

*Proof:* Let  $g_1, g_2 \in R$ . Note that  $(g_1f_1 + g_2f_2)(e_{2i}) = g_1(e_i)$  and  $(g_1f_1 + g_2f_2)(e_{2i+1}) = g_2(e_i)$ . Now, suppose  $g_1f_1 + g_2f_2 = 0$ . Then, by the note,  $g_1(e_i) = g_2(e_i) = 0$  which implies  $g_1 = g_2 = 0$  as the set  $\{e_i\}$  is a basis. Thus  $\{f_1, f_2\}$  is a linearly independent set. To show it is a generating set, let  $g \in R$ . Define  $g_1, g_2 \in R$  by  $g_1(e_i) = g(e_{2i})$  and  $g_2(e_i) = g(e_{2i+1})$  for all  $i \geq 0$ . Then  $(g_1f_1 + g_2f_2)(e_{2i}) = g_1(e_i) = g(e_{2i})$  and  $(g_1f_1 + g_2f_2)(e_{2i+1}) = g_2(e_i) = g(e_{2i+1})$ .

This shows  $R \cong R^2$ . Now, applying this inductively, we see  $R \cong R \oplus R \cong R \oplus R^2 \cong R^3 \cong \dots \cong R^n$ . □

### 3.2 Exact Sequences

**Definition 3.16.** Let  $L, M, N$  be  $A$ -modules and  $f : L \rightarrow M, g : M \rightarrow N$   $A$ -module homomorphisms. We say the sequence  $L \xrightarrow{f} M \xrightarrow{g} N$  is **exact at  $M$**  if  $\text{im } f = \ker g$ . More generally, if the sequence  $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} M_n$  is exact at each  $M_i$  for  $1 \leq i \leq n-1$ , then we say **the sequence is exact**. A **short exact sequence** is an exact sequence of the form  $0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$ . Equivalently,

1.  $f$  is injective
2.  $g$  is surjective
3.  $\text{im } f = \ker g$

**Examples.**

1. Suppose  $L$  is a submodule of  $M$ . Then the sequence  $0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0$  is exact.
2. Let  $M_1, M_2$  be  $A$ -modules. Then the sequence  $0 \rightarrow M_1 \rightarrow M_1 + M_2 \rightarrow M_2 \rightarrow 0$  is exact. This is called a **split short exact sequence**.

**Definition 3.17.** Let  $A$  be a ring and  $(*) 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  a short exact sequence of  $A$ -modules. We say  $(*)$  **splits** (or is **split exact**) if there exists an  $A$ -module homomorphism  $\phi : M \rightarrow L \oplus N$  such that the diagram commutes:

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\
 & & \downarrow 1_L & & \downarrow \phi & & \downarrow 1_N & & \\
 0 & \longrightarrow & L & \xrightarrow{i} & L \oplus N & \xrightarrow{j} & N & \longrightarrow & 0
 \end{array}$$

where  $i : L \rightarrow (L, 0)$  and  $j : (0, N) \rightarrow N$ .

**Proposition 3.18.** Let  $(*) 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  be a short exact sequence. TFAE

1.  $(*)$  splits



2. There exists an  $A$ -linear map  $\sigma : N \rightarrow M$  such that  $g\sigma = 1_N$

3. There exists an  $A$ -linear map  $\pi : M \rightarrow L$  such that  $\pi f = 1_L$ .

If any of these hold, then  $\phi : M \rightarrow L \oplus N$  is an isomorphism.

*Proof.* First, we prove  $\phi$  is an isomorphism. Suppose  $\phi(m) = 0$ . Then  $g \cdot 1_N(m) = j\phi(m) = 0$  implies  $m \in \ker g = \text{im } f$ . So there exists  $\ell \in L$  such that  $m = f(\ell)$ . Then  $i \cdot 1_L(\ell) = \phi f(\ell) = \phi(m) = 0$  and since  $i$  is injective, we have  $\ell = 0$  and thus  $m = 0$ . So  $\phi$  is injective. Now, let  $(\ell, n) \in L \oplus N$ . Since  $g$  is surjective, find  $m \in M$  such that  $g(m) = n$ . Then  $\phi(m) = (\ell', n)$  for some  $\ell' \in L$ . Consider  $\phi(f(\ell - \ell') + m)$ . We see  $\phi(f(\ell - \ell') + m) = \phi f(\ell - \ell') + \phi(m) = i \cdot 1_L(\ell - \ell') + \phi(m) = (\ell - \ell', 0) + (\ell', n) = (\ell, n)$ . Thus  $\phi$  is an isomorphism.

(1)  $\Rightarrow$  (2): Define  $\sigma : N \rightarrow M$  by  $n \mapsto \phi^{-1}((0, n))$ . Then  $g\sigma(n) = g\phi^{-1}((0, n)) = j(0, n) = n$ . Thus  $g\sigma = 1_N$ .

(2)  $\Rightarrow$  (3): Let  $m \in M$ . Note that  $g(m - \sigma g(m)) = g(m) - g\sigma g(m) = 0$  as  $g\sigma = 1_N$ . Thus  $m - \sigma g(m) \in \ker g = \text{im } f$ . As  $f$  is injective, there exists a unique  $\ell \in L$  such that  $f(\ell) = m - \sigma g(m)$ . Define  $\pi : M \rightarrow L$  by  $m \mapsto f^{-1}(m - \sigma g(m))$ . Then  $\phi$  is a homomorphism and  $\pi f(\ell) = f^{-1}(f(\ell) - \underbrace{\sigma g f}_{=0}(\ell)) = f^{-1}(f(\ell)) = 1_L$ .

(3)  $\Rightarrow$  (1): Define  $\phi : M \rightarrow L \oplus N$  by  $m \mapsto (\pi(m), g(m))$ . Then, for  $\ell \in L$ , we see  $\phi(f(\ell)) = (\pi f(\ell), g f(\ell)) = (\ell, 0) = i(\ell)$  and for  $m \in M$ , we see  $j\phi(m) = j(\pi(m), g(m)) = g(m)$ . Thus the diagram commutes.  $\square$

**Example.** Let  $A = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$ . Consider  $g : A^3 \rightarrow A$  by  $(a, b, c) \mapsto a\bar{x} + b\bar{y} + c\bar{z}$ . Note  $g$  is a surjective homomorphism as  $g(\bar{x}, \bar{y}, \bar{z}) = \bar{x}^2 + \bar{y}^2 + \bar{z}^2 = \bar{1} \in \text{im } g$  and since  $\text{im } g$  is an ideal, this says  $\text{im } g = A$ . Consider the short exact sequence  $0 \rightarrow \ker g \hookrightarrow A^3 \xrightarrow{g} A \rightarrow 0$ . Define  $\sigma : A \rightarrow A^3$  by  $1 \mapsto (\bar{x}, \bar{y}, \bar{z})$ . Note  $g\sigma(1) = 1$ , which implies  $g\sigma$  is the identity on the basis for  $A$ . Thus  $g\sigma = 1_A$ . By the proposition, the sequence splits and  $A^3 \cong A \oplus \ker g$ .

**Proposition 3.19.** Let  $F$  be a free  $A$ -module and suppose  $0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} F \rightarrow 0$  is exact. Then the sequence splits.

*Proof.* Let  $S$  be a basis for  $F$ . As  $g$  is onto, for all  $s \in S$  there exists  $m_s \in M$  such that  $g(m_s) = s$ . Define  $\sigma : F \rightarrow M$  by  $s \mapsto m_s$ . This gives a well defined map as  $S$  is a basis for  $F$ . Then by definition,  $g\sigma = 1_S$  and thus  $g\sigma = 1_F$ . Thus by the proposition, the sequence splits.  $\square$

### Examples.

1.  $0 \rightarrow (2) \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/(2) \rightarrow 0$  is a short exact sequence which does not split. Suppose that  $\sigma : \mathbb{Z}/(2) \rightarrow \mathbb{Z}$  defined by  $\bar{1} \mapsto m$  and  $\bar{0} \mapsto 0$  for some  $m \in \mathbb{Z}$ . Then  $0 = \sigma(\bar{0}) = \sigma(2 \cdot \bar{1}) = 2\sigma(\bar{1}) = 2m \in \mathbb{Z}$ . Thus  $m = 0$  and so  $\sigma = 0$ . But then,  $g\sigma = 0 \neq 1$ .

2. Let  $G$  be a finite group,  $k$  a field such that  $\text{char } k \neq |G|$ . Let  $A = k[G]$  and  $V$  any  $A$ -module. Let  $W = \{u \in V \mid gu = u \text{ for all } g \in G\}$ . Then  $W \neq \emptyset$  as  $0 \in W$ . So  $W$  is an  $A$ -submodule of  $V$ . So consider the short exact sequence  $0 \rightarrow W \hookrightarrow V \rightarrow V/W \rightarrow 0$ . This splits! Define  $\rho : V \rightarrow W$  by  $v \mapsto \frac{1}{|G|} \sum_{g \in G} gv$ . Then for  $w \in W$ ,  $\rho(w) = \frac{1}{|G|} |G| w = w$ . So  $\rho i = 1_W$ .

3. Let  $R$  be a PID and  $M$  a finitely generated  $R$ -module. Recall the torsion submodule of  $M$  is  $T(M) = \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus \{0\}\}$ . Also,  $M$  is called **torsion free** if  $T(M) = 0$ .

**Remark.**  $M/T(M)$  is torsion free.

**Fact.** Over a PID, finitely generated torsion free modules are free. (If  $A$  is a finitely generated abelian group, we know  $A \cong \mathbb{Z}^r \oplus \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$  and if torsion free, then it would just be  $A \cong \mathbb{Z}^r$ ).

**Example.** If  $R = \mathbb{Z}[x]$ ,  $I = (2, x)$ , then  $I$  is torsion free but not free (as  $I$  is not principal).

Thus  $0 \rightarrow T(M) \rightarrow M \rightarrow M/T(M) \rightarrow 0$  splits as  $M/T(M)$  is free. Hence  $T(M)$  is a direct summand of  $M$ .

4. Let  $R = k[x, y]$  for a field  $k$  (thus not a PID, but it is a UFD). Let  $M = R^2/R(x^2, xy)$ . Then  $T(M) = \overline{R(x, y)} \cong R/(x)$ , but  $T(M)$  is not a direct summand of  $M$ .

*Proof.* Clearly,  $\overline{x(x,y)} = \overline{(x^2, xy)} = \bar{0}$ . Thus  $\overline{(x,y)} \in T(M)$ . Suppose  $\overline{(a,b)} \in T(M)$ . Then there exists  $f \in k[x,y] \setminus \{0\}$  such that  $f\overline{(a,b)} = \bar{0}$  which implies  $f(a,b) = g(x^2, xy)$  for some  $g \in k[x,y]$ . WLOG, assume  $g \neq 0$  and  $\gcd(f,g) = 1$ . Then  $fa = x^2g$  and  $fb = xyg$  which implies  $f|x^2$  and  $f|xy$ . Thus  $f = u$  or  $f = ux$  for  $u \in k^*$ . If  $f = u$ , then  $(a,b) \in R(x^2, xy)$  which says  $\overline{(a,b)} = 0$ . If  $f = ux$ , then  $(a,b) \in R(x,y)$  (as  $a = u^{-1}xy$  and  $b = u^{-1}yg$ ). Thus  $T(M) = \overline{R(x,y)}$ .

Now suppose  $f\overline{(x,y)} = \bar{0}$ . Then  $f(x,y) = g(x^2, xy)$  which implies  $f = gx$ . So  $f \in (x)$ . Define  $\phi : R \rightarrow \overline{R(x,y)}$  by  $r \mapsto r\overline{(x,y)}$ . Then  $\phi$  is onto and  $\ker \phi = (x)$ . Thus  $R/(x) \cong \overline{R(x,y)} = T(M)$ .  $\square$

Now, we show the short exact sequence  $0 \rightarrow R/(x) \xrightarrow{f} M \xrightarrow{g} M/T(M) \rightarrow 0$  where  $f : \bar{r} \mapsto \overline{r(x,y)}$  does not split. Suppose it did. Let  $\rho : M \rightarrow R/(x)$  be a splitting map so that  $\rho f = 1$ . Let  $\bar{r} = \rho(\bar{0}, 1)$  and  $\bar{s} = \rho(\bar{0}, 1)$ . Then

$$\bar{1} = \rho(\overline{(x,y)}) = \rho(\overline{(x,0)} + \overline{(0,y)}) = x\rho(\overline{(1,0)}) + y\rho(\overline{(0,1)}) = x\bar{r} + y\bar{s} = \overline{xr + ys}.$$

Thus  $1 - xr - ys \in (x)$ . So  $1 - xr - ys = px$  for some  $p$ , a contradiction (just plug in  $x = 0$  and  $y = 0$  to get  $0 = 1$ ). Thus it doesn't split.

5. Let  $R \subseteq S$  be commutative rings and suppose  $S$  is an integral domain (thus  $R$  is as well),  $R$  is a UFD,  $\text{char } R = 0$  and  $S$  is a finitely generated  $R$ -module (thus  $S = Rx_1 + \dots + Rx_n$ ). Then  $R$  is a direct summand of  $S$  as an  $R$ -module, that is,  $0 \rightarrow R \rightarrow S \rightarrow S/R \rightarrow 0$  splits.

*Proof.* Let  $E = Q(S)$  and  $F = Q(R)$ . Then  $E$  is a finite vector space over  $F$  (generated by  $x_1, \dots, x_n$ ) and so  $[E : F] < \infty$ . Since  $\text{char } R = 0$ , we see  $\text{char } F = 0$  and thus  $E/F$  is separable. Define  $\rho : S \rightarrow R$  by  $s \mapsto \frac{1}{[E:F]} Tr_F^E(s)$ . There is more work from here, but its beyond the scope of this course.  $\square$

6. **Theorem (Miyata):** If  $R$  is a commutative, Noetherian ring and  $(*) 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$  is a short exact sequence of finitely generated  $R$ -modules, then  $(*)$  splits if and only if  $M \cong L \oplus N$ .

This is not true in general. For example, let  $R = \mathbb{Z}, F = \bigoplus_{n=1}^{\infty} \mathbb{Z}, T = \bigoplus_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ . Note that  $F/2F \cong T$ . Consider the short exact sequence  $0 \rightarrow F \oplus T \xrightarrow{\phi} F \oplus T \xrightarrow{\psi} T \rightarrow 0$  defined by  $\phi : (f, t) \mapsto (2f, t)$  and  $\psi : (f, t) \mapsto \bar{f}$ . This does not split.

*Proof.* Let  $e_i$  denote the standard basis for  $F$ . Let  $\rho : F \oplus T \rightarrow F \oplus T$  be a splitting map. Then  $\rho\phi = 1$ . Now  $\phi(e_1) = 2e_1$  implies  $e_1 = \rho\phi(e_1) = 2\rho(e_1) = 2\sum a_i e_i$ . Setting basis elements equal, we see  $e_1 = 0$  for  $i \neq 1$  and  $a_1 = \frac{1}{2}$ , contradiction.  $\square$

Note, however, that  $F \oplus T \cong (F \oplus T) \oplus T$  as  $T \oplus T = T$  (its a countable sum).

**Definition 3.20.** Let  $P$  be an  $A$ -module. Then  $P$  is called **projective** if whenever one has a diagram of the form

$$\begin{array}{ccc} M & \xrightarrow{f} & N \longrightarrow 0 \text{ exact} \\ & \nwarrow \exists h & \uparrow i \\ & & P \end{array}$$

then there exists  $h : P \rightarrow M$  such that  $i = fh$  (the diagram commutes). Note that this implies  $f$  and  $i$  are surjective.

**Remark.** Free modules are projective. Let  $F = P$  above, let  $S$  be a basis for  $F$ . For each  $s \in S$ , there exists  $m_s \in M$  such that  $f(m_s) = i(s)$ . Define  $h : F \rightarrow M$  by  $h(s) = m_s$ . Then the diagram commutes.

**Example.** Let  $R = \mathbb{Z}[\sqrt{-5}], I = (2, 1 + \sqrt{-5})$ . Then  $I$  is projective, but not free (as it is not principal).

**Proposition 3.21.** Let  $A$  be a ring and  $P$  an  $A$ -module. TFAE

1.  $P$  is projective
2. there exists an  $A$ -module  $Q$  such that  $P \oplus Q$  is free
3. Every short exact sequence  $0 \rightarrow L \rightarrow M \rightarrow P \rightarrow 0$  splits.

*Proof.* (1)  $\Rightarrow$  (3): Let  $0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} P \rightarrow 0$  be a short exact sequence. Since  $P$  is projective and we have  $1_P : P \rightarrow P$ , there exists  $\rho : P \rightarrow M$  such that the diagram below commutes:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & P \longrightarrow 0 \text{ exact} \\
 & & & & & \swarrow \rho & \uparrow 1_P \\
 & & & & & & P
 \end{array}$$

But then  $g\rho = 1_P$  and thus the SES splits.

(3)  $\Rightarrow$  (2): Let  $\phi : F \rightarrow P$  be a surjection, where  $F$  is free. Let  $Q = \ker \phi$ . Then  $0 \rightarrow Q \rightarrow F \rightarrow P \rightarrow 0$  is exact and splits by (3). Thus  $F \cong Q \oplus P$ .

(2)  $\Rightarrow$  (1):] Consider the diagram

$$\begin{array}{ccccc}
 M & \xrightarrow{f} & N & \longrightarrow & 0 \text{ exact} \\
 & \nearrow h & \uparrow i & & \\
 & & P & & \\
 & & \uparrow \pi & & \\
 & & P \oplus Q & & 
 \end{array}$$

Since free modules are projective, there exists  $h : P \oplus Q \rightarrow M$  such that  $fh = i\pi$ . Let  $j : P \rightarrow P \oplus Q$  be defined by  $p \mapsto (p, 0)$ . Then  $hj : P \rightarrow M$ . Also,  $f(hj) = fhj = i\pi j = i$ . Thus the diagram commutes.  $\square$

**Examples/Remarks.**

1. Every free module is projective.
2. Every projective module over  $k[x_1, \dots, x_n]$  (for a field  $k$ ) is free. (Quillen-Suslin, 1975).
3. If  $R$  is a commutative Noetherian domain, then every non-finitely generated projective  $R$ -module is free (Bass, 1963).
4.  $\mathbb{Z}/2\mathbb{Z}$  is not a projective  $\mathbb{Z}$ -module. Since the only map from  $\mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}$  is the 0-map, the diagram below, with  $f : 1 \mapsto \bar{1}$ , would never commute:

$$\begin{array}{ccccc}
 \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \text{ exact} \\
 & \nearrow 0 & \uparrow i & & \\
 & & \mathbb{Z}/2\mathbb{Z} & & 
 \end{array}$$

5.  $\mathbb{Z}/(6) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$ . Since  $\mathbb{Z}/(6)$  is free (as an  $\mathbb{Z}/(6)$ -module), we see that  $\mathbb{Z}/(2)$  and  $\mathbb{Z}/(3)$  are projective  $\mathbb{Z}/(6)$ -modules. However, they are not free (just count elements...there are too few elements to be a direct sum of copies of  $\mathbb{Z}/(6)$ .)
6. Let  $R = \mathbb{Z}[\sqrt{-5}]$ ,  $I = (2, 1 + \sqrt{-5})$ . Then  $I$  is not free (it's not principal), but it is projective.

*Proof.* Define  $\phi : R^2 \rightarrow I$  by  $(a, b) \mapsto 2a + (1 + \sqrt{-5})b$ . Let  $K = \ker \phi$ . We'll show  $0 \rightarrow K \rightarrow R^2 \rightarrow I \rightarrow 0$  splits. Define  $\rho : I \rightarrow R^2$  by  $x \mapsto x \left( \frac{1-3\sqrt{-5}}{2}, \frac{3\sqrt{-5}}{1+\sqrt{-5}} \right)$ . We need to show that the image is actually in  $R^2$ , but to do that it is enough to show for  $x = 2, 1 + \sqrt{-5}$ :

$$(1 + \sqrt{-5}) \left( \frac{1 - 3\sqrt{-5}}{2} \right) = \frac{1 - 2\sqrt{-5} + 15}{2} = 8 - \sqrt{-5}, \quad 2 \left( \frac{3\sqrt{-5}}{1 + \sqrt{-5}} \right) = \frac{6\sqrt{-5}}{1 + \sqrt{-5}} = (1 - \sqrt{-5})(\sqrt{-5}) \in R.$$

Since we are just multiplying, this is certainly a homomorphism. Note that  $\phi\rho(x) = \phi \left( x \left( \frac{1-3\sqrt{-5}}{2}, \frac{3\sqrt{-5}}{1+\sqrt{-5}} \right) \right) = x(1 - 3\sqrt{-5} + 3\sqrt{-5}) = x$ . Thus the SES splits which says that  $I$  is a direct summand of a free module, and thus projective.  $\square$

7. Let  $G$  be a finite group and  $k$  a field such that  $\text{char } k \nmid |G|$ . Let  $R = k[G]$ .

**Fact.** Let  $M$  be any  $R$ -module and  $N$  any  $R$ -submodule of  $M$ . Then  $N$  is a direct summand of  $M$ .

Let  $M$  be any  $R$ -module,  $F$  any free module. Consider the short exact sequence  $0 \rightarrow \ker \phi \rightarrow F \xrightarrow{\phi} M \rightarrow 0$ . Since  $\ker \phi$  is a summand, we get a splitting map. Thus  $F \cong \ker \phi \oplus M$  which implies every module is projective. However, there exist non-free modules. Let  $M = R(\sum_{g \in G} g) = k(\sum_{g \in G} g)$ . Then  $\dim_k M = 1$  and  $\dim_k R = |G|$ . Thus  $M$  cannot be a free  $R$ -module as the dimensions do not work out (unless of course  $|G| = 1$ ).

### 3.3 Localization

Let  $R$  be a ring. A set  $S \subseteq Z(R)$  is **multiplicatively closed** (mc) if  $ab \in S$  whenever  $a, b \in S$ .

**Definition 3.22.** Let  $R$  be a ring and  $S \neq \emptyset$  a mcs of  $R$ . The **localization of  $R$  at  $S$**  is a ring  $T$  together with a ring homomorphism  $\phi : R \rightarrow T$  such that

1.  $\phi(s)$  is a unit in  $T$  for all  $s \in S$ .
2. If  $f : R \rightarrow A$  is a ring homomorphism such that  $f(s)$  is a unit for all  $s \in S$ , then there exists a unique ring homomorphism  $g : T \rightarrow A$  such that

$$\begin{array}{ccc} R & \xrightarrow{\phi} & T \\ f \downarrow & \swarrow \exists! g & \\ A & & \end{array}$$

**Proposition 3.23.** If  $T$  exists, it is unique up to isomorphism

*Proof.* Show 2 maps compose to the identity  $\square$

**Notation.** We denote  $T$  by  $S^{-1}R$  or  $R_S$ .

**Theorem 3.24.**  $R_S$  exists.

*Proof.* Define an equivalence relation on  $R \times S$  by  $(r_1, s_1) \sim (r_2, s_2)$  if and only if  $t(s_2r_1 - s_1r_2) = 0$  for some  $t \in S$ .

Claim: This defines an equivalence relation.

*Proof:* We show transitivity. Suppose  $(r_1, s_1) \sim (r_2, s_2)$  and  $(r_2, s_2) \sim (r_3, s_3)$ . Then there exists  $t_1, t_2 \in S$  such that  $t_1s_2r_1 = t_1s_1r_2$  and  $t_2s_3r_2 = t_2s_2r_3$ . Then  $t_1s_2r_1s_3 = t_1s_1r_2s_3$  and  $t_2s_3r_2s_1 = t_2s_2r_3s_1$ . Then  $t_1t_2s_2(s_3r_1 - s_1r_3) = 0$ .

Denote the equivalence class of  $(r, s)$  by  $\frac{r}{s}$ . Let  $R_S := \{ \frac{r}{s} \mid (r, s) \in R \times S \}$ . Define  $+, \cdot$  on  $R_S$  in the usual manner (this requires a little work to show its well-defined). Thus  $R_S$  forms a ring with identity. The identity of  $R_S$  is  $\frac{s}{s}$  for any  $s \in S$ . Define  $\phi : R \rightarrow R_S$  by  $r \mapsto \frac{r}{s}$  for any  $s \in S$ . This is a ring homomorphism. Let  $t \in S$ . Then

$\phi(t) = \frac{ts}{s}$  and  $\phi(t)^{-1} = \frac{s}{ts}$ . Now, suppose  $f : R \rightarrow A$  is a ring homomorphism such that  $f(s)$  is a unit for all  $s \in S$ . Define  $g : R_S \rightarrow A$  by  $\frac{r}{s} \mapsto f(r)f(s)^{-1}$ . To show  $g$  is well-defined, suppose  $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ . Then  $t(r_1s_2 - r_2s_1) = 0$  for some  $t \in S$ . So  $f(t)(f(s_2)f(r_1) - f(s_1)f(r_2)) = 0$ . This implies  $f(s_2)f(r_1) = f(s_1)f(r_2)$  as  $f(t)$  is a unit and thus  $f(r_1)f(s_1)^{-1} = f(r_2)f(s_2)^{-1}$ . To show that  $g$  is unique, suppose there exists  $g_1 : R_S \rightarrow A$  such that  $g_1\phi = f$ . Then, for some  $t \in S$ , we see

$$g_1\left(\frac{r}{s}\right)f(s) = g_1\left(\frac{r}{s}\right)g_1\phi(s) = g_1\left(\frac{r}{s}\right)g_1\left(\frac{st}{t}\right) = g_1\left(\frac{rst}{st}\right) = g_1\phi(r) = f(r).$$

Thus  $g_1\left(\frac{r}{s}\right) = f(r)f(s)^{-1} = g\left(\frac{r}{s}\right)$ . □

### Remarks.

1. If  $S$  is a mcs of  $R$ , so is  $S' = S \cup \{1\}$ . Furthermore,  $R_S \cong R_{S'}$ . Thus, WLOG, we may assume  $1 \in S$  and the canonical ring homomorphism  $\phi : R \rightarrow R_S$  is  $r \mapsto \frac{r}{1}$ .
2.  $0 \in S$  if and only if  $R_S = \{0\}$  (as  $0(s_2r_1 - s_1r_2) = 0$ , i.e., there is only one equivalence class).
3. If  $S$  consists solely of units of  $R$ , then  $R_S \cong R$ .
4. If  $S$  consists solely of non-zero-divisors, then  $\frac{r_1}{s_1} = \frac{r_2}{s_2}$  if and only if  $s_2r_1 - s_1r_2 = 0$ . In particular,  $\phi : R \rightarrow R_S$  is one-to-one. So we can consider  $R$  as a subring of  $R_S$ .

### 3 Important Examples of Localizations

1. Let  $x \in Z(R)$  and  $S = \{x^n\}$ . The localization  $R_S$  is denoted by  $R_x$ . **Example.**  $\mathbb{Z}_2 = \mathbb{Z}[\frac{1}{2}]$ . (Don't confuse this with  $\mathbb{Z}_2 = \{0, 1\}$ ).
2. Let  $R$  be a commutative ring and  $S = \{x \in R \mid x \text{ is a non zero divisor}\}$ . Then  $R_S$  is called the **total quotient ring** of  $R$ , denoted  $Q(R)$ . If  $R$  is a domain,  $Q(R)$  is the field of fractions of  $R$ .
3. Let  $R$  be a commutative ring,  $p \neq R$  a prime ideal. Let  $S = R - p$ . Then  $S$  is mc. In this case, we denote  $R_S$  by  $R_p$ . **Example.**  $\mathbb{Z}_{(2)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid b\}$ .

**Definition 3.25.** Let  $R$  be a commutative ring. The **(prime) spectrum** of  $R$  is  $\text{Spec}R = \{p \mid p \neq R \text{ is a prime ideal of } R\}$ .

### Examples.

1. If  $K$  is a field, then  $\text{Spec}K = \{0\}$ .
2.  $\text{Spec}\mathbb{Z} = \{(0), (p) \mid p \text{ is prime}\}$ .
3.  $\text{Spec}\mathbb{C}[x] = \{(0), (x - a) \mid a \in \mathbb{C}\}$ .

**Proposition 3.26.** Let  $R$  be commutative,  $I$  an ideal of  $R$ . Let  $V(I) = \{p \in \text{Spec}R \mid p \supseteq I\}$ . Then there exists a bijective inclusion preserving correspondence  $V(I) \leftrightarrow \text{Spec}(R/I)$  defined by  $p \in V(I) \mapsto p/I$  and  $q \in \text{Spec}(R/I) \mapsto \phi^{-1}(q)$  where  $\phi : R \rightarrow R/I$  is the canonical map  $r \mapsto \bar{r}$ .

### Remarks.

1. If  $\phi : R \rightarrow S$  is a ring homomorphism and  $q \in \text{Spec}S$ , then  $\phi^{-1}(q) = \{r \in R \mid \phi(r) \in q\}$  is a prime ideal of  $R$ .
2. If  $p \in V(I)$ , then  $p/I \in \text{Spec}(R/I)$  as  $R/I/p/I \cong R/p$ , a domain.

### Examples.

1.  $\text{Spec}\mathbb{Z}/(30) = \{(\bar{2}), (\bar{3}), (\bar{5})\}$ .

$$2. \text{Spec}\mathbb{C}/(x^2 + 1) = \{(\overline{x+i}), (\overline{x-i})\}.$$

$$3. \text{Spec}\mathbb{R}[x]/(x^2 + 1) = \{(0)\}.$$

**Proposition 3.27.** Let  $R$  be a commutative ring,  $S$  a mcs of  $R$ . Then there exists a bijective inclusion preserving correspondence  $\{p \in \text{Spec}R | p \cap S = \emptyset\} \leftrightarrow \text{Spec}R_S$  defined by  $p \mapsto p_S = pR_S = \{\frac{a}{s} | a \in p, s \in S\}$  and  $q \in \text{Spec}R_S \mapsto \phi^{-1}(q)$  where  $\phi: R \rightarrow R_S$  is the canonical map  $r \mapsto \frac{r}{1}$ .

*Proof.* We will prove several claims.

Claim:  $p_S$  is a proper prime ideal of  $R_S$ .

Proof: Suppose  $\frac{a}{s} \cdot \frac{b}{t} \in p_S$ . Then  $\frac{ab}{st} = \frac{x}{s'}$  for some  $x \in p, s' \in S$ . Then there exists  $t' \in S$  such that  $t's'ab = t'stx \in p$ .

As  $t', s' \in S, t's' \notin p$ . So  $ab \in p$  which implies  $a \in p$  or  $b \in p$ . Thus  $\frac{a}{s} \in p_S$  or  $\frac{b}{t} \in p_S$ . Thus, it's a prime ideal. To show its proper, suppose  $p_S = R_S$ . Then  $\frac{1}{1} \in p_S$  which implies  $\frac{1}{1} = \frac{a}{s}$  for  $a \in p, s \in S$ . Then there exists  $t \in S$  such that  $t(s-a) = 0$  which implies  $ts = ta \in p$ , but  $t, s \in S$  implies  $ts \notin p$ , a contradiction.

Claim:  $\phi^{-1}(p) \in \text{Spec}R$  for  $q \in \text{Spec}R_S$ .

Proof: Since  $\phi(1) = 1$ , if  $1 \in \phi^{-1}(q), 1 \in q$ . So  $\phi^{-1}(q)$  is proper. It's a prime ideal by the remark.

Claim:  $\phi^{-1}(p_S) = p$ .

Proof: We know  $p \subseteq \phi^{-1}(p_S)$ . Suppose  $\phi(r) \in p_S$ . Then  $\frac{r}{1} = \frac{a}{s}, a \in p, s \in S$ . Then there exists  $t \in S$  such that  $tsr = ta \in p$ . Since  $t, s \in S, ts \notin p$  and so  $r \in p$ .

Claim:  $\phi^{-1}(q)_S = q$ .

Proof: Let  $\frac{a}{s} \in \phi^{-1}(q)_S$ , that is,  $a \in \phi^{-1}(q), s \in S$ . Then  $\frac{a}{1} = \phi(a) \in q$ . Thus  $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in q$  as it is an ideal. Let  $x \in q$ . Then  $x = \frac{r}{s}, r \in R, s \in S$ . Then  $sx = \frac{r}{1} \in q$ . So  $r \in \phi^{-1}(q)$  which implies  $x = \frac{r}{s} \in \phi^{-1}(q)_S$ .  $\square$

### Examples.

$$1. \text{Spec}\mathbb{Z}_2 = \{(p)\mathbb{Z}_2 | p > 2 \text{ is prime}\}.$$

$$2. \text{Spec}\mathbb{Z}_{30} = \{p\mathbb{Z}_{30} | p > 5 \text{ is prime}\}.$$

$$3. \text{Spec}\mathbb{Z}_{(2)} = \{(0)\mathbb{Z}_{(2)}, (2)\mathbb{Z}_{(2)}\} \text{ as } p \cap S = \emptyset \text{ if and only if } (p) \subseteq (2) \text{ where } S = R - (2).$$

**Remark.** If  $P \in \text{Spec}R$ , then  $\text{Spec}R_P = \{q_P | q \in \text{Spec}R, q \subseteq P\}$ . Thus  $R_P$  has a unique maximal ideal, namely  $PR_P = P_P$ .

**Definition 3.28.** A commutative ring which has a unique maximal ideal is called a **local (or quasilocal) ring**. Note: For some, local means Noetherian and has a unique maximal ideal.

**Remark.** Let  $(R, m)$  be the local ring where  $m$  denotes the unique maximal ideal. Then  $x \in R$  is a unit if and only if  $x \notin m$ .

*Proof.*  $x$  is a unit if and only if  $(x) = R$  if and only if  $(x)$  is not contained in any maximal ideal of  $R$  which is if and only if  $x \notin m$  as  $m$  is the unique maximal ideal.  $\square$

**Note.**  $R_m \cong R$ . This is because  $R_m = R_S$  where  $S = R - m$  and everything outside  $m$  is already a unit.

### Examples.

$$1. \mathbb{Z}/(8). \text{ The only prime ideal is } (\overline{2}).$$

$$2. \mathbb{C}[[x]]. \sum a_i x^i \text{ is a unit if and only if } a_0 \neq 0.$$

**Proposition 3.29.** Let  $S$  and  $T$  be mcs of  $R$ . WLOG, assume  $1 \in S \cap T$ . Then

1.  $ST = \{st | s \in S, t \in T\}$  is a mcs of  $R$  (containing both  $S$  and  $T$ ).
2.  $\frac{T}{1} = \{\frac{t}{1} \in R_S | t \in T\}$  is a mcs of  $R_S$ .
3.  $\frac{T}{S} = \{\frac{t}{s} \in R_S | t \in T, s \in S\}$  is a mcs of  $R_S$ .

Furthermore,  $R_{ST} \cong (R_S)_{\frac{T}{1}} \cong (R_S)_{\frac{T}{S}}$ .

*Proof.* Note that 1,2,3 are trivial. For the last statement, we will use the fact (without proof) that if  $S$  consists of units of  $R$ , then  $R_{ST} \cong R_T$ . Note  $\frac{T}{S} = \frac{T}{1} \cdot \frac{1}{S}$  and  $\frac{1}{S}$  consists of units of  $R_S$ . Thus by the fact,  $(R_S)_{\frac{T}{S}} \cong (R_S)_{\frac{T}{1}}$ . So it is enough to show  $R_{ST} \cong (R_S)_{\frac{T}{1}}$ . Consider the canonical map  $i : R \rightarrow R_{ST}$  where  $r \mapsto \frac{r}{1}$ . Note  $i(s)$  is a unit for all  $s \in S$  as  $S \subseteq ST$ . By the universal property, there exists a unique ring homomorphism  $g : R_S \rightarrow R_{ST}$  defined by  $\frac{r}{s} \mapsto \frac{r}{1} \cdot (\frac{s}{1})^{-1} = \frac{r}{s}$ . Note that  $g(\frac{t}{1}) = \frac{t}{1}$  is a unit in  $R_{ST}$  for all  $t \in T$  as  $T \subseteq ST$ . Thus, we can again use the universal property to obtain the ring homomorphism  $\phi : (R_S)_{\frac{T}{1}} \rightarrow R_{ST}$  defined by  $\frac{\frac{r}{s}}{\frac{t}{1}} \mapsto \frac{r}{s} (\frac{t}{1})^{-1} = \frac{r}{st}$ . Now, consider the composition of canonical maps  $\psi : R \rightarrow R_S \rightarrow (R_S)_{\frac{T}{1}}$ . Then  $\psi(st) = \frac{st}{1}$ , with inverse  $\frac{1}{st}$ . Thus  $\psi(st)$  is a unit for all  $s \in S, t \in T$  and so by the universal property there exists a ring homomorphism  $\psi : R_{ST} \rightarrow (R_S)_{\frac{T}{1}}$  defined by  $\frac{r}{st} \mapsto \frac{r}{st}$ . It is obvious that  $\phi\psi = \psi\phi = 1$ .  $\square$

**Corollary 3.30.** Suppose  $S \subseteq T$  are mcs of  $R$ . Then  $(R_S)_{\frac{T}{S}} \cong (R_S)_{\frac{T}{1}} \cong R_{ST} \cong R_T$  as  $ST = T$ .

**Corollary 3.31.** Let  $S$  be a mcs and  $P \in \text{Spec}R$  such that  $P \cap S \neq \emptyset$ . Then  $P_S \in \text{Spec}R_S$  and  $(R_S)_{P_S} \cong R_P$ .

*Proof.* Recall  $R_P = R_T$  where  $T = R - P$ . Also,  $(R_S)_{P_S} = (R_S)_{\frac{T}{S}} \cong R_T$  as  $P \cap S \neq \emptyset$  implies  $S \subseteq T$ .  $\square$

**Corollary 3.32.** Let  $P \subseteq Q$  be prime ideals of  $R$ . Then  $P \cap (R - Q) = \emptyset$ . Thus  $P_Q \in \text{Spec}R_Q$  and  $(R_Q)_{P_Q} \cong R_P$ .

**Example.**  $(\mathbb{Z}_{(2)})_{\frac{1}{2}}$ . Let  $S = \mathbb{Z} - (2) = \{a \in \mathbb{Z} | 2 \nmid a\}, T = \{2^n | n \geq 0\}$ . Then,  $(\mathbb{Z}_{(2)})_{\frac{1}{2}} \cong (\mathbb{Z}_S)_{\frac{T}{1}} \cong \mathbb{Z}_{ST} \cong \mathbb{Q}$  as  $ST = \mathbb{Z} \setminus \{0\}$ .

**Definition 3.33.** Let  $R$  be a commutative ring,  $I$  an ideal of  $R$ . The **radical** of  $I$  is  $\sqrt{I} = \{r \in R | r^n \in I, \text{ for some } n \geq 0\}$ . When  $I = (0)$ , we call  $\sqrt{(0)} = \text{nilrad}R = \{a \in R | a \text{ is nilpotent}\}$  the **nilradical**.

**Proposition 3.34.** Let  $I$  be an ideal of  $R$ . Then  $\sqrt{I} = \bigcap_{P \in V(I)} P$  where  $V(I) = \{P \in \text{Spec}R | P \supseteq I\}$ . In particular,  $\text{nilrad}R = \bigcap_{P \in \text{Spec}R} P$ .

*Proof.* Let  $r \in \sqrt{I}$  and  $P \in V(I)$ . Then  $r^n \in I$  for some  $n$ . As  $I \subseteq P, r^n \in P$ . Thus  $r \in P$  as  $P$  is prime. Suppose  $r \notin \sqrt{I}$ . Then we will show there exists  $P \in V(I)$  such that  $r \notin P$ . Note  $I_r \neq R_r$  as otherwise  $\frac{1}{r} \in I_r$  which implies  $\frac{1}{r} \in \frac{I}{r^n}$ , that is  $r^m(r^n - i) = 0$  which implies  $r^{m+n} = r^m i \in I$ , a contradiction as that says  $r \in \sqrt{I}$ . Therefore, there exists a prime (maximal) ideal of  $R_r$  containing  $I_r$ , that is, there exists  $P \in \text{Spec}R$  with  $r \notin \sqrt{P} = P$  such that  $P_r \supseteq I_r$ . Let  $\phi : R \rightarrow R_r$  be the canonical map. Then  $P = \phi^{-1}(P_r) \supseteq \phi^{-1}(I_r) \supseteq I$ . So  $P \in V(I)$  and  $r \notin P$ .  $\square$

**Proposition 3.35.** Let  $R$  be a commutative ring,  $I$  an ideal of  $R$  and  $S$  a mcs. Then  $\overline{S} = \{s = s + I | s \in S\}$  is a mcs of  $R/I$ . Then  $(R/I)_{\overline{S}} \cong R_S/I_S$ .

*Proof.* Consider the canonical maps  $\phi : R \rightarrow R/I \rightarrow (R/I)_{\overline{S}}$ . Note that  $\phi(S) = \frac{\overline{S}}{1}$  is a unit for all  $x \in X$ . Thus there exists a ring homomorphism  $f : R_S \rightarrow (R/I)_{\overline{S}}$  defined by  $\frac{r}{s} \mapsto \frac{\overline{r}}{1} \cdot (\frac{\overline{s}}{1})^{-1} = \frac{\overline{r}}{\overline{s}}$ . Clearly,  $f$  is surjective. Notice  $\ker f = I_S$  as  $\frac{r}{s} \in \ker f$  if and only if  $\frac{\overline{r}}{\overline{s}} = \frac{0}{1}$  if and only if there exists  $t \in S$  such that  $t\overline{r} = 0$  if and only if  $tr \in I$  for some  $t \in S$  if and only if  $\frac{r}{s} \in I_S$ . Thus, by the First Isomorphism Theorem, done.  $\square$

### Localization of Modules

Let  $R$  be a ring,  $S$  a mcs,  $M$  a left  $R$ -module. Define an equivalence relation on  $M \times S$  by  $(m_1, s_1) \sim (m_2, s_2)$  if and only if there exists  $t \in S$  such that  $t(s_2 m_1 - s_1 m_2) = 0$ . This defines an equivalence relation. Denote the equivalence class of  $(m, s)$  by  $\frac{m}{s}$ . Let  $M_S = \{\frac{m}{s} | m \in M, s \in S\}$ . Define  $\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$  and  $\frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{r m}{s_1 s_2}$ . These are well-defined and make  $M_S$  an  $R_S$ -module.

**Proposition 3.36.** *Let  $R$  be a commutative ring,  $M$  an  $R$ -module. TFAE*

1.  $M = 0$
2.  $M_p = 0$  for all  $p \in \text{Spec}R$ .
3.  $M_m = 0$  for all maximal ideals  $m$ .

*Proof.* (1)  $\Rightarrow$  (2)  $\Rightarrow$  (3) is trivial. So we will only prove (3)  $\Rightarrow$  (1). Let  $x \in M$  and  $I = \text{ann}_R x = \{r \in R \mid rx = 0\}$ . Let  $m$  be a maximal ideal of  $R$ . By (3),  $\frac{x}{1} \in M_m = 0$ . Thus there exists  $t$  not in  $m$  such that  $tx = 0$ . So  $t \in I$  and  $I \not\subseteq m$ . As  $m$  is arbitrary, we must have  $I = R$ . Thus  $x = 0$  as  $1 \in I$  which implies  $M = 0$ .  $\square$

Let  $f : M \rightarrow N$  be an  $R$ -module homomorphism. Let  $S$  be a mcs. For  $s \in S$ , define  $\frac{f}{s} : M_S \rightarrow N_S$  by  $\frac{m}{s'} \mapsto \frac{f(m)}{ss'}$ . This is a well-defined  $R_S$ -module homomorphism.

**Proposition 3.37.** *Let  $(*) 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  be a short exact sequence of  $R$ -modules. Then  $(**) 0 \rightarrow L_S \xrightarrow{\frac{f}{1}} M_S \xrightarrow{\frac{g}{1}} N_S \rightarrow 0$  is a short exact sequence of  $R_S$ -modules for any mcs  $S$  of  $R$ . Furthermore, if  $(*)$  splits, then  $(**)$  does.*

*Proof.*  $\frac{f}{1}$  is 1-1: Suppose  $\frac{f}{1}(\frac{\ell}{s}) = 0$ . Then  $\frac{f(\ell)}{s} = \frac{0}{1}$ . Thus there exists  $t \in S$  such that  $tf(\ell) = 0$ , which implies  $f(t\ell) = 0$  and thus  $t\ell = 0$ . Therefore  $\frac{\ell}{s} \equiv \frac{0}{1}$  in  $L_S$ .

$\frac{g}{1}$  is onto: Clear

$\text{im} \frac{f}{1} = \ker \frac{g}{1}$  : Since  $\text{im} f \subseteq \ker g$ ,  $gf = 0$ . Then  $\frac{g}{1} \cdot \frac{f}{1} = 0$ . Hence,  $\text{im} \frac{f}{1} \subseteq \ker \frac{g}{1}$ . Now, let  $\frac{m}{s} \in \ker \frac{g}{1}$ . Then there exists  $t \in S$  such that  $g(tm) = 0$ . So  $tm \in \ker g = \text{im} f$ . So  $tm = f(\ell)$ . Thus  $\frac{tm}{1} = \frac{f(\ell)}{1}$  which implies  $\frac{m}{s} = \frac{f(\ell)}{st} = \frac{f}{1}(\frac{\ell}{st}) \in \text{im} \frac{f}{1}$ .

Thus  $(**)$  is exact. If  $(*)$  splits, there exists  $h : N \rightarrow M$  such that  $gh = 1_N$ . Then  $\frac{g}{1} \cdot \frac{h}{1} = 1_{N_S}$ . Thus  $\frac{h}{1}$  is the splitting map for  $(**)$ .  $\square$

**Corollary 3.38.** *Suppose  $N \subseteq M$  are  $R$ -modules. Then  $(M/N)_S \cong M_S/N_S$ .*

*Proof.* Since  $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$  is exact, the above says  $0 \rightarrow N_S \rightarrow M_S \rightarrow (M/N)_S \rightarrow 0$  is exact. Thus  $M_S/N_S \cong (M/N)_S$ .  $\square$

**Corollary 3.39.**  $(A \oplus B)_S \cong A_S \oplus B_S$

*Proof.* Since  $0 \rightarrow A \rightarrow A \oplus B \rightarrow B \rightarrow 0$  is split exact, so is  $0 \rightarrow A_S \rightarrow (A \oplus B)_S \rightarrow B_S \rightarrow 0$  is split exact. Thus  $(A \oplus B)_S \cong A_S \oplus B_S$ .  $\square$

**Exercise:**  $(\oplus_{i \in I} A_i)_S \cong \oplus_{i \in I} (A_i)_S$ .

**Corollary 3.40.** *If  $F$  is a free  $R$ -module, then  $F_S$  is a free  $R_S$ -module.*

*Proof.* Since  $F \cong \oplus_{i \in I} R$ , we see  $F_S \cong \oplus_{i \in I} R_S$ .  $\square$

**Corollary 3.41.** *If  $P$  is a projective  $R$ -module, then  $P_S$  is a projective  $R_S$ -module.*

*Proof.* There exists  $Q$  such that  $P \oplus Q \cong F$ , a free module. Therefore  $P_S \oplus Q_S \cong F_S$  which is also free. So  $P_S$  is a projective  $R_S$ -module.  $\square$

**Definition 3.42.** *Let  $R$  be a commutative ring. The **Jacobson radical**, denoted  $J(R)$ , is defined to be the intersection of all maximal ideals of  $R$ .*

**Examples.**  $J(\mathbb{Z}) = 0$ ,  $J(k[x]) = 0$ , and  $J(\mathbb{Z}/(12)) = (\overline{2}) \cap (\overline{3}) = (\overline{6})$ .

**Remark.** If  $x \in J(R)$ , then  $1 - x$  is a unit.

*Proof.* If  $1 - x \in m$ , then  $1 \in m$ , a contradiction. So  $1 - x \notin m$  for all maximal ideals  $m$ . Thus  $1 - x$  is a unit.  $\square$



**Lemma 3.43 (Nakayama's Lemma).** *Let  $R$  be a commutative ring and  $M$  a finitely generated  $R$ -module. Suppose  $M = JM$  where  $J = J(R)$ . Then  $M = 0$ .*

*Proof.* Choose a least  $n$  such that  $M$  is generated by  $n$  elements, say  $x_1, \dots, x_n$ . We will show  $n = 0$  (and so  $M = 0$ ). Let  $x_n \in JM$ , so  $x_n = j_1x_1 + \dots + j_nx_n, j_i \in J$ . Then  $(1 - j_n)x_n = j_1x_1 + \dots + j_{n-1}x_{n-1}$ . Then, since  $1 - j_n$  is a unit,  $x_n = (1 - j_n)^{-1}j_1x_1 + \dots + (1 - j_n)^{-1}j_{n-1}x_{n-1} \in Rx_1 + \dots + Rx_{n-1}$ , a contradiction to the minimality of  $n$ .  $\square$

**Corollary 3.44.** *Suppose  $N \subseteq M$  are  $R$ -modules and  $M$  is finitely generated. Suppose  $M = N + JM$  where  $J = J(R)$ . Then  $M = N$ .*

*Proof.* Note that  $M/N = (N + JM)/N = J(M/N)$ . Since  $M$  is finitely generated, so is  $M/N$ . By Nakayama's Lemma,  $M/N = 0$ .  $\square$

**Corollary 3.45.** *Let  $M$  be a finitely generated  $R$ -module. Let  $x_1, \dots, x_n \in M$ . Then  $x_1, \dots, x_n$  generate  $M$  if and only if  $\bar{x}_1, \dots, \bar{x}_n$  generate  $M/JM$  where  $J = J(R)$ .*

*Proof.* Note that  $(\Rightarrow)$  is trivial. To show  $(\Leftarrow)$ , let  $N = Rx_1 + \dots + Rx_n$ . Since  $\bar{x}_1, \dots, \bar{x}_n$  generate  $M/JM$ , we have  $(N + JM)/JM = M/JM$  which implies  $M = N + JM$  which implies  $M = N$ .  $\square$

**Notation.** If  $M$  is an  $R$ -module, let  $\mu_R(M) = \inf\{n \mid M = Rx_1 + \dots + Rx_n \text{ for some } x_1, \dots, x_n \in M\}$  = the minimal number of generators for  $M$ .

**Corollary 3.46.** *Let  $M$  be a finitely generated  $R$ -module,  $J = J(R)$ . Then  $\mu_R(M) = \mu_{R/J}(M/JM)$ .*

**Corollary 3.47.** *Suppose  $(R, m)$  is local. For any finitely generated  $R$ -module  $M$ ,  $\mu_R(M) = \dim_{R/m} M/mM$ . In particular, any two minimal generating sets for  $M$  have the same number of elements.*

*Proof.* Since  $R/m$  is a field,  $\mu_R(M) = \mu_{R/m}(M/mM) = \dim_{R/m} M/mM$ .  $\square$

**Proposition 3.48.** *Let  $(R, m)$  be a local ring and  $P$  a finitely generated projective  $R$ -module. Then  $P$  is free.*

*Proof.* We will use the fact (without proof) that  $\oplus M_i/I(\oplus M_i) \cong \oplus (M_i/IM_i)$ . Let  $n = \mu_R(P) = \dim_{R/m}(P/mP)$ . Let  $x_1, \dots, x_n$  be a minimal generating set for  $P$ . Define  $\phi : R^n \rightarrow P$  by  $e_i \mapsto x_i$ . Then  $\phi$  is surjective. Let  $K = \ker \phi$ . Then we have the short exact sequence  $0 \rightarrow K \rightarrow R^n \xrightarrow{\phi} P \rightarrow 0$ . This splits as it ends with a projective module. So  $R^n \cong P \oplus K$  and  $K$  is finitely generated (as  $R^n$  is finitely generated and  $R^n \rightarrow P \oplus K \rightarrow K$  is onto). Then  $R^n/mR^n \cong (P \oplus K)/m(P \oplus K)$  which implies  $(R/m)^n \cong (P/mP) \oplus (K/mK)$  by our fact. This is an isomorphism as  $R/m$  vector spaces. Taking the dimensions of both sides, since  $\dim(R/m)^n = n = \dim P/mP$ , we have  $\dim K/mK = 0$ , that is,  $K/mK = 0$  and thus  $K = mK$ . Since  $K$  is finitely generated,  $K = 0$  by Nakayama's Lemma and thus  $\phi$  is an isomorphism. Thus  $R^n \cong P$ .  $\square$

### 3.4 Category Theory and the Hom Functor

**Definition 3.49.** *A **category**  $\mathcal{C}$  consists of a class of objects (denoted by  $\text{Obj } \mathcal{C}$ ) and a set of morphisms  $\text{Hom}_{\mathcal{C}}(A, B)$  for every pair of objects  $A, B$  of  $\mathcal{C}$  such that*

1. (Composition) there exists a function  $\text{Hom}_{\mathcal{C}}(B, C) \times \text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, C)$  sending  $(f, g) \mapsto f \circ g$  for all objects  $A, B, C$ .
2. (Associativity)  $(fg)h = f(gh)$  for all morphisms  $f, g, h$  where  $(fg)h$  is defined.
3. (Identity) For all objects  $A$  of  $\mathcal{C}$  there exists  $1_A \in \text{Hom}_{\mathcal{C}}(A, A)$  such that for all objects  $B$  of  $\mathcal{C}$  we have  $1_A f = f$  for all  $f \in \text{Hom}_{\mathcal{C}}(B, A)$  and  $f 1_A = f$  for all  $f \in \text{Hom}_{\mathcal{C}}(A, B)$ .

**Examples.**

1. The category of sets:  $\langle\langle \text{Sets} \rangle\rangle$  has sets as objects and functions as morphisms.
2. The category of groups:  $\langle\langle \text{Groups} \rangle\rangle$  has groups as objects and group homomorphisms as morphisms. This category has the **subcategory**  $\langle\langle \text{Abel} \rangle\rangle$  of abelian groups. Note that a subcategory is called a **full subcategory** if it retains all of the morphisms.
3. For a commutative ring  $R$ , the category of  $R$ -algebras:  $\langle\langle R\text{-algebra} \rangle\rangle$  has  $R$ -algebras as objects and  $R$ -algebra homomorphisms  $(\phi : S \rightarrow T$  where  $S, T$  are  $R$ -algebras such that  $\phi$  is a ring homomorphism where  $\phi(rs) = r\phi(s)$  for all  $r \in R$ ) as the set of morphisms.

**Note.** Every ring is a  $\mathbb{Z}$ -algebra. Thus  $\langle\langle \mathbb{Z}\text{-algebras} \rangle\rangle = \langle\langle \text{Rings} \rangle\rangle$ .

4. For a commutative ring  $R$ , the category of left  $R$ -modules is written  $\langle\langle R\text{-mod} \rangle\rangle$  and the category of right  $R$ -modules is written  $\langle\langle \text{mod-}R \rangle\rangle$ .

**Special Cases**

- (a)  $\langle\langle \mathbb{Z}\text{-mod} \rangle\rangle = \langle\langle \text{Abel} \rangle\rangle$
- (b) If  $k$  is a field,  $\langle\langle k\text{-mod} \rangle\rangle = \langle\langle k\text{-vector spaces} \rangle\rangle$

**Definition 3.50.** Let  $\mathcal{C}$  and  $\mathcal{D}$  be categories. A (**covariant**) **functor**  $F : \mathcal{C} \rightarrow \mathcal{D}$  is a rule which associates to each object  $A$  of  $\mathcal{C}$  an object  $F(A)$  of  $\mathcal{D}$  and for each morphism  $f \in \text{Hom}_{\mathcal{C}}(A, B)$  a morphism  $F(f) \in \text{Hom}_{\mathcal{D}}(F(A), F(B))$  with the following properties:

1.  $F(fg) = F(f)F(g)$  for all morphisms  $f, g$  of  $\mathcal{C}$  where  $fg$  is defined.
2.  $F(1_A) = 1_{F(A)}$  for all objects  $A$  of  $\mathcal{C}$ .

**Examples.**

1. The **forgetful functor**  $F : \langle\langle \text{Groups} \rangle\rangle \rightarrow \langle\langle \text{Sets} \rangle\rangle$  defined by sending a group  $G$  to the set  $G$  and the group homomorphism  $g$  to the function  $g$ . Another forgetful functor is  $F' : \langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle \text{Abel} \rangle\rangle$ .
2. The Localization functor:  $F : \langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle R_S\text{-mod} \rangle\rangle$  where  $F(M) = M_S$  and  $F(f) = \frac{f}{1}$ .
3. The Modding Out functor: Let  $I$  be a 2-sided ideal of  $R$ . Then we can define  $F : \langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle R/I\text{-mod} \rangle\rangle$  by  $F(M) = M/IM$  and for an  $R$ -homomorphism  $f : M \rightarrow N$ ,  $F(f) : M/IM \rightarrow N/IN$  where  $m + IM \mapsto f(m) + IN$ .

**Note.** You can mod out by a left ideal, however the functor would then be  $\langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle R\text{-mod} \rangle\rangle$ .

**Definition 3.51.** Let  $M, N$  be left  $R$ -modules. Then  $\text{Hom}_R(M, N)$  denotes the set of left  $R$ -module homomorphisms from  $M \rightarrow N$ .

**Remarks.**

1.  $\text{Hom}_R(M, N)$  is an abelian group.
2. Generally,  $\text{Hom}_R(M, N)$  is not a left  $R$ -module, unless  $R$  is commutative.
3. Let  $M$  be a left  $R$ -module. Define a functor  $\text{Hom}_R(M, -) : \langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle \text{Abel} \rangle\rangle$  by  $\text{Hom}_R(M, -)(N) = \text{Hom}_R(M, N)$  and if  $f : N_1 \rightarrow N_2$  is an  $R$ -module homomorphism, then  $f_* := \text{Hom}_R(M, -)(f) : \text{Hom}_R(M, N_1) \rightarrow \text{Hom}_R(M, N_2)$  defined by  $g \mapsto fg$ . Note that  $(fg)_* = f_*g_*$  and  $(1_N)_* = 1_{\text{Hom}_R(M, N)}$  (and thus it really is a functor).

**Definition 3.52.** A **contravariant functor**  $F : \mathcal{C} \rightarrow \mathcal{D}$  is a rule which associates to each object  $A$  of  $\mathcal{C}$  an object  $F(A)$  of  $\mathcal{D}$  and for every pair of objects  $A, B$  of  $\mathcal{C}$  a map  $\text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{D}}(F(B), F(A))$  defined by  $f \mapsto F(f)$  such that  $F(fg) = F(g)F(f)$  and  $F(1_A) = 1_{F(A)}$ .

**Example.** Let  $N$  be a left  $R$ -module. Define the contravariant functor  $Hom_R(-, N) : \langle\langle R\text{-mod} \rangle\rangle \rightarrow \langle\langle \text{Abel} \rangle\rangle$  by  $M \mapsto Hom_R(M, N)$  and  $(f : M_1 \rightarrow M_2) \mapsto (f^* : Hom_R(M_2, N) \rightarrow Hom_R(M_1, N))$  where  $g \mapsto gf$ . One can check that  $(fg)^* = g^*f^*$ .

**Definition 3.53.** Let  $F$  be a functor (of either variance) on module categories. We say  $F$  is **additive** if for every pair of objects  $A, B$  of the initial category, the map  $F : Hom_C(A, B) \rightarrow Hom_D(F(A), F(B))$  (or  $F : Hom_C(A, B) \rightarrow Hom_D(F(B), F(A))$ ) is a group homomorphism, that is,  $F(f + g) = F(f) + F(g)$  for all  $f, g \in Hom_C(A, B)$ .

**Remarks.**

1. Localization, Modding Out, and the Hom functors are all additive.
2. Suppose  $A \xrightarrow{f} B \xrightarrow{g} C$  is exact and let  $F$  be an additive covariant functor. Consider  $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ . In general, this is not exact - but we do still get  $imF(f) \subseteq kerF(g)$ .

*Proof.* This is equivalent to showing  $F(g)F(f) = 0$ . Of course,  $F(g)F(f) = F(gf) = F(0) = 0$  as  $F$  is additive ( $F(0) = F(0) + F(0)$  implies  $F(0) = 0$ ). □

**Definition 3.54.** As additive functor on module categories is **exact** if whenever  $A \xrightarrow{f} B \xrightarrow{g} C$  is exact in the initial category, then  $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$  is exact (or in the contravariant case  $F(C) \rightarrow F(B) \rightarrow F(A)$  is exact). Suppose  $F$  is covariant. Say  $F$  is **left exact** if

$$0 \rightarrow A \rightarrow B \rightarrow C \text{ exact implies } 0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C) \text{ is exact}$$

and  $F$  is **right exact** if

$$A \rightarrow B \rightarrow C \rightarrow 0 \text{ exact implies } F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0 \text{ is exact.}$$

Suppose  $F$  is contravariant. Say  $F$  is **left exact** if

$$A \rightarrow B \rightarrow C \rightarrow 0 \text{ exact implies } 0 \rightarrow F(C) \rightarrow F(B) \rightarrow F(A) \text{ is exact}$$

and  $F$  is **right exact** if

$$0 \rightarrow A \rightarrow B \rightarrow C \text{ exact implies } F(C) \rightarrow F(B) \rightarrow F(A) \rightarrow 0 \text{ is exact.}$$

**Proposition 3.55.** Let  $F$  be an additive functor. TFAE

1.  $F$  is exact
2.  $F$  takes short exact sequences to short exact sequences
3.  $F$  is both left and right exact.

**Remark.** We've shown localization is an exact covariant functor.

**Proposition 3.56.** The modding out functor is right exact, but not generally exact.

*Proof.* Let  $I$  be a left ideal of  $R$ ,  $L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  an exact sequence of  $R$ -modules. Consider  $L/IL \xrightarrow{\bar{f}} M/IM \xrightarrow{\bar{g}} N/IN \rightarrow 0$  where  $\bar{f}(\ell + IL) = f(\ell) + IM$  and  $\bar{g}(m + IM) = g(m) + IN$ . As  $g$  is onto, so is  $\bar{g}$ . Also,  $im\bar{f} \subseteq ker\bar{g}$  as modding out is an additive functor. So we need only show  $im\bar{f} \supseteq ker\bar{g}$ . Let  $x \in ker\bar{g}$ . Then  $\bar{g}(x) = \bar{g}(\bar{x}) = \bar{0}$  which implies  $g(x) \in IN$ . Thus there exists  $i_j \in I, n_j \in N$  such that  $g(x) = \sum_{j=1}^k i_j n_j$ . Let  $u_j \in M$  such that  $g(u_j) = n_j$ . Then  $g(x) = \sum u_j g(u_j) = g(\sum i_j u_j)$ . Thus  $g(x - \sum i_j u_j) = 0$  which implies  $x - \sum i_j u_j \in ker g = im f$ . Let  $\ell \in L$  such that  $f(\ell) = x - \sum i_j u_j$ . Then  $\bar{f}(\bar{\ell}) = \bar{x} \in im\bar{f}$ .

To show it is not always left exact, consider  $0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z}$  where  $n \mapsto 2n$ . Modding out by (2) gives us  $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{2} \mathbb{Z}/2\mathbb{Z}$  where  $\bar{n} \mapsto 2\bar{n} = 0$ . Thus the map is not injective.  $\square$

**Proposition 3.57.** *Let  $M$  be a left  $R$ -module. Then  $\text{Hom}_R(M, -)$  and  $\text{Hom}_R(-, M)$  are both left exact, but not generally exact.*

*Proof.* We will prove only for  $\text{Hom}_R(M, -)$ . Let  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C$  be exact and consider  $0 \rightarrow \text{Hom}_R(M, A) \xrightarrow{f_*} \text{Hom}_R(M, B) \xrightarrow{g_*} \text{Hom}_R(M, C)$ . As  $f$  is 1-1, we have  $fh = f_*(h) = 0$  which implies  $h = 0$ . Thus  $f_*$  is 1-1. By additivity,  $\text{im}f_* \subseteq \ker g_*$ . Thus we need only show  $\text{im}f_* \supseteq \ker g_*$ . Let  $h \in \ker g_*$  where  $h : M \rightarrow B$ . So  $g_*(h) = gh = 0$ . This says  $\text{im}h \subseteq \ker g = \text{im}f$ . Thus for all  $m \in M$  there exists a unique  $a_m \in A$  such that  $f(a_m) = h(m)$ . Define  $k : M \rightarrow A$  by  $k(m) = a_m$ . Then  $k \in \text{Hom}_R(M, A)$  and  $f_*(k) = h \in \text{im}f_*$ .

To show it is not always right exact, consider  $\mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ . This gives us  $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \rightarrow 0$ . Now, the first two modules are 0 and the last is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ . Thus it does not preserve surjectivity.  $\square$

**Proposition 3.58.** *Let  $R$  be a ring and  $P$  a left  $R$ -module. Then  $P$  is projective if and only if  $\text{Hom}_R(P, -)$  is exact.*

*Proof.* We will only prove the forward direction. The backward direction is similar. Let  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  be exact and apply the Hom functor:

$$0 \rightarrow \text{Hom}(P, A) \xrightarrow{f_*} \text{Hom}(P, B) \xrightarrow{g_*} \text{Hom}(P, C) \rightarrow 0.$$

By the previous proposition, it is enough to show  $g_*$  is onto. Let  $h \in \text{Hom}_R(P, C)$ . By the definition of projective, there exists  $k : P \rightarrow B$  such that  $gk = h$  which implies  $g_*(k) = h$ . Thus  $h \in \text{im}g_*$  and is thus onto.  $\square$

### 3.5 Tensor Products

**Definition 3.59.** *Let  $R, S$  be rings. An  $R - S$  bimodule is a left  $R$ -module  $M$  which is also a right  $S$ -module such that  $(rm)s = r(ms)$  for all  $r \in R, s \in S, m \in M$ .*

**Examples.**

1. Any ring  $R$  is an  $R - R$  bimodule.
2. Let  $S$  be an  $R$ -algebra ( $\rho : R \rightarrow S, \rho(R) \subseteq Z(S), R$  commutative). Any left  $S$  module is an  $S - R$  bimodule via  $m \cdot r = \rho(r)m$  for all  $r \in R, m \in M$  (in general, we will just say  $m \cdot r = rm$  for simplicity).  
Check:  $(sm)r = r(sm) = (rs)m = (sr)m = s(rm) = s(mr)$ .

**Special Case.**

1. If  $R$  is a commutative ring, every left  $R$ -module is an  $R - R$  bimodule ( $R$  is an  $R$ -algebra)
2. Any ring is a  $\mathbb{Z}$ -algebra (as every ring is an abelian group). Thus every left  $R$ -module is an  $R - \mathbb{Z}$  bimodule.
3.  $S = M_n(k), k$  a field. Any left  $S$ -module is an  $S - k$  bimodule (i.e., every left  $S$ -module is a  $k$ -vector space).

**Remark.** Let  $M$  be an  $R - S$  bimodule and  $N$  a left  $R$ -module. Then  $\text{Hom}_R(M, N)$  is a left  $S$  module via  $(sf)(m) := f(ms)$ . Check:  $(sf)(rm) = f((rm)s) = f(r(ms)) = rf(ms) = r(sf)(m)$ .

If  $M$  is an  $R - S$  bimodule, then  $\text{Hom}_R(M, -) : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle S - \text{mod} \rangle\rangle$ . Check: Suppose  $f : N_1 \rightarrow N_2$  is an  $R$ -module homomorphism. Then we have  $f_* : \text{Hom}_R(M, N_1) \rightarrow \text{Hom}_R(M, N_2)$  defined by  $g \mapsto fg$  and we see  $f_*(sg)(m) = f \circ (sg)(m) = f(g(ms)) = sf g(m)$ . Thus  $f_*(sg) = sf_*(g)$ .

Similarly, if  $S$  is an  $R - S$  bimodule, then  $\text{Hom}_R(M, N)$  is a right  $S$ -module via  $fs(m) = f(m)s$ .

**Definition 3.60.** *Let  $A$  be a right  $R$ -module and  $B$  a left  $R$ -module. An  $R$ -biadditive map on  $A \times B$  is a function  $f : A \times B \rightarrow G$  where  $G$  is an abelian group such that for  $a_i \in A, b_i \in B, r \in R$*

1.  $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$
2.  $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$
3.  $f(ar, b) = f(a, rb)$

**Definition 3.61.** Let  $A$  be a right  $R$ -module,  $B$  a left  $R$ -module. The **tensor product** of  $A, B$  is an abelian group  $A \otimes_R B$  and an  $R$ -biadditive map  $\phi : A \times B \rightarrow A \otimes_R B$  such that given any  $R$ -biadditive map  $f : A \times B \rightarrow T$  (an abelian group), there exists a unique group homomorphism  $\tilde{f} : A \otimes_R B \rightarrow T$  such that  $\tilde{f}\phi = f$ .

**Note.** Hom and  $\otimes$  are in some sense adjoints of each other.

**Exercise.** If it exists,  $A \otimes_R B$  is unique up to isomorphism.

**Theorem 3.62.**  $A \otimes_R B$  exists.

*Proof.* Let  $F = \bigoplus_{(a,b) \in A \times B} \mathbb{Z}$  (a free  $\mathbb{Z}$ -module). Let  $[a, b]$  be the standard basis element with 1 in the  $[a, b]$ <sup>th</sup> coordinate and 0's elsewhere. Thus every element of  $F$  is uniquely expressed as  $\sum_{i=1}^n m_i [a_i, b_i]$ . Let  $S$  be the subgroup of  $F$  generated by all the elements of the form

$$[a, b_1 + b_2] - [a, b_1] - [a, b_2], [a_1 + a_2, b] - [a_1, b] - [a_2, b], [ar, b] - [a, rb].$$

Define  $A \otimes_R B = F/S$ , with generating elements  $a \otimes b = [a, b] + S$ . (Note: For  $m \in \mathbb{Z}, m > 0$ , we have  $m(a \otimes b) = (ma) \otimes b$ . So every element looks like  $\sum a_i \otimes b_i$ , but is non uniquely represented).

Claim: The tensor product is biadditive, that is,

1.  $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$
2.  $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$
3.  $(ar) \otimes b = a \otimes (rb)$ .

Proof: Since  $[a, b_1 + b_2] - [a, b_1] - [a, b_2] \in S$ , we know  $[a, b_1 + b_2] + S = [a, b_1] + S + [a, b_2] + S$ . Thus (1) holds. Similarly, (2) and (3) are true.

Define  $\phi : A \times B \rightarrow A \otimes_R B$  by  $(a, b) \mapsto a \otimes b$ . By the remarks above,  $\phi$  is clearly biadditive.

Now, let  $f : A \times B \rightarrow T$  be a biadditive map. Define  $f' : F \rightarrow T$  by  $[a, b] \mapsto f(a, b)$ . As  $f$  is biadditive,  $S \subseteq \ker f'$ . Thus there exists an induced homomorphism  $\tilde{f} : F/S \rightarrow T$  defined by  $[a, b] \mapsto f(a, b)$ , that is  $\tilde{f} : A \otimes_R B \rightarrow T$  with  $a \otimes b \mapsto f(a, b)$ . This makes the diagram commute. Clearly,  $\tilde{f}$  is unique since  $A \otimes_R B$  is generated by  $\{a \otimes b | a \in A, b \in B\}$ . □

**Example.**  $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong 0$ . A typical generator looks like  $\bar{a} \otimes \bar{b}$ . Since 2, 3 are relatively prime, there exists  $r, s, p, q \in \mathbb{Z}$  such that  $a = 2r + 3s, b = 2p + 3q$ . Thus  $\bar{a} \otimes \bar{b} = 3\bar{s} \otimes 2\bar{p} = 2\bar{s} \otimes 3\bar{p} = 0 \otimes 0 = 0$ .

**Proposition 3.63.** Let  $R$  be a ring,  $f : A_1 \rightarrow A_2$  an  $R$ -homomorphism of right  $R$ -modules and  $g : B_1 \rightarrow B_2$  an  $R$ -homomorphism of left  $R$ -modules. Then there exists a unique group homomorphism  $f \otimes g : A_1 \otimes_R B_1 \rightarrow A_2 \otimes_R B_2$  defined by  $a \otimes b \mapsto f(a) \otimes g(b)$ .

*Proof.* Define  $f \times g : A_1 \times B_1 \rightarrow A_2 \otimes_R B_2$  by  $(a, b) \mapsto f(a) \otimes g(b)$ . Clearly this is  $R$ -biadditive. Thus we get the unique homomorphism  $f \otimes g$ . □

**Remarks.**  $(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g$  and  $(f \otimes g)(h \otimes \ell) = fh \otimes g\ell$ .

**Corollary 3.64.** Let  $R$  be a ring and  $A$  a right  $R$ -module. Define  $A \otimes_R - : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle \text{Abel} \rangle\rangle$  by  $B \mapsto A \otimes_R B$  and  $(f : B_1 \rightarrow B_2) \mapsto (1_A \otimes f : A \otimes_R B_1 \rightarrow A \otimes_R B_2)$ . Then  $A \otimes_R -$  is an additive covariant functor.

**Note.** If  $A$  is a left  $R$ -module, we get  $- \otimes_R B : \langle\langle \text{mod} - R \rangle\rangle \rightarrow \langle\langle \text{Abel} \rangle\rangle$ .

**Theorem 3.65.** *Let  $A$  be a right  $R$ -module. Then  $A \otimes_R -$  is right exact.*

*Proof.* Let  $L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  be an exact sequence of left  $R$ -modules. We want to show  $A \otimes_R L \xrightarrow{1 \otimes f} A \otimes_R M \xrightarrow{1 \otimes g} A \otimes_R N \rightarrow 0$  is exact.

$1 \otimes g$  is onto: Since  $A \otimes N$  is generated by  $a \otimes n$ , it is enough to show  $a \otimes n \in \text{im}(1 \otimes g)$ . For  $n \in N$ , there exists  $m \in M$  such that  $g(m) = n$  as  $g$  is onto. Then  $(1 \otimes g)(a \otimes m) = a \otimes g(m) = a \otimes n$ .

$\text{im}(1 \otimes f) \subseteq \ker(1 \otimes g)$ : Notice  $(1 \otimes g)(1 \otimes f) = 1 \otimes gf = 1 \otimes 0 = 0$ .

$\text{im}(1 \otimes f) \supseteq \ker(1 \otimes g)$ : By the above, we get an induced map  $\overline{1 \otimes g} : A \otimes_R M / \text{im}(1 \otimes f) \rightarrow A \otimes_R N$  defined by  $\overline{a \otimes m} \mapsto a \otimes g(m)$ . It is enough to show  $\overline{1 \otimes g}$  is 1-1. Define  $h : A \times N \rightarrow A \otimes M / \text{im}(1 \otimes f)$  by  $(a, n) \mapsto \overline{a \otimes m}$  where  $m \in M$  is such that  $g(m) = n$ .

Claim:  $h$  is well-defined.

Proof: Suppose  $g(m_1) = g(m_2) = n$ . Since  $g(m_1 - m_2) = 0$ , we have  $m_1 - m_2 \in \ker g = \text{im} f$ . Let  $\ell \in L$  such that  $f(\ell) = m_1 - m_2$ . Then  $a \otimes m_1 - a \otimes m_2 = a \otimes (m_1 - m_2) = a \otimes f(\ell) = (1 \otimes f)(a \otimes \ell) \in \text{im}(1 \otimes f)$ . Thus  $\overline{a \otimes m_1} = \overline{a \otimes m_2}$ .

It is easy to show  $h$  is  $R$ -biadditive. Thus, there exists a unique group homomorphism  $\tilde{h} : A \otimes_R N \rightarrow A \otimes_R M / \text{im}(1 \otimes f)$  defined by  $a \otimes n \mapsto h(a, n)$ . Note that  $\tilde{h}(1 \otimes g)(\overline{a \otimes m}) = \overline{a \otimes m}$ . Thus it fixes the generating set, which is enough to say  $\tilde{h}(1 \otimes g) = 1$ . Thus  $1 \otimes g$  is injective and thus  $\ker(1 \otimes g) = \text{im}(1 \otimes f)$ .  $\square$

**Example.**  $\mathbb{Z}/2\mathbb{Z} \oplus_{\mathbb{Z}} -$  is not exact. Consider the injection  $0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z}$  defined by  $m \mapsto 2m$ . This yields  $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{1 \otimes 2} \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$  defined by  $\bar{a} \otimes m \mapsto \bar{a} \otimes 2m = 2\bar{a} \otimes m = 0$ , but  $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$  is not 0.

**Proposition 3.66.** *Let  $M$  be a left  $R$ -module. Then there exists a group isomorphism  $f : R \otimes M \rightarrow M$  defined by  $r \otimes m \mapsto rm$ .*

*Proof.* Define  $f' : R \times M \rightarrow M$  defined by  $(r, m) \mapsto rm$ . This is  $R$ -biadditive. Thus we have the unique group homomorphism  $f : R \otimes M \rightarrow M$ . Define  $g : M \rightarrow R \otimes M$  by  $m \mapsto 1 \otimes m$ . This is clearly well defined and a group homomorphism. Also  $fg = gf = 1$ . So  $f$  is an isomorphism.  $\square$

**Proposition 3.67.** *Let  $R, S$  be rings,  $M$  an  $S - R$  bimodule and  $N$  a left  $R$ -module. Then  $M \otimes_R N$  is a left  $S$ -module under the action  $s(\sum m_i \otimes n_i) = \sum (sm_i) \otimes n_i$ .*

*Proof.* The  $S$ -module axioms are trivial. Thus we just need to show it is well-defined. Let  $s \in S$ . Define  $\mu_S : M \times N \rightarrow M \otimes_R N$  by  $(m, n) \mapsto (sm, n)$ . We see  $\mu_S$  is  $R$ -biadditive. Thus we get the group homomorphism  $\widetilde{\mu}_S : M \otimes_R N \rightarrow M \otimes_R N$  defined by  $m \otimes n \mapsto (sm) \otimes n$ . Define  $s(\sum m_i \otimes n_i) = \widetilde{\mu}_S(\sum m_i \otimes n_i) = \sum \widetilde{\mu}_S(m_i \otimes n_i) = \sum (sm_i) \otimes n_i$ . Thus it is well-defined.  $\square$

**Corollary 3.68.** *In this situation,  $M \otimes_R - : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle S - \text{mod} \rangle\rangle$ .*

**Examples.**

1. If  $R$  is commutative, every  $R$ -module  $M$  is an  $R - R$  bimodule. So  $M \otimes_R - : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle R - \text{mod} \rangle\rangle$ .
2. Let  $k$  be commutative and  $R$  a  $k$ -algebra. Let  $M$  be a right  $R$ -module. Then  $M$  is a  $k - R$  bimodule. So  $M \otimes_R - : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle k - \text{mod} \rangle\rangle$ .

**Theorem 3.69.** *Let  $R, S$  be rings,  $A$  a right  $R$ -module,  $B$  an  $R - S$  bimodule, and  $C$  a left  $S$ -module. Then there exists a group isomorphism  $g : A \otimes_R (B \otimes_S C) \rightarrow (A \otimes_R B) \otimes_S C$  defined by  $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ . In addition, if  $A$  is an  $R - R$  bimodule, then  $g$  is a homomorphism of left  $R$ -modules.*

*Proof.* Fix  $a \in A$ . Define  $g_a : B \times C \rightarrow (A \otimes_R B) \otimes_S C$  by  $(b, c) \mapsto (a \otimes b) \otimes c$ .

Claim:  $g_a$  is  $S$ -biadditive.

Proof: Let  $s \in S$ . Then  $g_a(bs, c) = (a \otimes (bs)) \otimes c = ((a \otimes b)s) \otimes c = (a \otimes b) \otimes (sc) = g_a(b, sc)$ . The other properties follow similarly.

So there exists a unique group homomorphism  $\tilde{g}_a : B \otimes_S C \rightarrow (A \otimes_R B) \otimes_S C$ . Now, define  $f : A \times (B \otimes_S C) \rightarrow (A \otimes_R B) \otimes_S C$  by  $(a, x) \mapsto \tilde{g}_a(x)$ . A little work shows  $f$  is also biadditive. Thus, we get  $\tilde{f} : A \otimes_R (B \otimes_S C) \rightarrow (A \otimes_R B) \otimes_S C$  defined by  $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ . Analogously, there exists a homomorphism  $\tilde{h} : (A \otimes_R B) \otimes_S C \rightarrow A \otimes_R (B \otimes_S C)$  defined by  $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$ . Then  $\tilde{f}\tilde{h} = \tilde{h}\tilde{f} = 1$  (its clearly true on the generators and thus all elements as they are group homomorphisms). Take  $g = \tilde{f}$ .

To show  $g$  is a homomorphism of left  $R$ -modules when  $A$  is an  $R - R$  bimodule, just need to check the following:

$$\begin{aligned} g(r(a \otimes (b \otimes c))) &= g((ra) \otimes (b \otimes c)) \\ &= (ra) \otimes b \otimes c \\ &= (r(a \otimes b)) \otimes c \\ &= r((a \otimes b) \otimes c) = rg(a \otimes (b \otimes c)). \end{aligned}$$

□

### Change of Rings

**Proposition 3.70.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Let  $M$  be a left  $R$ -module. Then  $S \otimes_R M$  is a left  $S$ -module. Thus  $S \otimes_R - : \langle\langle R - \text{mod} \rangle\rangle \rightarrow \langle\langle S - \text{mod} \rangle\rangle$ .

Proof. Note that  $S$  is an  $S - R$  bimodule, where  $s \cdot r = s\phi(r)$ . □

### Examples.

1. If  $I$  is a 2 sided ideal, then  $R/I \otimes_R M$  is a left  $R/I$  module. In particular,  $R/m \otimes_R M$  is an  $R/m$  vector space (as  $R/m$  is a field).
2. If  $S$  is a multiplicatively closed set, then  $R_S \otimes_R M (\cong M_S)$  is an  $R_S$ -module.
3. Let  $\phi : G_1 \rightarrow G_2$  be a group homomorphism. Then there exists an induced ring homomorphism  $\tilde{\phi} : k[G_1] \rightarrow k[G_2]$  sending  $g \mapsto \phi(g)$  for a field  $k$ . Let  $V$  be a left  $k[G_1]$ -module. Then  $k[G_2] \otimes_{k[G_1]} V$  is a left  $k[G_2]$ -module. This is called the **induced representation** of  $V$  to  $G_2$ .

**Proposition 3.71.** If  $I$  is a 2 sided ideal, then  $R/I \otimes_R M \rightarrow M/IM$  defined by  $\bar{r} \otimes m \mapsto \overline{rm}$  is an isomorphism.

**Exercise.** Let  $F$  be an additive functor on module categories. Then  $F$  preserves split exact sequences, that is, if  $F$  is covariant and  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  is split exact, then  $0 \rightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \rightarrow 0$  is split exact. In particular,  $F$  preserves the split exactness of  $0 \rightarrow A \rightarrow A \oplus C \rightarrow C \rightarrow 0$ . Hence,  $F(A \oplus C) \cong F(A) \oplus F(C)$ .

**Corollary 3.72.**  $\text{Hom}(A \oplus B, C) \cong \text{Hom}(A, C) \oplus \text{Hom}(B, C)$

$\text{Hom}(A, B \oplus C) \cong \text{Hom}(A, B) \oplus \text{Hom}(A, C)$

$A \otimes_R (B \oplus C) \cong (A \otimes_R B) \oplus (A \otimes_R C)$

**Note.** By induction, we can show the Corollary is true for finite sums. In general, this does not apply to infinite sums with the Hom functors, however, it is true for the tensor product.

**Proposition 3.73.** Let  $A$  be a right  $R$ -module and  $\{B_i\}_{i \in I}$  a family of left  $R$  modules. Then  $A \otimes_R (\bigoplus_{i \in I} B_i) \cong \bigoplus_{i \in I} (A \otimes_R B_i)$  via  $a \otimes (b_i) \mapsto (a \otimes b_i)$ .

**Example.**  $R^m \otimes_R R^n \cong R^m \otimes (\bigoplus_{i=1}^n R) \cong \bigoplus_{i=1}^n (R^m \otimes_R R) \cong \bigoplus_{i=1}^n R^m \cong R^{mn}$ .

**Corollary 3.74.** Suppose  $\phi : R \rightarrow S$  is a ring homomorphism. If  $F$  is a free left  $R$ -module, then  $S \otimes_R F$  is a free left  $S$ -module.

*Proof.* Recall  $F \cong \bigoplus_{i \in I} R$ . So  $S \otimes F \cong \bigoplus_{i \in I} (S \otimes_R R) \cong \bigoplus_{i \in I} S$ , a free left  $S$ -module.  $\square$

**Corollary 3.75.** *Let  $P$  be a projective left  $R$ -module. Then  $S \otimes_R P$  is a projective left  $S$ -module.*

*Proof.* Recall that there exists a left  $R$ -module  $Q$  such that  $P \oplus Q = F$ , a free  $R$ -module. Then  $(S \otimes_R P) \oplus (S \otimes_R Q) \cong S \otimes_R (P \oplus Q) = S \otimes_R F$ , a free  $S$ -module. Thus  $S \otimes_R P$  is a direct summand of a free  $S$  module and is thus projective.  $\square$

**Definition 3.76.** *Let  $R$  be a commutative ring,  $M$  an  $R$ -module. An element  $m \in M$  is **torsion** if there exists a non zero divisor  $r \in R$  such that  $rm = 0$ . Say  $M$  is **torsion free** if the only torsion element is 0.*

**Note.** Ideals are always torsion free (as if  $r \cdot i = 0$ , then either  $r$  is a zero divisor or  $i = 0$ ).

**Example.** Let  $R = k[[x, y]]/(xy)$ ,  $k$  is a field. This is local. Let  $m = (x, y)R$ , the maximal ideal. Then  $m$  is torsion free.

Claim:  $x \otimes y \in m \otimes m$  is torsion.

Proof: We can see  $x+y$  is not a zero divisor in  $R$ . However,  $(x+y)(x \otimes y) = (x+y)x \otimes y = (x+y) \otimes (xy) = (x+y) \otimes 0 = 0$ .  
(In fact,  $\text{Ann}_R x \otimes y = m$ ).

Claim:  $x \otimes y \neq 0$ .

Proof: Recall if  $(R, m)$  is local and  $M$  is finitely generated, then the minimal number of generators,  $\mu_R(M) = \dim_{R/m} M/mM$ . Consequently,  $\mu_R(M \otimes N) = \mu_R(M)\mu_R(N)$  (if  $M, N$  are f.g.). Let  $h = (x, y)k[[x, y]]$ . Clearly,  $\mu_{k[[x, y]]}(h) = 2$ . Note that  $m = n/(xy)$  and  $m/m^2 = \frac{n/(xy)}{n^2/(xy)} = n/n^2$ . So  $\mu_R(m) = \mu_{k[[x, y]]}(n) = 2$ . Thus  $\mu_R(m \otimes m) = 4$ . Every element of  $m \otimes m$  is an  $R$ -linear combination of  $x \otimes x, x \otimes y, y \otimes x, y \otimes y$ , which implies this is a minimal generating set and thus  $x \otimes y \neq 0$ .

**Example.** Let  $R = k[[x, y]], m = (x, y)R$ . Note  $R$  is a domain (so there are no zero divisors). In  $m \otimes m$ , consider  $u = x \otimes y - y \otimes x$ . Note that  $u \neq 0$  as  $x \otimes y, y \otimes x$  are generators and thus basis elements in  $R/m$ , a field. Let  $r \in m$ . Then  $ru = r \otimes xy - r \otimes xy = 0$ . Thus  $\text{Ann}_R u = m$ .

**Theorem 3.77 (Hom - Tensor adjointness).** *Let  $R, S$  be rings,  $A$  a left  $R$ -module,  $B$  an  $S - R$  bimodule,  $C$  a left  $S$ -module. Then*

$$\text{Hom}_S(B \otimes_R A, C) \cong \text{Hom}_R(A, \text{Hom}_S(B, C)).$$

*Note that this is an isomorphism of abelian groups. However, if  $A$  is an  $R - S$  bimodule, then it is an isomorphism of left  $S$ -modules.*

*Proof.* Let  $f \in \text{Hom}_S(B \otimes_R A, C)$ . Fix  $a \in A$ . Define  $f_a : B \rightarrow C$  by  $b \mapsto f(b \otimes a)$ .

Claim:  $f_a$  is  $S$ -linear.

Proof:  $f_a(sb) = f((sb) \otimes a) = f(s(b \otimes a)) = sf(b \otimes a) = sf_a(b)$  as  $f$  is  $S$ -linear. Additivity follows similarly. Thus  $f_a \in \text{Hom}_S(B, C)$ .

Define  $\tilde{f} : A \rightarrow \text{Hom}_S(B, C)$  by  $a \mapsto f_a$ . This is  $R$ -linear as  $\tilde{f}(ra) = f_{ra}$  and  $r\tilde{f}(a) = r \cdot f_a$  implies  $r \cdot f_a(b) = f_a(br) = f(br) \otimes a = f(b \otimes (ra)) = f_{ra}(b)$ . Now, define  $\tau : \text{Hom}_S(B \otimes_R A, C) \rightarrow \text{Hom}_R(A, \text{Hom}_S(B, C))$  by  $f \mapsto \tilde{f}$ . Check that this is additive (and thus a group homomorphism. Let  $f \in \text{Hom}_R(A, \text{Hom}_S(B, C))$ . Define  $g' : B \times A \rightarrow C$  by  $(b, a) \mapsto g(a)(b)$ .

Claim:  $g'$  is  $R$ -biadditive.

Proof:  $g'(br, a) = g(a)(br) = (r \cdot g(a))(b)$  as  $\text{Hom}_S(B, C)$  is a left  $R$ -module. Now,  $(r \cdot g(a))(b) = g(ra)(b) = g'(b, ra)$  by definition of  $g$ .

Thus we get  $\bar{g} : B \otimes_R A \rightarrow C$  defined by  $b \otimes a \mapsto g(a)(b)$ . Now, define  $\pi : \text{Hom}_R(A, \text{Hom}_S(B, C)) \rightarrow \text{Hom}_S(B \otimes_R A, C)$  by  $g \mapsto \bar{g}$ . Check that  $\pi$  is additive and  $\pi\tau = \tau\pi = 1$ .  $\square$



### 3.6 Noetherian/Artinian Rings

**Definition 3.78.** Let  $R$  be a ring and  $M$  a left  $R$ -module. We say  $M$  is **left Noetherian** if every ascending chain of left  $R$ -submodules of  $M$  stabilizes, that is, if  $M_0 \subseteq M_1 \subseteq \dots$  is an ascending chain of left  $R$ -submodules, then there exists  $n$  such that  $M_n = M_{n+1} = M_{n+2} = \dots$ . Say  $M$  is **left Artinian** if every descending chain of left  $R$ -modules of  $M$  stabilizes. Say  $R$  is a **left Noetherian/Artinian ring** if  $R$  is left Noetherian/Artinian as an  $R$ -module. Say  $R$  is **Noetherian/Artinian** if it is both left and right Noetherian/Artinian.

**Remarks.**

1. Every division ring (and thus every field) is both Noetherian and Artinian (since the only ideals are 0 and 1).
2. Let  $R$  be a ring and  $D \subseteq R$  a division ring. Suppose  $R$  is finite dimensional as a  $D$ -module. Then  $R$  is Noetherian and Artinian. (The length of every proper ascending/descending chain of  $D$ -submodules over  $R$  is bounded by  $\dim_D R$ .)
3. Any PID is Noetherian (but not necessarily Artinian). For example  $\mathbb{Z}$  is not Artinian as  $(2) \subsetneq (4) \subsetneq (8) \subsetneq \dots$  does not stabilize.

**Example.** Let  $R = M_n(k)$ , where  $k$  is a field. Then  $\dim_k R = n^2$ . So  $R$  is Noetherian and Artinian.

**Theorem 3.79 (Hilbert Basis Theorem).** Let  $R$  be a commutative Noetherian ring. Then  $R[x]$  is Noetherian.

**Corollary 3.80.** If  $R$  is a commutative Noetherian ring, then  $R[x_1, \dots, x_n]$  is Noetherian.

**Fact.** Any left Artinian ring is left Noetherian. (We will prove this later, once we build up more machinery).

The fact is not true for modules. Let  $R = \mathbb{Z}_{(2)} \subseteq \mathbb{Q}$ . Note that every element of  $\mathbb{Q}$  can be expressed uniquely as  $u2^\ell$  for some  $u \in R$  which is a unit and  $\ell \in \mathbb{Z}$ .

Claim: The only  $R$ -submodules of  $\mathbb{Q}$  are  $N_\ell = R2^\ell$  for  $\ell \in \mathbb{Z}$  and  $0, \mathbb{Q}$ .

Proof: First note

- $\dots \supseteq N_{\ell-1} \supseteq N_\ell \supseteq N_{\ell+1} \supseteq \dots$
- $\cup_\ell N_\ell = \mathbb{Q}$ .

Now, let  $N$  be an  $R$ -submodule of  $\mathbb{Q}$  such that  $N \neq 0, \mathbb{Q}$ . Choose smallest  $\ell$  such that  $N_\ell \subseteq N$  (such an  $\ell$  exists as  $N_\ell \subsetneq N_{\ell-1} \subsetneq \dots$ ).

Subclaim:  $N = N_\ell$ .

Proof: Choose  $n \in N$ . Then  $n = u2^r$ . Note that  $r \geq \ell$  as otherwise  $2^r \in N$  which implies  $N_r \subseteq N$ . Then  $n = u2^r = u2^{r-\ell}2^\ell$  and since  $u2^{r-\ell} \in R$ , we see  $n \in N_\ell$ .

Now, let  $M = \mathbb{Q}/N_0 = \mathbb{Q}/R$ . Then the  $R$ -submodules of  $M$  are

$$M \supseteq \dots \supseteq N_\ell/R \supseteq N_{\ell-1}/R \supseteq \dots \supseteq N_0/R = 0.$$

Clearly,  $M$  satisfies DCC on  $R$ -submodules, but not ACC.

**Proposition 3.81.** Let  $R$  be a ring and  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  a short exact sequence of left  $R$ -modules. Then  $B$  is left Noetherian (resp Artinian) if and only if  $A$  and  $C$  are.

*Proof.* We will prove for Noetherian modules. The proof for Artinian is similar. WLOG, we may assume  $A \subseteq B$  and  $C = B/A$ . Now, the forward direction is clear. To prove the backward direction, let  $B_1 \subseteq B_2 \subseteq \dots$  be an ascending chain in  $B$ . Consider the chains  $(*)B_1 + A \subseteq B_2 + A \subseteq \dots$  and  $(**)B_1 \cap A \subseteq B_2 \cap A \subseteq \dots$ . As  $A$  is Noetherian,  $(**)$  stabilizes. Since  $B/A$  is Noetherian, we can mod  $(*)$  by  $A$  and that also stabilizes. Thus there exists  $n$  such that  $B_n + A = B_{n+1} + A = \dots$  and  $B_n \cap A = B_{n+1} \cap A = \dots$ .

Claim:  $B_n = B_{n+1} = \dots$ .

Proof: Let  $b \in B_{n+1} \subseteq B_{n+1} + A = B_n + A$ . Say  $b = b_n + a$  for  $b_n \in B_n$  and  $a \in A$ . Now,  $b - b_n = a \in A \cap B_{n+1} = A \cap B_n$ . So  $b - b_n \in B_n$  which implies  $b \in B_n$ .  $\square$

**Corollary 3.82.** *A left  $R$ -module  $M$  is left Noetherian (resp. Artinian) if and only if  $M^n = \bigoplus_{i=1}^n M$  is left Noetherian (resp. Artinian). In particular, if  $R$  is a left Noetherian (resp. Artinian) ring, then so is  $R^n$  for all  $n \geq 1$ .*

*Proof.* The backwards direction is clear. For the forward direction, use induction and the fact that  $0 \rightarrow M \rightarrow M + M \rightarrow M \rightarrow 0$  is a short exact sequence.  $\square$

**Corollary 3.83.** *If  $R$  is a left Noetherian (resp. Artinian) ring and  $M$  a finitely generated left  $R$ -module, then  $M$  is left Noetherian (resp. Artinian).*

*Proof.* Since  $M$  is finitely generated,  $M = Rx_1 + \dots + Rx_n$  which induces the short exact sequences  $0 \rightarrow \ker \phi \rightarrow R^n \xrightarrow{\phi} M \rightarrow 0$  where  $\phi: e_i \mapsto x_i$ . Apply previous corollary.  $\square$

**Proposition 3.84.** *Let  $M$  be a left  $R$ -module. TFAE*

1.  $M$  is left Noetherian (resp. Artinian).
2. Every set of  $R$ -submodules of  $M$  has a maximal (resp. minimal) element.

*For Noetherian only, these are equivalent to*

3. Every  $R$ -submodule of  $M$  is finitely generated.

*Proof.* Note that  $1 \Leftrightarrow 2$  is clear.

$2 \Rightarrow 3$  Let  $A$  be a submodule of  $M$  and  $\Lambda = \{N \mid N \text{ is a f.g. } R\text{-submodule of } A\}$ . Let  $M'$  be maximal in  $\Lambda$ . If  $M' \neq A$ , choose  $x \in A \setminus M'$ . Then  $M' \subsetneq M' + Rx$ , a finitely generated submodule of  $A$ , a contradiction. Thus  $A = M'$  is finitely generated.

$3 \Rightarrow 1$  Let  $M_1 \subseteq M_2 \subseteq \dots$  be an ascending chain. Let  $N = \bigcup_{i=1}^{\infty} M_i$ . Then  $N$  is an  $R$ -submodule (as the  $M_i$  are nested), which implies  $N$  is finitely generated. Say  $N = Rx_1 + \dots + Rx_n$ . Choose  $\ell$  large enough so that  $x_i \in M_\ell$  for all  $i$ . Then  $N \subseteq M_\ell \subseteq M_{\ell+1} \subseteq \dots \subseteq N$ .  $\square$

**Corollary 3.85.** *Let  $\phi: R \rightarrow S$  be a ring homomorphism. Suppose  $S$  is a finitely generated left  $R$ -module. If  $R$  is left Noetherian (resp. Artinian), then so is  $S$ .*

*Proof.* By the above corollary,  $S$  is Noetherian (resp. Artinian) as a left  $R$ -module. Every left ideal of  $S$  is a left  $R$ -module. Therefore  $S$  satisfies ACC (resp. DCC) on left ideals.  $\square$

**Remark.** If  $S$  is a finite dimensional  $k$ -algebra (for a division ring  $k$ ), then  $S$  is both Noetherian and Artinian (as it satisfies ACC and DCC).

**Example.**  $k[x]/(x^n)$  (this is Artinian, but not a field) and  $M_n(k)$  are Noetherian and Artinian by the above remark.

**Remarks.**

1. If  $R$  is Noetherian (resp. Artinian) and  $I$  is an ideal of  $R$ , then  $R/I$  is Noetherian (resp. Artinian) (as  $R/I$  is a finitely generated  $R$ -module, generated by  $\bar{1}$ .)
2. Let  $R$  be a ring,  $S \subseteq Z(R)$  a mcs of  $R$ . If  $R$  is Noetherian (resp. Artinian), then so is  $R_S$ .
3. Let  $R, S$  be commutative rings and suppose  $S$  is a finitely generated  $R$ -algebra. Then  $R$  Noetherian implies  $S$  is Noetherian.

*Proof.* WLOG, assume  $R \subseteq S$ . So say  $S = R[u_1, \dots, u_n]$  for  $u_i \in S$ . Define a ring homomorphism  $\phi : R[x_1, \dots, x_n] \rightarrow S$  by  $x_i \mapsto u_i$ . This is surjective and so  $S \cong R[x_1, \dots, x_n]/\ker \phi$ . By the Hilbert Basis Theorem and Remark 1,  $S$  is Noetherian.  $\square$

Note that this is not true for Artinian rings. For example, the division ring  $k$  is Artinian but  $k[x]$  is not as  $(x) \supseteq (x^2) \supseteq \dots$ .

4. Subrings of Noetherian rings are *not* necessarily Noetherian. For example  $R = \mathbb{Q}[x, y]$  is Noetherian, but  $S = \mathbb{Q}[x, xy, xy^2, \dots] \subseteq R$  is not.

**Examples.**

1.  $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$  is right Noetherian, but not left Noetherian.
2.  $S = \left\{ \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} \mid r \in \mathbb{Q}, s, t \in \mathbb{R} \right\}$  is right Artinian, but not left Artinian.

**Definition 3.86.** A left  $R$ -module  $M$  is **simple** or **irreducible** if  $M \neq 0$  and has no submodules other than  $0$  and  $M$ .

**Proposition 3.87.** Let  $M$  be an  $R$ -module. TFAE

1.  $M$  is simple.
2.  $M = Rx$  for all  $x \in M \setminus \{0\}$ .
3.  $M \cong R/I$  where  $I$  is a maximal left ideal.

*Proof.*  $1 \Leftrightarrow 2$   $Rx \neq 0$  is a submodule of  $M$ .

$3 \Rightarrow 1$  Any submodule of  $M$  corresponds to  $R/J$  where  $I \subseteq J$ . Since  $I$  is maximal, done.

$2 \Rightarrow 3$  Define  $\phi : R \rightarrow Rx = M$  by  $r \mapsto rx$ . So  $M \cong R/\ker \phi$  where  $\ker \phi$  is a left ideal. Since  $M$  has only 2 submodules,  $\ker \phi$  must be maximal.  $\square$

**Definition 3.88.** Let  $M$  be an  $R$ -module. A **normal series** for  $M$  is a finite chain of submodules  $(*)M = M_0 \supseteq M_1 \supseteq \dots \supseteq M_n = (0)$ . The **factors** of  $(*)$  are  $M_i/M_{i+1}$  for  $i = 0, \dots, n-1$ . The **length** of  $(*)$  is the number of nonzero factors. We say two normal series are **equivalent** if there exists a bijection between the nonzero factors of the two series such that the corresponding factors are isomorphic. In particular, two equivalent normal series for  $M$  have the same length. A **composition series** is a normal series for  $M$  such that all nontrivial factors are simple. A **refinement** of  $(*)$  is a normal series obtained by inserting additional modules between two links in the chain. A **proper refinement** is a refinement which has length larger than the original normal series.

**Note.** A composition series has no proper refinements.

**Theorem 3.89 (Jordan-Hölder Theorem).** Any two normal series for  $M$  have equivalent refinements.

**Corollary 3.90.** Suppose  $M$  has a composition series. Then any normal series has a refinement which is equivalent to the given composition series. Therefore, any normal series has length less than the length of a given composition series. In particular, any two composition series are equivalent and have the same length.

**Definition 3.91.** If  $M$  has a composition series, define the **length of  $M$**  (denoted  $\lambda_R(M)$ ) as the length of any composition series for  $M$ . If  $M$  does not have a composition series, we say it has infinite length.

**Proposition 3.92.**  $\lambda_R(M) < \infty$  if and only if  $M$  is both Noetherian and Artinian.

*Proof.*  $\Rightarrow$   $\lambda_R(M)$  is a bound on the length of any chain. Thus any chain must stabilize.

$\Leftarrow$  Let  $M_0 = M$ . Let  $\Lambda = \{N \mid N \subsetneq M \text{ is a submodule}\}$ . As  $M$  is Noetherian,  $\Lambda$  has a maximal element, call it  $M_1$ . Then,  $M_1 \subsetneq M_0$  and  $M/M_1$  is simple. If  $M_1 \neq 0$ , repeat. In this way, we get a descending chain  $M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$  which must terminate as  $M$  is Artinian, that is, there exists  $M_n = 0$ . This is a composition series.  $\square$

**Definition 3.93.** A ring has finite (**left**) **length** if  $\lambda_R(R) < \infty$ .

**Examples.**

1.  $\lambda_R(k) < \infty$  for a division ring  $k$ . (In this case, the length is the dimension).
2. Let  $R = M_N(k)$  for a division ring  $k$ . Then  $\lambda_R(R) < \infty$ .
3. Let  $R = k[x]$ . Then  $\lambda_R(R) = \infty$ .

**Proposition 3.94.** Suppose  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  is a short exact sequence. Then  $\lambda_R(B) = \lambda_R(A) + \lambda_R(C)$ .

*Proof.* By the previous proposition, we may assume  $\lambda_R(B), \lambda_R(A), \lambda_R(C) < \infty$ . Induct on  $\lambda_R(B)$ . If  $\lambda_R(B) = 1$ , then  $B$  is simple. Since  $A \hookrightarrow B$ , either  $A = B$  (and  $C = 0$ ) or  $A = 0$  (and  $C = B$ ). In either case, the equality holds. Otherwise, assume  $C = B/A$  and consider the normal series  $B \supseteq A \supseteq (0)$ . We may refine this series to get a composition series  $B \supsetneq B_1 \supsetneq \cdots \supsetneq B_{n-1} \supsetneq B_n = (0)$ . Then  $A \supseteq B_{n-1}$ . Consider  $0 \rightarrow A/B_{n-1} \rightarrow B/B_{n-1} \rightarrow B/A \rightarrow 0$ . By induction, since  $\lambda_R(B/B_{n-1}) = \lambda_R(B) - 1$ , we see  $\lambda_R(B/B_{n-1}) = \lambda_R(A/B_{n-1}) + \lambda_R(B/A)$ . Of course,  $\lambda_R(A/B_{n-1}) = \lambda_R(A) - 1$  and thus  $\lambda_R(B) = \lambda_R(A) + \lambda_R(C)$ .  $\square$

**Definition 3.95.** Let  $R$  be a ring and  $M$  a left  $R$ -module.  $M$  is **completely reducible** or **semisimple** if  $M$  is a direct sum of a family of simple submodules.  $R$  is left **semisimple** if it is as an  $R$ -module.

**Proposition 3.96.** Let  $M$  be an  $R$ -module. TFAE

1.  $M$  is semisimple.
2.  $M$  is a sum of a family of simple submodules.
3. Every submodule of  $M$  is a direct summand of  $M$ .

*Proof.*  $1 \Rightarrow 2$  Trivial, as the direct sum is a sum.

$2 \Rightarrow 3$  Given  $M = \sum_{i \in I} M_i$ , where  $M_i$  is simple, let  $N$  be a submodule of  $M$ . Let  $\Lambda = \{J \subseteq I \mid N + \sum_{j \in J} M_j = N \oplus (\oplus_{j \in J} M_j)\}$ . Since  $N \neq M$ , there exists  $M_i$  such that  $M_i \not\subseteq N$ . Then  $N \cap M_i \subseteq M_i$  implies  $N \cap M_i = \emptyset$ . Thus  $\Lambda \neq \emptyset$ . By Zorn's Lemma, there exists a maximal element  $J \in \Lambda$ . Let  $F = \oplus_{j \in J} M_j$ .

Claim:  $N \oplus F = M$ .

Proof: Note  $N \cap F = (0)$  by choice of  $J$ . Suppose  $N \oplus F \neq M$ . Then there exists  $i$  such that  $M_i \not\subseteq N \oplus F$ . Note  $M_i \cap (N \oplus F) = (0)$  or  $M_i$  as  $M_i$  is simple. Since  $M_i \not\subseteq N \oplus F$ ,  $M_i \cap (N \oplus F) = (0)$ . Hence  $N + F + M_i = N \oplus F \oplus M_i$ , a contradiction to the maximality of  $J$ . Thus  $N \oplus F = M$ .

$3 \Rightarrow 1$  First, we need a claim.

Claim: Assuming  $M$  satisfies (3), every nonzero submodule of  $M$  contains a simple submodule.

Proof: Let  $N \neq 0$  be a submodule of  $M$ . WLOG, assume  $N$  is cyclic, that is  $N = Rx$  for  $x \in M \setminus \{0\}$ . Then  $N \cong R/I$  where  $I = \text{Ann}(x)$ . Note  $I \neq R$  as  $N \neq 0$ . Thus  $I \subseteq m$  where  $m$  is a maximal left ideal. Then  $m/I$  is a maximal proper submodule of  $R/I \cong N$ . Thus  $N$  has a maximal proper submodule  $N'$  and so  $N/N'$  is simple. By (3),  $M = N' \oplus F$  for some  $F \subseteq M$ . Note  $N = N' \oplus (F \cap N)$ . Thus  $F \cap N \cong N/N'$ , which is simple. Thus  $F \cap N$  is a simple submodule of  $M$ .

Let  $T = \{E \mid E \subseteq M \text{ is simple}\}$ . Let  $\Lambda = \{J \subseteq T \mid \sum_{E \in J} E = \oplus_{E \in J} E\}$ . By Zorn's Lemma, there exists a maximal element  $J \in \Lambda$ .

Claim:  $M = \bigoplus_{E \in J} E$ .

Proof: If not, let  $M' = \bigoplus_{E \in J} E$ . By (3),  $M = M' \oplus F$  where  $F \subseteq M$ . Since  $F \neq 0$  as  $M \neq M'$ ,  $F$  contains a simple submodule  $E' \in T$ . Then  $J \cup E' \in \Lambda$ , a contradiction to maximality.  $\square$

**Corollary 3.97.** *Submodules, quotients, and (direct)sums of semisimple modules are semisimple.*

*Proof.* • Let  $M$  be semisimple and  $N \subseteq M$  a submodule. Let  $N'$  be the sum of all simple submodules of  $N$ .

Claim:  $N = N'$ .

Proof: By 3 of the proposition, there exists  $F \subseteq M$  such that  $M = N' \oplus F$ . So  $N = N' \oplus (F \cap N)$ . If  $F \cap N \neq (0)$ , it contains a simple submodule  $E$ . Then  $E \subseteq N'$ , a contradiction as  $M = N' \oplus F$ . Thus  $F \cap N = 0$  and  $N = N'$ .

- For quotients, say  $M/N$ , we know  $M/N \cong F$  where  $M = N \oplus F$ . Done by previous bullet point.
- Suppose  $\{M_i\}_{i \in I}$  is a family of semisimple submodules. Then  $M_i = \bigoplus_{j \in J_i} E_{i_j}$ ,  $E_{i_j}$  is simple. Then  $\bigoplus_{i \in I} M_i = \bigoplus_{i \in I, j \in J_i} E_{i_j}$  is semisimple.  $\square$

**Proposition 3.98.** *If  $R$  is semisimple, every  $R$ -module is semisimple.*

*Proof.*  $R$  semisimple implies every free module is semisimple which implies quotients of free modules are semisimple which implies all modules are semisimple.  $\square$

**Examples.**

- Division Rings are Semisimple.
- Let  $R_1, \dots, R_t$  be rings so that  $S = R_1 \times \dots \times R_t$  is a ring. The left ideals of  $S$  are of the form  $I_1 \times \dots \times I_t$  where  $I_i$  is a left ideal of  $R_i$ . Consequently,  $S$  is left Noetherian/Artinian/has finite length/is semisimple if and only if each  $R_i$  has the corresponding property.
- Let  $G$  be a finite group and  $k$  a field such that  $\text{char } k \nmid |G|$ . Then  $R = k[G]$  is semisimple.

*Proof.* Let  $I$  be a left ideal of  $R$ . So  $I$  is a  $k$ -subspace of  $R$ . Let  $\Pi : R \rightarrow I$  be a projection onto  $I$  as  $k$ -vector spaces, that is,  $\Pi$  is  $k$ -linear and  $\Pi(i) = i$  for all  $i \in I$ . Define  $\tilde{\Pi} = \frac{1}{|G|} \sum_{g \in G} g \Pi g^{-1}$ .

Claim:  $\tilde{\Pi}$  is  $R$ -linear.

Proof: It suffices to show  $\tilde{\Pi}(hr) = h\tilde{\Pi}(r)$  for all  $r \in R, h \in G$ . Notice

$$\begin{aligned} \tilde{\Pi}(hr) &= \frac{1}{|G|} \sum_{g \in G} g \Pi g^{-1}(hr) \\ &= \frac{1}{|G|} \sum_{hg \in G} (hg) \Pi (hg)^{-1} hr \\ &= \frac{1}{|G|} \sum_{g \in G} hg \Pi g^{-1} h^{-1} hr \\ &= \frac{1}{|G|} \sum_{g \in G} hg \Pi g^{-1}(r) = h\tilde{\Pi}(r). \end{aligned}$$

Note that if  $i \in I$ , then

$$\tilde{\Pi}(i) = \frac{1}{|G|} \sum_{g \in G} g \Pi g^{-1}(i) = \frac{1}{|G|} \sum_{g \in G} gg^{-1}(i) = i$$

as  $g^{-1}(i) \in I$ . This gives rise to the short exact sequence  $0 \rightarrow I \hookrightarrow R \rightarrow R/I \rightarrow 0$  with splitting map  $\tilde{\Pi} : R \rightarrow I$ . Thus  $R \cong I \oplus R/I$ . Thus every submodule of  $R$  is a direct summand of  $R$  which implies  $R$  is semisimple.  $\square$

Let  $M$  be a left  $R$ -module. Let  $\text{End}_R(M) = \text{Hom}_R(M, M)$ . Note  $\text{End}_R(M)$  is a ring under composition. If  $R$  is commutative and  $F = R^n$ , then  $\text{End}_R(F) \cong M_n(R)$ . This is not true if  $R$  is noncommutative.

**Definition 3.99.** *Let  $R$  be a ring. Define the **opposite ring**  $R^{op}$  by  $R^{op} = R$  as abelian groups with multiplication in  $R^{op}$  defined by  $r \cdot s := sr$ .*

**Claim.**  $\text{End}_R(R) \cong R^{\text{op}}$  as rings.

*Proof.* Let  $a \in R$ . Define  $f_a : R \rightarrow R$  by  $r \mapsto ra$ . Then  $f_a \in \text{End}_R(R)$ . Furthermore, if  $g \in \text{End}_R(R)$ , then  $g = f_a$  where  $a = g(1)$ . Observe  $(f_a \circ f_b)(r) = f_a(rb) = rba = f_{ba}(r)$ . Now define  $\phi : \text{End}_R R \rightarrow R^{\text{op}}$  by  $f_a \mapsto a$ .  $\square$

**Note.** If  $R$  is a division ring, so is  $R^{\text{op}}$ . It is easily shown that if  $F \cong R^n$  as left  $R$ -modules, then  $\text{End}_R(F) \cong M_n(R^{\text{op}})$ .

**Proposition 3.100.** *Let  $D$  be a division ring,  $M$  a finitely generated  $D$ -module. Then  $\text{End}_D(M)$  is semisimple.*

*Proof.* As a  $D$ -module,  $M \cong D^n$  for some  $n$ . Thus  $\text{End}_D(M) \cong M_n(D^{\text{op}})$ . Since  $D^{\text{op}}$  is a division ring, it is enough to show  $M_n(D)$  is semisimple where  $D$  is a division ring. Let  $e_i$  be the matrix with a 1 in the  $i, i^{\text{th}}$ -position and zeros elsewhere. Then  $M_n(D)e_i$  is the ring with a nonzero  $i^{\text{th}}$  column and zeros elsewhere. This is simple by Exam 1. Thus  $M_n(D) \cong M_n(D)e_1 \oplus \cdots \oplus M_n(D)e_n$ , a direct sum of simple modules. Then  $M_n(D)$  is semisimple.  $\square$

**Corollary 3.101.** *Let  $D_1, \dots, D_k$  be division rings,  $n_1, \dots, n_k \in \mathbb{N}$ . Then  $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$  is semisimple.*

**Note.** These rings are left and right Artinian/Noetherian and also right semisimple.

**Proposition 3.102.** *Let  $R$  be a semisimple ring. Then  $\lambda_R(R) < \infty$ . Thus  $R$  is left/right Artinian/Noetherian.*

*Proof.* As  $R$  is semisimple,  $R = \bigoplus_{\alpha \in \Lambda} I_\alpha$ , where  $I_\alpha$  are simple left ideals. Then  $1 = e_{\alpha_1} + \dots + e_{\alpha_k}$  where  $e_{\alpha_i} \in I_{\alpha_i} \setminus \{0\}$  and  $\alpha_1, \dots, \alpha_k \in \Lambda$ .

Claim:  $R = I_{\alpha_1} \oplus \cdots \oplus I_{\alpha_k} \in \Lambda$ .

Proof: Suppose there exists  $\alpha \in \Lambda$  such that  $I_\alpha \neq I_{\alpha_i}$  for  $i = 1, \dots, k$ . Then for  $r \in I_\alpha$ ,  $r = re_{\alpha_1} + \dots + re_{\alpha_k}$  where  $re_{\alpha_i} \in I_{\alpha_i}$  which implies  $r \in I_\alpha \cap (\sum I_{\alpha_i})$ , a contradiction as  $R$  is the direct sum of  $I_\alpha$ 's.

Relabel  $I_{\alpha_i}$  as  $I_i$  for simplicity. Let  $M_i = I_1 \oplus \cdots \oplus I_i$ . Then  $M_i/M_{i-1} = I_i$ , which is simple. Thus  $0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k = R$  is a composition series. Thus  $\lambda_R(R) = k < \infty$ .  $\square$

**Proposition 3.103.** *Let  $R$  be a semisimple ring. Then*

1. *Every simple left  $R$ -module is isomorphic to a simple left ideal.*
2. *There are only finitely many distinct simple left  $R$ -modules up to isomorphism.*

*Proof.* Let  $R = I_1 \oplus \cdots \oplus I_k$ ,  $I_i$  are simple as in the previous proposition. Let  $J$  be a simple left ideal. Then the normal series  $0 \subseteq J \subseteq R$  can be refined to a composition series for  $R$ . Then  $J$  is a factor of the composition series for  $R$  which says  $J \cong I_i$  for some  $i$  by the Jordan-Hölder Theorem. Thus there are only finitely many distinct simple left ideals. Thus it suffices to prove (1). Let  $M$  be a simple left  $R$ -module. Let  $x \in M \setminus \{0\}$ . Then  $Rx$  is a nonzero submodule of  $M$  which implies  $M = Rx$ . Thus  $M$  is cyclic and we have the sequence  $0 \rightarrow \ker \phi \rightarrow R \xrightarrow{\phi} M \rightarrow 0$  where  $\phi(r) = rx$  is exact. As  $\ker \phi$  is a left ideal of  $R$ ,  $\ker \phi$  is a direct summand of  $R$  by definition of semisimple. Thus the sequence splits and thus there exists a splitting map  $\psi : M \rightarrow R$  such that  $\phi\psi = 1_M$ . Then  $\psi$  is injective and  $M$  is isomorphic to a simple left ideal of  $R$ .  $\square$

**Definition 3.104.** *A ring is **simple** if the only two sided ideals of  $R$  are  $(0)$  and  $R$ . Note: Simple rings are not necessarily semisimple (this differs from Lang's definition).*

**Note.** An Artinian simple ring is semisimple.

**Lemma 3.105.** *Let  $R$  be a ring,  $I$  a simple left ideal,  $M$  a simple left  $R$ -module. If  $I \not\cong M$ , then  $IM = 0$ .*

*Proof.* Suppose  $IM \neq 0$ . Then there exists  $e \in M$  such that  $Ie \neq 0$ . Now  $Ie \subseteq M$  is a left  $R$ -module. Since  $M$  is simple,  $Ie = M$ . Define  $\phi : I \rightarrow M$  by  $i \mapsto ie$ . This is a left  $R$ -module homomorphism. Since  $Ie = M$ ,  $\phi$  is surjective. Also,  $\ker \phi \neq I$  as  $\phi \neq 0$  and so  $\ker \phi = \{0\}$  as  $I$  is simple. Thus  $\phi$  is an isomorphism.  $\square$

**Theorem 3.106.** Let  $R$  be semisimple,  $\{I_1, \dots, I_k\}$  the set of all distinct left  $R$ -modules. Let  $R_i = \sum_I \text{left ideal} \cong_{I_i} I$ . Then

1.  $R_i$  is a ring with identity.
2.  $R_i$  is semisimple with only 1 distinct simple module.
3.  $R_i$  is a simple ring.
4.  $R \cong R_1 \times \dots \times R_k$  as rings.

*Proof.* By the Lemma,  $R_i R_j = 0$  for all  $i \neq j$ . Note  $R = R_1 + \dots + R_k$  and  $R_j \subseteq R_j R = R_j(R_1 + \dots + R_k) = R_j^2 \subseteq R_j$ . Hence  $R_j = R_j R$ . Thus  $R_j$  is a two sided ideal. Write  $1 = e_1 + \dots + e_k$  for  $e_i \in R_i$ . Let  $x \in R$ . We can write  $x = x_1 + \dots + x_k$  for  $x_i \in R_i$ . Note  $x_i = x_i \cdot 1 = x_i(e_1 + \dots + e_k) = x_i e_i = (x_1 + \dots + x_k)e_i = x e_i$  and similarly  $x_i = e_i x$ . Thus  $x_i$  is uniquely determined by  $x$  which implies  $R = \oplus R_i$ . Also, if  $x \in R_i$ , then  $x = x e_i = e_i x$  implies that  $e_i$  is the identity on  $R_i$ . Thus  $R_i$  is a ring with identity. Its easy to show  $R \cong R_1 \times \dots \times R_k$  by mapping  $r \mapsto (r_1, \dots, r_k)$ . Now, note that if  $J$  is a left ideal of  $R_i$  then  $RJ = (R_1 + \dots + R_k)J = R_i J = J$ . So  $J$  is a left ideal of  $R$  contained in  $R_i$ . Conversely, if  $J \subseteq R_i$  is an ideal of  $R$ , then  $J$  is an ideal of  $R_i$ . Thus the left ideals of  $R_i$  are exactly the left ideals of  $R$  contained in  $R_i$ . Thus  $R_i = \sum I$  (where  $I$  are in fact simple ideals of  $R_i$ ) which implies  $R_i$  is semisimple. Also, every simple left ideal of  $R_i$  is isomorphic to  $I_i$ .

Let  $J \neq 0$  be a two sided ideal of  $R_i$ . Then  $J$  is a left ideal of  $R$  which implies  $J$  contains a simple left ideal  $I$  of  $R$ . Since  $J \subseteq R_i$ , this says  $I \cong I_i$ . Let  $K$  be a left ideal of  $R$  such that  $K \cong I$ . Then  $K \cong I_i$  which implies  $K \subseteq R_i$ .

Claim:  $K \subseteq J$ .

Proof: As  $R$  is semisimple, there exists a left ideal  $I'$  such that  $I \oplus I' = R$ . Then  $1 = e + e'$  for  $e \in I, e' \in I'$  where  $e \neq 0$ . Then  $e = e^2 + ee'$ . Since  $I \cap I' = (0)$ , we have  $e = e^2$  and thus  $Ie \neq 0$ . As  $Ie \subseteq I$  and  $I$  is simple, this says  $I = Ie$ . Let  $\phi : I \rightarrow K$  be a left  $R$ -module isomorphism. Then  $K = \phi(I) = \phi(Ie) = I\phi(e) \subseteq J\phi(e) \subseteq J$  as  $J$  is two sided.

Since  $K$  was arbitrary, this says  $J \supseteq R_i$  which implies  $J = R_i$ . □

**Corollary 3.107.** Let  $R$  be a semisimple ring. TFAE

1.  $R$  is simple.
2. There exists a unique left simple ideal up to isomorphism.

**Example.** Let  $D$  be a division ring and  $n \geq 1$ . Then  $M_n(D)$  is simple and semisimple.

*Proof.* Let  $R = M_n(D)$  and  $e_i$  be the matrix with a 1 in the  $i, i$ -spot and zeroes elsewhere. Then  $R = Re_1 \oplus \dots \oplus Re_n$ , where  $Re_i$  are simple left ideals and  $\phi : Re_i \rightarrow Re_j$  defined by  $re_i \mapsto re_i E_{ij}$  is an isomorphism. Then  $R$  has a unique maximal simple left ideal. Thus  $R$  is simple. □

**Notation.** Let  $R$  be a ring and  $E$  an  $R$ -module. Let  $R'(E) = \text{End}_R(E)$ . If  $a \in R$ , define  $r_a : E \rightarrow E$  by  $e \mapsto ea$ . Then  $r_a \in R'(E)$ . Let  $R''(E) = \text{End}_{R'}(E)$ . (Note that if  $E$  is an  $R'$ -module, then for  $\phi \in R', e \in E$ , we can define  $\phi e := \phi(e)$ ). For  $a \in R$ , define  $\ell_a : E \rightarrow E$  by  $e \mapsto ae$ .

Claim:  $\ell_a \in R''(E)$ .

Proof: Let  $f \in R', e \in E$ . Then  $f\ell_a(e) = f(ae) = af(e) = \ell_a(f(e))$ .

This gives yield to the natural homomorphism  $\lambda : R \rightarrow R''(E)$  defined by  $a \mapsto \ell_a$ . Note that  $\lambda$  is injective if and only if  $\ell_a \neq 0$  for all  $a \in R \setminus \{0\}$  which is if and only if  $\text{ann}_R(E) = (0)$  (that is,  $E$  is a **faithful**  $R$ -module).

**Schur's Lemma:** Let  $R$  be a ring and  $E$  a simple  $R$ -module. Then  $R'(E)$  is a division ring.

*Proof.* Let  $\phi \in R'(E) \setminus \{0\}$ . It is enough to show  $\phi$  is an isomorphism. Of course,  $\ker \phi$  is a submodule of  $E$  (which is simple) and since  $\phi \neq 0$  we have  $\ker \phi \neq E$  and so  $\ker \phi = (0)$ . Similarly,  $\text{im} \phi$  is a submodule of  $E$  and since  $\phi \neq (0)$  we have  $\text{im} \phi = E$ . □

**Theorem 3.108.** *Let  $R$  be a simple ring and  $I \neq (0)$  a left ideal. Then  $\lambda : R \rightarrow R''(I)$  is an isomorphism.*

*Proof.* (Rieffel) Since  $\ker \lambda$  is a two sided ideal and  $R$  is simple,  $\ker \lambda = 0$  or  $R$ . Since  $1 \mapsto \ell_1$ , which is clearly not zero, we see  $\ker \lambda = 0$ . Thus  $\lambda$  is injective. Note that  $IR \neq (0)$  is a two sided ideal of  $R$ . Thus  $IR = R$ . Then  $\{\sum \lambda(i_k)\lambda(r_k) | i_k \in I, r_k \in R\} = \lambda(I)\lambda(R) = \lambda(IR) = \lambda(R)$ .

Claim:  $\lambda(I)$  is a left ideal of  $R''$ .

*Proof:* Let  $f \in R''$ ,  $\ell_a \in \lambda(I)$  where  $a \in I$ . Let  $i \in I$ . Then  $f\ell_a(i) = f(ai) = f(r_i(a)) = r_i(f(a)) = f(a)i = \ell_{f(a)}(i)$ . Thus  $f\ell_a = \ell_{f(a)} \in \lambda(I)$  as  $f(a) \in I$ .

Now,  $\underbrace{R'' = R''\lambda(R)}_{\text{since } 1 = \ell_1 \in \lambda(R)} = R''\lambda(I)\lambda(R) = \lambda(I)\lambda(R) = \lambda(R)$ . Thus  $\lambda$  is onto. □

**Theorem 3.109** (Artin-Wedderburn). *Let  $R$  be a simple ring. TFAE*

1.  $R$  is semisimple.
2.  $R$  is left Artinian.
3.  $R \cong M_n(D)$ ,  $n \in \mathbb{N}$ ,  $D$  a division ring.

*Proof.*  $3 \Rightarrow 1 \Rightarrow 2$  already done.

$2 \Rightarrow 3$  Since a minimal nonzero left ideal is a simple left ideal and  $R$  is left Artinian, we see that there exists a simple left ideal, call it  $I$ . By the Theorem,  $\lambda : R \rightarrow R''(I) = \text{End}_{R'}(I)$  is an isomorphism. Since  $I$  is simple,  $R' = \text{End}_R(I)$  is a division ring by Schur's Lemma.

Claim:  $I$  is finitely generated as an  $R'$  module.

*Proof:* Suppose not. Then there exists an infinite set  $\{e_1, e_2, \dots\} \subseteq I$  which is linearly independent over  $R'$ . For each  $n \in \mathbb{N}$ , let  $J_n = \{f \in R''(I) | f(e_1) = \dots = f(e_n) = 0\}$ . Note  $J_n$  is a left ideal of  $R''$  and  $J_n \supsetneq J_{n+1}$  for all  $n$ . This says  $R'' \cong R$  is not left Artinian, a contradiction.

Thus  $I$  is finitely generated as an  $R'$ -module. So  $I \cong (R')^n$  for some  $n$ . Thus  $R'' = \text{End}_{R'}((R')^n) \cong M_n((R')^{op})$  as  $(R')^n$  is a free module. Let  $D = (R')^{op}$ , a division ring. □

**Corollary 3.110.** *Let  $R$  be a ring. TFAE*

1.  $R$  is semisimple.
2.  $R \cong M_{n_1}(D_1) \times \dots \times M_{n_\ell}(D_\ell)$  for  $n_i \in \mathbb{N}$ ,  $D_i$  division rings.

*Proof.*  $2 \Rightarrow 1$  Done, as products of semisimple rings are semisimple.

$1 \Rightarrow 2$   $R \cong R_1 \times \dots \times R_\ell$  where  $R_i$  are left Artinian simple rings. □

**Corollary 3.111.** *If  $R$  is semisimple, then  $R$  is left/right Artinian and left/right Noetherian. Also, left semisimple if and only if right semisimple.*

*Proof.* Clear as  $M_{n_1}(D_1) \times \dots \times M_{n_\ell}(D_\ell)$  are. □



**Notation.** Let  $R$  be a ring,  $E$  an  $R$ -module,  $R' = R'(E) = \text{End}_R(E)$  and  $R'' = R''(E) = \text{End}_{R'}(E)$ . Let  $E^n = \bigoplus_{i=1}^n E$  and  $E_i := 0 \oplus \cdots \oplus 0 \oplus E \oplus 0 \oplus \cdots \oplus 0$ . Let  $\pi_i : E^n \rightarrow E_i$  and  $\mu_i : E_i \rightarrow E^n$  be the natural maps. Let  $\psi \in \text{End}_R(E^n)$  and  $\psi_{ij} = \pi_i \psi \mu_j : E_j \rightarrow E_i$ . So  $\psi_{ij} \in \text{Hom}_R(E_j, E_i) \cong \text{End}_R(E) = R'$ . Thus we can represent  $\psi$  as a matrix  $(\psi_{ij})_{n \times n}$  where

$$\psi \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (\psi_{ji}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n \psi_{j1}(x_j) \\ \vdots \\ \sum_{j=1}^n \psi_{jn}(x_j) \end{pmatrix} \text{ for } \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in E^n.$$

Thus  $\text{End}_R(E^n) \cong M_n(\text{End}_R(E))$ , that is  $R'(E^n) \cong M_n(R')$ .

**Remark.** Let  $f \in R''(E)$ . So  $f : E \rightarrow E$  and  $f(\phi(x)) = \phi(f(x))$  for all  $\phi \in R', x \in E$ . Thus  $f\phi = \phi f$  for all  $\phi \in R'$ . Define  $f^{(n)} : E^n \rightarrow E^n$  by  $f^{(n)}(x_1, \dots, x_n) = (f(x_1), \dots, f(x_n))$ . As a matrix, this says  $f^{(n)} = fI_n$ . Let  $\psi \in R'(E^n)$ . Then  $(fI_n)(\psi_{ij}) = \psi_{ij}(fI_n)$  since  $f\psi_{ij} = \psi_{ij}f$  for all  $i, j$ . Thus  $f^{(n)}\psi = \psi f^{(n)}$  for all  $\psi \in R'(E^n)$ . Thus  $f^{(n)} \in R''(E^n)$  (its clearly additive and we just showed we can pull out elements from  $R'$ .) Therefore,

$$f \in R''(E) \Rightarrow f^{(n)} \in R''(E^n).$$

**Lemma 3.112.** Let  $R$  be a ring,  $E$  a semisimple  $R$ -module. Let  $f \in R''(E), x \in E$ . Then there exists  $\alpha \in R$  such that  $f(x) = \alpha x$  (note that  $\alpha$  depends on  $x$ ).

*Proof.* Fix  $x \in E$ . Since  $E$  is semisimple and  $Rx$  is a submodule of  $E$ , we have  $E = Rx \oplus F$  for some left submodule  $F$ . Define  $\pi : E \rightarrow E$  by  $rx + f \mapsto rx$  (the projection onto  $Rx$ ). So  $\pi \in R'$  and since  $\pi(x) = x$  we have  $f(x) = f(\pi(x)) = \pi(f(x)) \in Rx$ . □

**Theorem 3.113 (Jacobson Density Theorem).** Let  $R$  be a ring and  $E$  a semisimple left  $R$ -module. Let  $f \in R''(E)$  and  $x_1, \dots, x_n \in E$ . Then there exists  $\alpha \in R$  such that  $f(x_i) = \alpha x_i$  for all  $i \in [n]$ .

*Proof.* Let  $f^{(n)} : E^n \rightarrow E^n$  be as above and  $x = (x_1, \dots, x_n) \in E^n$ . By the remark,  $f^{(n)} \in R''(E^n)$  and  $E^n$  is semisimple. By the lemma, there exists  $\alpha \in R$  such that  $f^{(n)}(x) = \alpha x$  which implies  $f(x_i) = \alpha x_i$  for all  $i \in [n]$ . □

**Corollary 3.114.** If  $E$  is finitely generated over  $R'$ , then  $\lambda : R \rightarrow R''(E)$  defined by  $\alpha \mapsto \lambda_\alpha$  is surjective.

*Proof.* Let  $x_1, \dots, x_n$  be generators for  $E$  as an  $R'$ -module. If  $f \in R''$  and  $f(x_i) = \lambda_\alpha(x_i)$  for  $i \in [n]$ , then  $f = \lambda_\alpha$ . □

**Corollary 3.115.** Let  $R$  be a semisimple ring and  $E = R^n$  a left  $R$ -module. Then  $\lambda : R \rightarrow R''(E)$  defined by  $\alpha \mapsto \lambda_\alpha$  is an isomorphism.

*Proof.* As  $R$  is semisimple,  $E$  is. So  $\ker \lambda = \text{Ann}_R(E) = (0)$  as  $R^n$  is faithful (it's free!). Note that  $E$  is generated over  $R'$  by  $\{e_1\}$  (Let  $x \in E$ . As  $\{e_1\}$  is part of an  $R$ -basis for  $E$ , there exists an endomorphism  $\phi e_1 = \phi(e_1) = x$ . Thus  $R'e_1 = E$ ). By the previous corollary,  $\lambda$  is surjective. □

**Corollary 3.116.** Let  $D$  be a division ring and  $E$  a finitely generated  $D$ -module. Then  $D \cong \text{End}_{D'}(E)$ , that is,  $\lambda : D \rightarrow D''(E)$  is an isomorphism.

*Proof.*  $D$  is semisimple and  $E = D^n$  for some  $n$ . Done by previous corollary. □

In matrix notation, this says  $\text{End}_D(D^n) \cong M_n(D^{op}) =: D'$ . So  $D^n$  is an  $M_n(D^{op})$ -module. Then  $\text{End}_{D'}(D^n) = D$ .

**Corollary 3.117 (Wedderburn).** Let  $R$  be a finite dimensional  $k$ -algebra, where  $k$  is a field. Let  $E$  be a simple  $R$ -module. Then  $\lambda : R \rightarrow R''(E)$  is surjective. If, in addition, we have  $E$  is faithful, then  $\lambda$  is an isomorphism.

*Proof.* By the first corollary, it is enough to show  $E$  is finitely generated as an  $R'$ -module. Since  $E$  is simple,  $E = Rx$  for  $x \in E$ . So  $\dim_k E < \infty$ . Since  $k \subset Z(R)$ , we have  $k \hookrightarrow R'(E)$  via  $\alpha \mapsto \ell_\alpha$  ( $\ell_\alpha \in R'(E)$  as  $k$  is commutative). So  $E$  finitely generated over  $k$  implies  $E$  is finitely generated over  $R'$ .  $\square$

**Note.**  $E$  a finitely generated  $R$ -module does NOT imply  $E$  is a finitely generated  $R'(E)$ -module.

**Example.** Let  $A$  be the ring from Exam 1 #6.  $A$  is called the (first) Weyl algebra of  $F$  and is denoted  $A_1(F)$ . An equivalent definition for  $A$  is  $A_1(F) \cong F\{x, y\} / \langle xy - yx - 1 \rangle$  where  $F\{x, y\}$  is the free algebra generated by  $x, y$  (i.e.,  $x, y$  do not commute). Let  $I$  be a maximal left ideal of  $A$  and  $E = A/I$ . Then  $E$  is a simple  $A$ -module. Thus  $A'(E) = \text{End}_A(E)$  is a division ring (as  $E$  is simple). If  $E$  is finitely generated as an  $A'$ -module, then  $E \cong (A')^n$  and by the corollary,  $\lambda : A \rightarrow A''(E)$  would be surjective, where  $A''(E) = \text{End}_{A'}((A')^n) = M_n(A')$  is semisimple. Since  $A$  is simple,  $\ker \lambda = 0$  which implies  $A \cong M_n(A')$ , a contradiction as  $A$  is not Artinian by  $M_n(A')$  is. Thus  $E$  is not a finitely generated  $A'$ -module.

**Remark.** Let  $R$  be a ring,  $E$  an  $R$ -module. Let  $r \in Z(R)$ . Then  $\ell_r \in R'(E)$ . Thus there exists a ring homomorphism  $\phi : Z(R) \rightarrow R'(E)$  mapping  $r \mapsto \ell_r$ . Denote  $\phi(Z(R))$  by  $Z(R) \cdot I_E$  where  $I_E$  is the identity map on  $E$ . If  $E$  is a finitely generated  $Z(R)$ -module, then  $E$  is a finitely generated  $Z(R)I_E$ -module (the actions on  $E$  are the same).

**Observation.** If  $E$  is a finitely generated  $R$ -module and  $R$  a finitely generated  $Z(R)$ -module, then  $E$  is a finitely generated  $Z(R)$ -module and hence a finitely generated  $R'$ -module.

*Proof.* Let  $E = Rz_1 + \dots + Rz_m, R = Zu_1 + \dots + Zu_n$ . Then  $E = \sum_{i,j} Zu_ix_j$ . Now,  $Z(R)I_E$  is a subring of  $R'$  and thus  $E$  finitely generated over  $Z(R)$  implies  $E$  is finitely generated over  $R'$ .  $\square$

**Proposition 3.118.** Suppose  $R$  is finitely generated over  $Z(R)$  and  $E$  is a finitely generated semisimple  $R$ -module. Then  $\lambda : R \rightarrow R''$  is onto.

**Note.** Suppose  $r \in Z(R)$ . Then  $\ell_r \in R'(E)$ . In fact,  $\ell_r \in Z(R')$  as for  $f \in R', f\ell_r(x) = f(rx) = rf(x) = (\ell_r f)(x)$  for all  $x \in E$ . Hence  $Z(R)I_E \subset Z(R')$ .

**Proposition 3.119.** Suppose  $\lambda : R \rightarrow R''(E)$  is an isomorphism. Then  $Z(R') = Z(R)I_E = \{\ell_r | r \in Z(R)\}$ .

*Proof.* Only need to show  $(\subset)$ . Let  $f \in Z(R')$ . Then for all  $\phi \in R', f(\phi x) = \phi f(x)$  which implies  $f \in \text{End}_{R'}(E) = R''(E)$ . So  $f = \ell_r$  for some  $r \in R$ . Want to show  $r \in Z(R)$ . Let  $s \in R$ . Then  $rsx = \ell_r(sx) = f(sx) = sf(x) = s\ell_r(x) = srx$ . Thus  $rs(x) = sr(x)$  for all  $x \in E$  which says  $(rs - sr)E = 0$ . Of course,  $E$  is faithful which implies  $rs = sr$ .  $\square$

**Corollary 3.120.** Let  $D$  be a division ring. Then  $Z(M_n(D)) = \{xI_n | x \in Z(D)\}$ .

*Proof.* Let  $R = D, E = D^n$ . Then  $R'(E) = M_n(D^{op})$  and since  $E$  is a finitely generated semisimple ring over a division ring, we've seen  $\lambda : R \rightarrow R''(E)$  is an isomorphism. Thus  $Z(R') = Z(R)I_E$ . Now, note that  $Z(M_n(D)) = Z(M_n(D^{op}))$ .  $\square$

**Proposition 3.121.** Let  $D_1, D_2$  be division rings,  $V_1, V_2$  finitely generated  $D_1, D_2$  vectors spaces. Then  $\text{End}_{D_1}(V_1) \cong \text{End}_{D_2}(V_2)$  if and only if  $D_1 \cong D_2$  and  $\dim_{D_1} V_1 = \dim_{D_2} V_2$ .

*Proof.* Let  $R = \text{End}_{D_1} V_1$  and  $\phi : R \rightarrow \text{End}_{D_2} V_2$ . Then  $V_1$  is an  $R$ -module and  $V_2$  is an  $R$ -module through  $\phi$ . Note  $V_1$  is a simple  $R$ -module (let  $v \in V \setminus \{0\}$  and  $u \in V_1$ . Then there exists  $\sigma \in \text{End}_{D_1} V_1 = R$  such that  $\sigma v = u$ . Thus  $Rv = V_1$ ). Similarly,  $V_2$  is simple over  $\text{End}_{D_2}(V_2) \cong R$ . Recall  $R$  is simple Artinian and thus has a unique simple  $R$ -module. Thus  $V_1 \cong V_2$ . So  $D_1 \cong D_1''(V_1) \cong \text{End}_R(V_1) = \text{End}_R(V_2) \cong D_2''(V_2) \cong D_2$ . If  $V_1 = D_1^{n_1}$ , then  $\dim_{D_1} \text{End}_{D_1} V_1 = n_1^2$ . So  $n_1^2 = \dim_{D_1} R = \dim_{D_2} R = n_2^2$ . Thus  $n_1 = n_2$ .  $\square$

**Proposition 3.122.** Suppose  $A_1 \times \dots \times A_k \cong B_1 \times \dots \times B_\ell$  as a ring isomorphism where  $A_i$ 's and  $B_j$ 's are nonzero simple rings. Then  $k = \ell$  and  $A_i = B_j$  after reordering.

*Proof.* Suppose they are isomorphic via  $\phi$ .  $A_1$  is an ideal of  $A_1 \times \cdots \times A_k$ . Thus  $\phi(A_1)$  is an ideal of  $B_1 \times \cdots \times B_\ell$ . Since ideals of  $B_1 \times \cdots \times B_\ell$  are of the form  $I_1 \times \cdots \times I_\ell$  where  $I_i$  is an ideal of  $B_i$ , but  $I_i = (0)$  or  $I_i = B_i$ , we have  $\phi(A_1) = B_1 \times \cdots \times B_t \times (0) \times \cdots \times (0)$  (after reordering). If  $t > 1$ , then  $\phi(A_1)$  has nontrivial proper ideals, a contradiction as  $A_1$  simple. So  $\phi(A_1) = B_1$ . Use induction (mod out and repeat) to get  $A_i = B_i$  and  $k = \ell$ .  $\square$

**Theorem 3.123.** *Let  $R$  be a semisimple ring. Then there exist unique division rings  $D_1, \dots, D_k$  and natural numbers  $n_1, \dots, n_k$  such that  $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ . Furthermore, every such  $R$  is semisimple.*

**Definition 3.124.** *An ideal  $I$  is **nilpotent** if  $I^n = 0$  for some  $n$  and  $I$  is called **nil** if every element in  $I$  is nilpotent.*

**Note.**  $I$  nilpotent implies  $I$  nil, but the converse is false.

**Example.**  $R = k[[x_1, \dots, x_n]]/(x_1, x_2^2, x_3^3, \dots)$ .  $R$  is quasilocal and  $m = (x_1, \dots, x_n)$  is nil, but not nilpotent.

In 1907, Wedderburn proved: *If  $R$  is a finite dimensional  $k$ -algebra (where  $k$  is a field), then there exists a largest nilpotent left ideal of  $R$  (that is, it contains all other nilpotent ideals).* 20 years later, Artin proved the same result for left Artinian rings. This largest nilpotent ideal is called the **Wedderburn radical**. Wedderburn defined a finite dimensional  $k$ -algebra to be semisimple if the Wedderburn radical was 0. In 1945, Jacobson extended the definition of the Wedderburn radical:

**Definition 3.125.** *Let  $R$  be a ring. The **Jacobson Radical** of  $R$  is  $\text{rad}R = J(R) = \bigcap m$ , where the intersection runs over all maximal left ideals.*

**Note.** If  $R$  has DCC, then  $J(R)$  is exactly the Wedderburn radical.

**Lemma 3.126.** *Let  $R$  be a ring and  $y \in R$ . TFAE*

1.  $y \in J(R)$
2.  $1 - xy$  is left invertible for all  $x \in R$ .
3.  $yM = 0$  for all simple left  $R$ -modules.

*Proof.*  $1 \Rightarrow 2$  If  $1 - xy$  is not left invertible, then  $R(1 - xy) \neq R$ , which says  $R(1 - xy) \subseteq m$  for some maximal left ideal  $m$ . Since  $y \in m$ , we know  $xy \in m$  and thus  $1 \in m$ , a contradiction.

$2 \Rightarrow 3$  Suppose  $yM \neq 0$ . Then  $yu \neq 0$  for some  $u \in M$ . Then  $Ryu \neq 0$  which implies  $Ryu = M$  as  $M$  is simple. So  $u = xyu$  for some  $x \in R$  which says  $(1 - xy)u = 0$ . By 2,  $u = 0$ , a contradiction.

$3 \Rightarrow 1$  Let  $m$  be a left maximal ideal. Then  $R/m$  is simple which implies  $y(R/m) = 0$  and thus  $y \in m$ . Since  $m$  was arbitrary,  $y \in J(R)$ .  $\square$

**Definition 3.127.** *For all  $R$ -modules  $M$ , the **annihilator** of  $M$  is defined as  $\text{Ann}_R(M) = \{r \in R \mid rM = 0\}$ .*

Recall that  $\text{Ann}_R(M)$  is a two-sided ideal ( $\text{Ann}_R(M) = \ker(\lambda : M \rightarrow \text{End}_R M)$ ).

**Corollary 3.128.**  $J(R) = \bigcap \text{Ann}_R M$ , where the intersection runs over all simple left  $R$ -modules. In particular,  $J(R)$  is an ideal.

**Proposition 3.129.** *Let  $R$  be a ring and  $y \in R$ . TFAE*

1.  $y \in J(R)$
2.  $1 - xyz$  is a unit for  $x, z \in R$ .

*Proof.*  $2 \Rightarrow 1$  Let  $z = 1$  and use previous lemma.

**1  $\Rightarrow$  2** By the corollary,  $yz \in J(R)$ . Thus  $1 - xyz$  is left invertible. Let  $u$  be its left inverse (so  $u$  is right invertible). Then  $u(1 - xyz) = 1$  which implies  $u = 1 + uxyz$ . Note  $uxyz \in J(R)$  and thus  $u = 1 + uxyz$  is left invertible. Thus  $u$  is a unit, which implies its left inverse is its right inverse and thus  $1 - xyz$  is a unit.  $\square$

**Corollary 3.130.** *Let  $R$  be a ring. Then  $J(R) = \cap m$ , where the intersection runs over all maximal right ideals.*

*Proof.* We can prove the above results for the “right” Jacobson radical and then (2) of the proposition says they must be the same.  $\square$

**Definition 3.131.** *A ring is called **semiprimitive/Jacobson semisimple/J-semisimple** if  $J(R) = 0$ .*

**Remark.** Semisimple rings are semiprimitive.

*Proof.* Let  $R$  be semisimple and  $y \in J(R)$ . Now  $R = I_1 \oplus \dots \oplus I_k$  where  $I_j$  are simple. Now  $yI_j = 0$  for all  $j$  which implies  $yR = 0$  and in particular  $y \cdot 1 = 0$ .  $\square$

**Examples.**  $\mathbb{Z}$ ,  $F[x]$  for a field  $F$  are semiprimitive, but not semisimple.

**Theorem 3.132.** *Let  $R$  be a ring. TFAE*

1.  $R$  is semisimple
2.  $R$  is left Artinian and  $J(R) = 0$ .

*Proof.* Note that 1  $\Rightarrow$  2 is done by the remark. For the other direction, note that by DCC, every nonzero left ideal of  $R$  contains a simple (that is, minimal nonzero) left ideal.

Claim: Every simple left ideal is a direct summand of  $R$ .

Proof: Let  $I$  be a simple left ideal (so  $I \neq 0$ ). Since  $J(R) = 0$ ,  $I \not\subseteq m$  for some maximal  $m$ . Since  $m$  is maximal, this says  $I + m = R$ . Since  $I$  is simple,  $I \cap m = 0$ . Thus  $I \oplus m = R$ .

Let  $I_1$  be a simple left ideal of  $R$ . Then  $R = I_1 \oplus J_1$  for some ideal  $J_1$  by the claim. If  $J_1 = 0$ , done. Otherwise,  $J_1$  contains a simple ideal  $I_2$ . By the Claim,  $R = I_2 \oplus A_2$  and thus  $J_1 = I_2 \oplus A_2 \cap J_1$ . Let  $J_2 := A_2 \cap J_1$ . Then  $R = I_1 \oplus I_2 \oplus J_2$ . Continuous in this manner. By DCC, the chain must eventually end at a simple  $J_n$ . Then  $R$  is the direct sum of simple modules and therefore semisimple.  $\square$

**Proposition 3.133.** *Let  $R$  be a commutative ring,  $x$  an indeterminate. Then  $J(R[x]) = \text{Nilrad}(R[x]) = (\text{Nilrad}(R))[x]$ .*

*Proof.* Note that  $\text{Nilrad}(R[x]) = \cap_{p \in \text{Spec}R[x]} p \subseteq \cap_{m \in \text{Spm}R[x]} m = J(R[x])$ . Let  $f = a_0 + \dots + a_n x^n \in J(R[x])$ . Then  $1 - xf = 1 - a_0 x - a_1 x^2 - \dots - a_n x^{n+1}$  is a unit in  $R[x]$ . By a previous exercise, this implies  $a_0, \dots, a_n$  are nilpotent. Thus  $f \in \text{Nilrad}(R[x])$ .  $\square$

**Corollary 3.134.** *If  $R$  is reduced (that is,  $\text{Nilrad}R = 0$ ), then  $R[x]$  is semiprimitive. In fact,  $R[x_\alpha | \alpha \in I]$  is semiprimitive.*

**Lemma 3.135.** *Let  $I_1, \dots, I_k$  be nilpotent left ideals. Then  $I_1 + \dots + I_k$  is nilpotent.*

*Proof.* By induction, it suffices to prove for  $k = 2$ . Let  $n$  be such that  $I_1^n = I_2^n = 0$ . Then we see  $(I_1 + I_2)^{2n-1} = 0$  by showing  $(a_1 + b_1) \dots (a_{2n-1} + b_{2n-1}) = 0$  for  $a_i \in I_1, b_i \in I_2$ .  $\square$

**Corollary 3.136.** *If  $R$  is a left Noetherian ring, then there exists a nilpotent left ideal containing all other nilpotent ideals (and is itself contained in  $J(R)$ ).*

**Remark.** The set of nilpotents in a noncommutative ring does not necessarily form a left or right ideal.

**Lemma 3.137.** *If  $I$  is a nil left ideal, then  $I \subseteq J(R)$ .*

*Proof.* Let  $y \in I$ . It is enough to show  $1 - xy$  is a unit for all  $x \in R$ . Now  $y \in I$  implies  $xy \in I$  and therefore  $xy$  is nilpotent. In general, we've seen if  $a^n = 0$ , then  $(1 - a)^{-1} = 1 + \dots + a^{n-1}$ . Thus  $1 - xy$  is a unit and  $y \in J(R)$ .  $\square$

**Theorem 3.138.** *Let  $R$  be a left Artinian ring. Then  $J(R)$  is nilpotent. Hence  $J(R)$  is the largest nilpotent left or right ideal and so  $J(R)$  is the Wedderburn Radical.*

*Proof.* Let  $J = J(R)$ . By DCC, the descending chain  $J \supseteq J^2 \supseteq J^3 \supseteq \dots$  stabilizes. So there exists  $k$  such that  $J^k = J^{k+1} = \dots$ . Let  $I = J^k \subseteq J(R)$ .

Claim:  $I = 0$ .

*Proof:* Suppose not. Consider  $\Lambda = \{J | J \text{ is a left ideal such that } IJ \neq 0\}$ . Note  $R \in \Lambda$  so  $\Lambda \neq \emptyset$ . So there exists a minimal element  $J \in \Lambda$  by DCC. Choose  $y \in J$  such that  $Iy \neq 0$ . Note  $Iy \subseteq J$  is a left ideal and  $I(Iy) = I^2y = Iy \neq 0$ . Thus  $Iy \in \Lambda$  and by minimality, we have  $Iy = J$ . Now  $y \in J$  implies  $y = iy$  for some  $i \in I$ . Thus  $(1 - i)y = 0$  but  $i \in J(R)$  implies  $1 - i$  is a unit. Thus  $y = 0$ , a contradiction.  $\square$

**Remark.** Let  $R$  be a semisimple ring and  $M$  a left  $R$ -module. TFAE

1.  $M$  is (left) Artinian
2.  $M$  is (left) Noetherian
3.  $M$  is finitely generated
4.  $\lambda_R(M) < \infty$ .

*Proof.* If  $R$  is semisimple, then  $M$  is. Thus  $M = \bigoplus_{i \in \Lambda} I_i$  for  $I_i$  simple. If  $\Lambda$  is finite, we have a composition series. If  $\Lambda$  is infinite, then we can find an ascending/descending chain that does not stabilize (just add on/pluck off components).  $\square$

**Theorem 3.139.** *Let  $R$  be a left Artinian ring. Then  $R$  is left Noetherian (and hence  $\lambda(R) < \infty$  where  $R$  is considered a left  $R$ -module).*

*Proof.* Let  $J = J(R)$ . Note that  $R/J$  is semisimple (as  $R$  is left Artinian,  $R/J$  is left Artinian and  $J(R/J) = 0$  by the bijection of maximal ideals of  $R$  and  $R/J$ ). For any  $i$ , we see  $J^i/J^{i+1}$  is an  $R/J$ -module as  $J(J^i/J^{i+1}) = 0$ . Since  $R$  is left Artinian and  $J^i \subseteq R$ , we see  $J^i$  is left Artinian and thus  $J^i/J^{i+1}$  is left Artinian as an  $R$  module and thus as an  $R/J$ -module. Thus  $\lambda_{R/J}(J^i/J^{i+1}) < \infty$  by the remark which says  $J^i/J^{i+1}$  satisfies ACC as an  $R/J$ -module and thus as an  $R$ -module and so  $\lambda_R(J^i/J^{i+1}) < \infty$ . (\*)

Claim:  $\lambda(R/J^i) < \infty$  for all  $i$ .

*Proof:* For  $i = 1$ , we see  $\lambda(R/J) < \infty$  by the  $i = 0$  case of (\*). For  $i > 1$ , consider the short exact sequence  $0 \rightarrow J^{i-1}/J^i \rightarrow R/J^i \rightarrow R/J^{i-1} \rightarrow 0$ . Since  $\lambda_R(J^{i-1}/J^i) < \infty$  by (\*) and  $\lambda_R(R/J^{i-1}) < \infty$  by induction, we have  $\lambda_R(R/J^i) < \infty$ .

By the Theorem,  $J^n = 0$  for some  $n$  and thus we get  $\lambda_R(R) = \lambda_R(R/J^n) < \infty$ .  $\square$

**Proposition 3.140.** *Let  $R$  be a commutative Artinian ring. Then  $R$  has only finitely many prime ideals, each of which is maximal (that is,  $\dim R = 0$ ).*

*Proof.* Recall that  $\dim R = \sup\{n | p_0 \subsetneq p_1 \subsetneq \dots \subsetneq p_n, p_i \in \text{Spec}R\}$ .

Claim:  $R$  has only finitely many maximal ideals

*Proof:* Suppose not. Let  $m_1, m_2, \dots$ , be an infinite list of distinct maximal ideals. Then  $m_1 \supset m_1 \cap m_2 \supset m_1 \cap m_2 \cap m_3 \supset \dots$  is a descending chain of ideals. By DCC, there exists  $k$  such that  $m_1 \cap \dots \cap m_k = m_1 \cap \dots \cap m_k \cap m_{k+1}$ . Since maximal ideals are prime,  $m_{k+1} \supseteq m_i$  for some  $i = 1, \dots, k$ . Since both are maximal, this says  $m_{k+1} = m_i$ , a contradiction as they are distinct.

Thus  $J(R) = m_1 \cap \dots \cap m_k$ . Let  $p \in \text{Spec}R$ . As  $J(R)$  is nilpotent,  $p \supseteq J(R)$  (as the nilradical is the intersection of all primes). Then  $p \supseteq m_1 \cap \dots \cap m_k$  which implies  $p \supseteq m_i$ . Since  $m_i$  is maximal,  $p = m_i$ . Thus every prime is maximal.  $\square$

**Definition 3.141.** Let  $R$  be a commutative ring,  $I$  an ideal. Say  $\text{Min}_R R/I = \{p \in \text{Spec}R \mid p \text{ is minimal over } I\}$  (Recall by  $p$  minimal over  $I$ , we mean there does not exist  $q \in \text{Spec}R$  such that  $p \supsetneq q \supseteq I$ .)

By the bijection between primes  $p$  of  $R/I$  and primes  $I \subseteq p$  in  $R$ , these are the minimal primes of  $R/I$ . Thus  $\text{Min}_R R/I \leftrightarrow \text{Min}_{R/I} R/I$ . Also, note that  $\text{Min}_R R/(0)$  are just the minimal primes of  $R$ .

**Remarks.**

1.  $\sqrt{I} = \bigcap_{p \in \text{Min}_R R/I} p$ .
2.  $\text{Min}_R R/I$  is a finite set if and only if  $\sqrt{I}$  is the intersection of finitely many prime ideals.

**Proposition 3.142.** Let  $R$  be commutative and Noetherian,  $I$  an ideal. Then  $\text{Min}_R(R/I)$  is finite.

*Proof.* Let  $\Gamma = \{I \subsetneq R \mid \text{Min}_R R/I \text{ is not finite}\}$ . By way of contradiction, suppose  $\Gamma \neq \emptyset$ . Choose  $I$  maximal in  $\Gamma$  by ACC. Then, by maximality,  $I = \sqrt{I}$  as they have the same minimal primes. Replacing  $R/I$  with  $R$ , we have a Noetherian ring  $R$  such that

1.  $\text{Min}_R R$  is infinite
2.  $\text{Min}_R R/J$  is finite for all  $J \neq 0$
3.  $R$  is reduced (as  $I = \sqrt{I}$ ).

Note also that  $R$  is not a domain as otherwise  $\text{Min}_R R = (0)$ . Choose  $a \in R \setminus \{0\}$  such that  $a$  is a zero divisor. Consider  $\text{ann}_R a \subseteq \text{ann}_R a^2 \subseteq \dots$ . By ACC, there exists  $n$  such that  $\text{ann}_R a^n = \text{ann}_R a^{n+1}$ . Let  $b = a^n$ . Then  $\text{ann}_R b = \text{ann}_R b^2$ .

Claim:  $(b) \cap \text{ann}_R b = (0)$ .

*Proof:* First note that since  $R$  is reduced,  $b \neq 0$  and since  $a$  is a zero divisor,  $\text{ann}_R b \neq 0$ . Now, let  $x \in (b) \cap \text{ann}_R b$ . So  $x = rb \in \text{ann}_R b$  which implies  $xb = rb^2 = 0$ . Thus  $r \in \text{ann}_R b^2 = \text{ann}_R b$ . So  $x = rb = 0$ .

Thus  $(0) = \sqrt{(0)} = \sqrt{(b) \cap \text{ann}_R b} = \sqrt{(b)} \cap \sqrt{\text{ann}_R b} = (P_1 \cap \dots \cap P_\ell) \cap (Q_1 \cap \dots \cap Q_k)$  (since  $\text{Min}_R(R/J) < \infty$ , for an ideal  $J$  we have  $\sqrt{J}$  is the intersection of finitely many primes). Thus  $0$  is the intersection of finitely many primes which implies  $\text{Min}_R R$  is finite, a contradiction.  $\square$

**Theorem 3.143.** Let  $R$  be a commutative, Noetherian ring. Then every ideal has only finitely many minimal primes.

*Proof.* Let  $\Lambda = \{I : I \text{ has infinitely many min'l primes}\}$ . Let  $I \in \Lambda$  be maximal. Clearly,  $I$  is not prime. Choose  $a, b \in R$  such that  $a, b \notin I$  but  $ab \in I$ . Let  $J_1 = (I, a) = I + aR$  and  $J_2 = (I, b) = I + bR$ . Then  $J_i \supsetneq I$  and  $J_1 J_2 \subseteq I$ . Note that  $\text{Min}_R R/I \subseteq \text{Min}_R R/J_1 \cup \text{Min}_R R/J_2$ , which are both finite (as  $J_1, J_2 \notin \Lambda$ ). Thus  $\text{Min}_R R/I$  is finite, a contradiction.  $\square$

**Theorem 3.144.** If  $V$  is a vector space over a division ring, then TFAE

1.  $V$  is Noetherian.
2.  $V$  is Artinian.
3.  $\lambda(V) < \infty$ .
4.  $\dim V < \infty$ .
5.  $V$  is finitely generated.

**Theorem 3.145.** Let  $M$  be a semisimple left  $R$ -module. TFAE

1.  $M$  is left Noetherian.
2.  $M$  is left Artinian.
3.  $\lambda_R(M) < \infty$ .
4.  $M$  is finitely generated.

*Proof.* To show any of 1,2,3 implies 4, use contrapositive. To show 4 implies any of 1,2, or 3, note that  $M \cong \bigoplus_{i=1}^n Re_i$ . Thus submodules are of the form  $\bigoplus_{j \in J} Re_j$  which says there are finitely many submodules.  $\square$

**Theorem 3.146.** *Let  $R$  be a commutative ring. TFAE*

1.  $R$  is Artinian.
2.  $\lambda(R) < \infty$ .
3.  $R$  is Noetherian and  $\dim R = 0$ .

*Proof.* Recall that  $R$  Artinian implies all prime ideals are maximal and so  $\dim R = 0$ . Thus, the only thing needed to prove is  $3 \Rightarrow 2$ . Let  $J = J(R)$ . Since  $R$  is Noetherian and every prime ideal is maximal (as  $\dim R = 0$ ),  $\text{Spec}R = \{m_1, \dots, m_r\}$ . So  $J(R) = \bigcap_{i=1}^r m_i$ . So  $R/J = R/(m_1 \cap \dots \cap m_r)$ . Now  $m_i + m_j = R$  for all  $i \neq j$ , thus by the Chinese Remainder Theorem, we have  $R/J \cong R/m_1 \times \dots \times R/m_r$ . So  $R/J$  is semisimple. Now, since  $J$  is nilpotent as  $J = m_1 \cap \dots \cap m_r = \sqrt{(0)}$  and  $J$  is finitely generated, there exists  $n$  such that  $J^n = 0$ . Consider  $R = J^0 \supseteq J \supseteq \dots \supseteq J^n = (0)$ . Note that  $J^i/J^{i+1}$  is a finitely generated  $R/J$  module for all  $i$  which implies it is semisimple  $R/J$  module as  $R/J$  is. Thus it is a semisimple  $R$ -module. (Recall an  $R$ -module  $M$  is simple if and only if  $M$  is a simple  $R/J$ -module). Now,  $R$  Noetherian implies  $J^i$  is finitely generated and thus  $\lambda_R(J^i/J^{i+1}) < \infty$  for all  $i$ . But  $\lambda(R) = \sum_{i=0}^{n-1} \lambda_R(J^i/J^{i+1}) < \infty$ .  $\square$

**Example.**  $R = k[x, y, z]/(x^3, xy, y^2, xz, z^6)$  where  $k$  is a field. Note that  $\text{Spec}R = \{(x, y, z)R\}$  which implies  $\dim 0$ . Now  $R$  is Noetherian as  $k$  is. Consider  $k[x, y, z]/(x^3, xy, xz, z^6)$ . Here,  $(x, y, z) \subsetneq (x, z)$  which implies it has  $\dim > 0$  and is thus not Artinian.

**Definition 3.147.** *Let  $R$  be a ring.  $R$  is called von Neumann regular if for all  $a \in R$ , there exists  $x \in R$  such that  $axa = a$ .*

**Examples.**

1. Division rings are von Neumann regular
2. Products of von Neumann regular rings are von Neumann regular.
3. Example of a commutative von Neumann regular ring which is not a product of fields: Let  $F$  be a finite field and  $S = \prod_{i=1}^{\infty} F$ . Consider  $S$  as an  $F$ -algebra via  $F \rightarrow S$  defined by  $1 \mapsto (1, 1, \dots)$ . Let  $R = F1_S + \bigoplus_{i=1}^{\infty} F = \{(a_i) \in S : \text{there exists } c \in F \text{ such that } a_i = c \text{ for all but finitely many } i\}$ .  $R$  is easily seen to be von Neumann regular (take  $x_i = a_i^{-1}$ ).

The idempotents of  $R$  fall into disjoint sets  $A = \{(e_i) : e_i = 1 \text{ for all but finitely many } i\}$  and  $B = \{1 - e : e \in A\}$ . Observe  $e \in A$  if and only if  $1 - e \in B$ . If  $e \in B$ , then  $|Re| < \infty$ . Thus there do not exist idempotents  $e \in R$  such that  $|Re| = \infty$  and  $|R(1 - e)| = \infty$ . But any infinite product of fields has such idempotents:  $e = (1, 0, 1, 0, \dots)$  and  $1 - e = (0, 1, 0, 1, \dots)$ .

**Proposition 3.148.** *Let  $R$  be a ring. TFAE*

1.  $R$  is von Neumann regular
2. Every finitely generated left ideal is generated by an idempotent.

3. Every finitely generated left ideal is a direct summand of  $R$ .

*Proof.*  $1 \Rightarrow 2$  Let  $I = Ra_1 + \dots + Ra_n$ . If  $n = 1$ , then there exists  $x \in R$  such that  $a = axa$ . Let  $e = xa \in Ra$ . Then  $e^2 = xaxa = xa = e$ . Clearly,  $Re \subseteq Ra$ . But  $a = ae \in Re$ . So  $Ra = Re$ . For  $n > 1$ , note that it is enough to show the  $n = 2$  case. Let  $I = Ra_1 + Ra_2$ . By the  $n = 1$  case, we have  $I = Re_1 + Re_2$  where  $e_1^2 = e_1$  and  $e_2^2 = e_2$ . Note that  $I = Re_1 + Re_2(1 - e_1)$  as  $re_1 + se_2(1 - e_1) = re_1 + se_2 - se_2e_1$ . Let  $f$  be an idempotent such that  $Rf = Re_2(1 - e_1)$ . Then  $fe_1 \in Re_2(1 - e_1)e_1 = 0$ . So  $f(f + e_1) = f$ .

Claim:  $I = R(f + e_1)$ .

*Proof:* We've shown  $f \in R(f + e_1)$ . Thus  $e_1 \in R(f + e_1)$ . So  $Rf + Re_1 \subseteq R(f + e_1)$ . Of course,  $I = Re_2(1 - e_1) + Re_1 = Rf + Re_1 \subseteq R(f + e_1)$  and since  $I \supseteq R(f + e_1)$ , we see  $I = R(f + e_1)$ .

By the  $n = 1$  case,  $R(f + e_1)$  is generated by an idempotent.

$2 \Rightarrow 3$  Let  $I$  be a finitely generated ideal. Then  $I = Re, e^2 = e$ . Then  $R = Re \oplus R(1 - e) = I \oplus R(1 - e)$ .

$3 \Rightarrow 1$  Let  $a \in R$ . Then  $R = Ra \oplus J$ . So  $1 = ra + j$  such that  $j \in J$ . This implies  $a = ara + aj$ . Now,  $aj = a - ara = (1 - ar)a \in Ra$  and  $aj \in J$ . Thus  $aj = 0$  which implies  $a = ara$ .  $\square$

**Corollary 3.149.** *Let  $R$  be a ring. TFAE*

1.  $R$  is semisimple.

2.  $R$  is von Neumann regular and left Noetherian.

**Example.**  $\prod_{i=1}^{\infty} F$  is von Neumann regular but not semisimple for a field  $F$ .

**Proposition 3.150.** *von Neumann regular rings are semiprimitive.*

*Proof.* Let  $a \in J(R)$ . Then there exists  $x \in R$  such that  $a = axa$ . Then  $a(1 - xa) = 0$ . As  $a \in J(R)$ ,  $1 - xa$  is a unit which implies  $a = 0$ .  $\square$

**Example.** Let  $F$  be a field,  $V$  an infinite dimensional  $F$ -vector space. Then  $End_F V$  is not Artinian and hence not semisimple. It is also not Noetherian.

*Proof.* Let  $\{e_1, e_2, \dots\}$  be part of an  $F$ -basis for  $V$ . Let  $I_n = \{f \in End_F V | f(e_1) = \dots = f(e_n) = 0\}$ . These are left ideals of  $End_F V$  and  $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ . Thus it is not left Artinian.  $\square$

**Proposition 3.151.** *Let  $M$  be a semisimple left  $R$ -module. Then  $End_R M$  is von Neumann regular.*

*Proof.* Let  $f \in End_R M$ . Want to find  $g \in End_R M$  such that  $fgf = f$ . Let  $K = \ker f$ . Then there exists  $N$  such that  $M = K \oplus N$  since  $M$  is semisimple. Also, there exists  $K'$  such that  $M = K' \oplus f(N)$ . Note  $f|_N : N \rightarrow f(N)$  is an isomorphism as  $N \cap K = 0$ . Define  $g : M \rightarrow M$  by  $g|_{K'} = 0$  and  $g|_{f(N)} = (f|_N)^{-1}$ . Then  $g \in End_R M$  and  $fgf = f$ .  $\square$

**Theorem 3.152** (Wedderburn 1905). *Every finite division ring is a field.*

*Proof.* Let  $D$  be a finite division ring. Let  $F = Z(D)$ , a subfield of  $D$ . Say  $F = \mathbb{F}_q$  (that is,  $|F| = q = p^m$ ,  $char F = p$ ). Let  $n = \dim_F D$  (so that  $|D| = q^n$ ) as  $D$  is an  $F$ -vector space. For each  $a \in D$ , let  $C(a) = \{d \in D | da = ad\}$ , the centralizer. It is easily seen that  $F \subseteq C(a)$  is a division subring of  $D$  (if  $d$  commutes with  $a$  so does  $d^{-1}$ ). Let  $r_a = \dim_F C(a)$ ,  $m_a = \dim_{C(a)} D$ . Just as in the proof for fields, we can show  $m_a r_a = n$ . In particular,  $r_a | n$ . By the class equation,  $|D^*| = |Z(D^*)| + \sum \frac{|D^*|}{|C(a)^*|}$ , where the sum runs over the distinct conjugacy classes. Since  $|Z(D^*)| = |F^*|$ , we see  $(*) |D^*| = q - 1 + \sum_a \frac{q^n - 1}{q^{r_a} - 1}$  where  $r_a < n$  as  $a \notin F$ . Suppose, by way of contradiction, that  $n > 1$ . Recall  $x^n - 1 = \prod_{d|n} \phi_d(x)$ . Then for all  $a \notin F$ , we see  $r_a | n$  and  $r_a < n$ . This says  $x^n - 1 = (x^{r_a} - 1)\phi_n h_a(x)$  for some  $h_a(x) \in \mathbb{Z}[x]$ . Letting  $x = q$  we see  $\phi_n(q) | \frac{q^n - 1}{q^{r_a} - 1}$  in  $\mathbb{Z}$  for all  $a \notin F$ . By  $(*)$ , we have  $\phi_n(q) | q - 1$ . Of course,  $\phi_n(q) = \prod (q - w)$  where  $w$  are the primitive  $n^{\text{th}}$  roots of unity. So  $|q - 1| = |q - w_1| \cdots |q - w_t| |z|$ . By the triangle inequality and the fact that  $w \notin \mathbb{R}^+$ , we see  $|q - w| > |q| - |w| = q - 1$ , a contradiction.  $\square$



**Corollary 3.153.** Any finite subring of a division ring is a field.

*Proof.* Any finite subring of a division ring is a division ring. □

**Corollary 3.154.** Let  $D$  be a division ring with  $\text{char } D > 0$ . Then any finite subgroup of  $D^*$  is cyclic.

*Proof.* Note that  $\mathbb{F}_p \subseteq Z(D)$ . Let  $G = \{g_1, \dots, g_n\}$  be a finite subgroup of  $D^*$ . Let  $R = \{\sum \alpha_i g_i \mid \alpha_i \in \mathbb{Z}_p, g_i \in G\}$ . Then  $R$  is a finite subring of  $D$  which implies  $R$  is a field. Now,  $G$  is a finite subgroup of  $R^*$  which implies  $G$  is cyclic. □

**Example.** The division ring of quaternions  $D = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ . Now,  $Q_8$  is a finite subgroup of  $D^*$  which is not cyclic.

## 4 Representation Theory

**Exercise.** Let  $M$  be a finitely generated semisimple left  $R$ -module. Then  $M \cong n_1 V_1 \oplus \dots \oplus n_k V_k$  where  $n_i$  are positive integers,  $V_i$  are simple left  $R$ -modules with  $V_i \not\cong V_j$  for all  $i \neq j$ , and  $n_i V_i = \underbrace{V_i \oplus \dots \oplus V_i}_{n_i \text{ times}}$ . Furthermore, if

$M = m_1 W_1 \oplus \dots \oplus m_\ell W_\ell$ , then  $k = \ell$  and, after reordering,  $n_i = m_i$  and  $V_i \cong W_i$  for all  $i$ .

*Proof.* The first statement is the additive version of  $M \cong \prod M_i^{e_i}$ , which is proven in HW5#2. For uniqueness, note that these yield composition series which are unique by Jordan Hölder. □

**Definition 4.1.** The  $n_i$ 's in the above exercise are called the **multiplicity** of  $V_i$  in  $M$ .

**Recall.** Let  $R$  be a semisimple ring,  $I_1, \dots, I_t$  the distinct simple left ideals of  $R$ . Then  $R \cong n_1 I_1 \oplus \dots \oplus n_t I_t \cong B(I_1) \times \dots \times B(I_t)$  as rings where  $B(I_j) = \sum_{J \cong I_j} J$  (see Exam 1#1). Note that  $B(I_j)$  are two sided ideals of  $R$ . They are not subrings of  $R$  (as they have different identities), but  $B(I_j)$  are simple Artinian rings (where  $I_j$  is the unique simple left ideal of  $B(I_j)$ ). Furthermore,  $\text{End}_{B(I_j)} I_j = \text{End}_R I_j$  (Write  $r = b_1 + \dots + b_t$ . Then  $r I_j = b_j I_j$ ), which is a division ring, say  $D_j$ . By Artin Wedderburn,  $B(I_j) = \text{End}_{D_j} I_j \cong M_{n_j}(D_j^{op})$  where  $n_j = \dim_{D_j} I_j$ .

**Theorem 4.2.** Let  $R$  be a semisimple finite dimensional  $k$  algebra for  $k = \bar{k}$  a field. Let  $R \cong n_1 I_1 \oplus \dots \oplus n_t I_t$  where  $I_i$  are simple left ideals and  $I_i \not\cong I_j$  for all  $i \neq j$ . Then

1.  $n_j = \dim_k I_j$  for all  $j = 1, \dots, t$ .

2.  $\dim_k R = \sum_{j=1}^t n_j^2$ .

*Proof.* Clearly  $1 \Rightarrow 2$ . So its only left to prove 1. Let  $m_j = \dim_k I_j$ . Since  $\dim_k I_j \leq \dim_k R < \infty$ , we see  $m_j < \infty$ . Let  $D_j = \text{End}_R I_j$ . Note that  $\dim_k D_j \leq \dim_k \text{End}_k I_j = \dim_k M_{m_j}(k) = m_j^2 < \infty$ . Now,  $k \subseteq Z(R)$ . Hence, multiplication by elements of  $k$  are in  $\text{End}_R I_j$ . So  $k \hookrightarrow \text{End}_R I_j$ . In fact,  $k \subseteq Z(D_j)$  (Let  $f \in D_j$  and  $\mu_a$  multiplication by  $a$ . Then  $(f \mu_a)(i) = f(ai) = af(i) = (\mu_a f)(i)$ ). Now,  $k = \bar{k}$  and  $k \subseteq Z(D_j)$  which implies  $k = D_j$  for all  $j$  (Choose  $\alpha \in D_j$ . Then  $k(\alpha)/k$  is algebraic, but  $k = \bar{k}$  so  $k(\alpha) = k$ ). Now  $n_j I_j \cong B(I_j) \cong \text{End}_{D_j} I_j = \text{End}_k I_j \cong M_{m_j}(k)$ . Thus  $n_j m_j = \dim_k n_j I_j = \dim_k M_{m_j}(k) = m_j^2$ . Thus  $n_j = m_j$ . □

**Theorem 4.3 (Maschke's Theorem).** Let  $G$  be a finite group and  $F$  a field. If  $\text{char } F \nmid |G|$ , then  $F[G]$  is semisimple.

*Proof.* We proved this shortly after the definition of semisimple. □

**Note.** The converse is true!

*Proof.* Let  $|G| = n$  and  $e = \sum_{g \in G} e_g \in F[G]$ . Observe  $e_g e = e = e e_g$  for all  $g \in G$ . Thus  $F e$  is a two sided ideal. Furthermore,  $e^2 = e e_{g_1} + \dots + e e_{g_n} = n e$  as  $e e_g = e$ . Thus, if  $\text{char } F \mid n$ , then  $(1 - x e y)$  is a unit for all  $x, y \in F[G]$  as  $(1 - x e y)(1 + x e y) = 1 - (x^2) e^2 (y^2) = 1 - (x^2) n e (y^2) = 1$ . Thus  $e \in J(F[G])$  and since  $e$  is not zero (the  $e_g$  are linearly independent), we see  $F[G]$  is not semisimple. □

**Proposition 4.4.** *Let  $G$  be a finite group,  $F$  a field. Let  $C_1, \dots, C_r$  be the distinct conjugacy classes of  $G$ . Let  $z_i = \sum_{g \in C_i} g \in F[G]$ . Then  $\{z_1, \dots, z_r\}$  is an  $F$ -basis for  $Z(F[G])$ .*

*Proof.* For all  $i$  and for all  $g \in G$ ,  $gC_i g^{-1} = C_i$ . Thus  $gz_i g^{-1} = z_i$ . Of course,  $z_i$  commutes with elements in  $F$  and so  $z_i \in Z(F[G])$  for all  $i$ . As  $C_1, \dots, C_r$  are disjoint,  $\{z_1, \dots, z_r\}$  is linearly independent over  $F$ . Let  $c \in Z(F[G])$ . Say  $c = \sum_{g \in G} \gamma_g g$ , where  $\gamma_g \in F$ . For  $h \in G$ , we see  $c = hch^{-1} = \sum_{g \in G} \gamma_g hgh^{-1} = \sum_{g \in G} \gamma_{h^{-1}gh} g$ . As the  $g$ 's form a basis for  $F[G]$ , we see  $\gamma_g = \gamma_{h^{-1}gh}$  for all  $h \in G$ . Hence, if  $g_1, g_2$  are in the same conjugacy class, then  $\gamma_{g_1} = \gamma_{g_2}$ . Thus  $c$  is a linear combination of  $z_1, \dots, z_r$ .  $\square$

**Theorem 4.5.** *Let  $G$  be a finite group,  $F$  an algebraically closed field,  $\text{char } F \nmid |G|$ . Then the number of distinct simple  $F[G]$ -modules is equal to the number of conjugacy classes of  $G$ .*

*Proof.* By Maschke's Theorem,  $F[G]$  is semisimple. By Artin-Wedderburn,  $F[G] \cong n_1 I_1 \oplus \dots \oplus n_t I_t$  and thus  $F[G] \cong M_{n_1}(D_1) \times \dots \times M_{n_t}(D_t)$ , where  $D_j = \text{End}_{F[G]}(I_j)$ . Moreover,  $t$  is the number of distinct simple  $F[G]$ -modules.

Claim:  $D_i = F$ .

*Proof:* By definition of the group ring,  $F \subseteq Z(F[G])$ . Thus multiplication by any element of  $F$  induces an  $F[G]$ -endomorphism of  $I_j$ . Thus  $F \subseteq D_j$ . Furthermore,  $F \subseteq Z(D_j)$  as multiplication by  $F$  commutes with elements of  $\text{End}_{F[G]}(I_j)$ . As  $F[G]$  is left Noetherian, we see  $I_j$  is a finitely generated ideal. Further, as  $F[G]$  is a finitely generated  $F$ -vector space, we can conclude  $I_j$  is a finitely generated  $F$ -vector space. Since  $D_j = \text{End}_{F[G]}(I_j) \subseteq \text{End}_F(I_j)$  and  $\text{End}_F(I_j)$  is a finite dimensional  $F$ -vector space, we see  $D_j$  is a finite dimensional  $F$ -vector space. Thus we have  $F \subseteq Z(D_j)$  where  $D_j$  is a finite dimensional  $F$ -vector space. Now, for  $u \in D_j$  we have  $F[u]$  is a domain (it is contained in  $D_j$ ), is a finite dimensional  $F$ -vector space, and is also commutative. Thus  $F[u]$  is a field. Of course,  $F = \overline{F}$  and so  $F = F[u]$ . Since  $u \in D_j$  was arbitrary, we see  $F = D_j$ .

Therefore,  $Z(F[G]) \cong Z(M_{n_1}(F)) \times \dots \times Z(M_{n_t}(F))$ . Recall  $Z(M_n(F)) = \{\lambda I_n \mid \lambda \in F\} \cong F$ . Hence  $Z(F[G]) \cong \underbrace{F \times \dots \times F}_{t \text{ times}}$ . Recall the number of conjugacy classes of  $G$  is  $\dim_F Z(F[G]) = \dim_F F^t = t$ .  $\square$

For simplicity, we will refer to the assumptions " $G$  a finite group,  $F = \overline{F}$  a field,  $\text{char } F \nmid |G|$ " as the **Standard Hypothesis**. Summarizing, under the standard hypothesis, let  $I_1, \dots, I_t$  be the distinct simple left ideals of  $F[G]$ . Let  $n_i = \dim_F I_i$ . Then

1.  $\sum_{i=1}^t n_i^2 = |G|$ .
2.  $t$  is the number of conjugacy classes of  $G$ .
3.  $n_i$  is the number of times  $I_i$  appears in a decomposition into simple submodules of  $F[G]$  (the decomposition is called the "regular representation" of  $G$ ).

**Corollary 4.6.** *Under the standard hypothesis,  $G$  is abelian if and only if  $\dim_F V = 1$  for all simple  $F[G]$ -modules  $V$ .*

*Proof.* Now  $G$  is abelian if and only if  $t$  (the number of conjugacy classes) is  $|G|$  which is if and only if  $n_i = 1$  for all  $i$  by property (1) above.  $\square$

**Remark.** Let  $M$  be an  $F[G]$ -module. Then  $M$  is an  $F$ -vector space. In general, we want  $M$  to be finitely generated. So then  $M = F^n$ . So an  $F[G]$ -module structure is determined by how  $g$  acts on  $F^n$  for all  $g \in G$ . Now  $\tilde{g} : M \rightarrow M$  defined by  $m \mapsto gm$  is an  $F$ -endomorphism of  $M$  which implies  $\tilde{g}$  can be represented by an invertible matrix.

**Example.** Let  $G = C_n$ . Let  $M$  be a simple  $F[G]$ -module. By the corollary,  $M = Fu$ . Let  $C_n = \langle a \rangle$ . Then  $\tilde{a} : M \rightarrow M$  defined by  $u \mapsto au = \lambda u$  for some  $\lambda \in F$ . Of course,  $a^n = 1$  and so  $u = \tilde{1}u = \tilde{a}^n u = \tilde{a}^n u = \lambda^n u$  which implies  $\lambda^n = 1$ . So  $\lambda$  is an  $n^{\text{th}}$  root of unity (not necessarily primitive). Thus each  $n^{\text{th}}$  root of unity determines an  $F[G]$ -module structure on  $F$  via  $a^i u = \lambda^i u$ . Since  $F[G]$  has  $n$  distinct simple  $F[G]$ -modules, all of these simple modules given by the roots of unity are non-isomorphic.

**Example.** Let  $G = V_4 = \{1, a, b, ab\}$  and  $M = Fu$ . Since  $a, b$  are order 2 elements,  $\tilde{a} : M \rightarrow M$  and  $\tilde{b} : M \rightarrow M$  are defined by  $u \mapsto \pm u$ . This yields 4  $F[G]$ -module structures. Since  $G$  is abelian, there must be exactly 4 simple  $F[G]$ -modules which says these maps are distinct and determine all of the simple  $F[G]$ -modules.

**Example.** Let  $G = S_3$ . Then  $S_3$  has 3 conjugacy classes which means there are 3 simple  $F[G]$ -modules, call them  $V_1, V_2, V_3$  where  $n_i = \dim_F V_i$ . Recall that  $n_1^2 + n_2^2 + n_3^2 = 6$ . So WLOG,  $n_1 = n_2 = 1$  and  $n_3 = 2$ . Then

- $V_1 = F$  with  $G$  acting trivially on  $F$  (there is always the trivial representation, which means we may always assume  $n_1 = 1$ )
- $V_2 = Fu$ . So  $1u = u, (12)u = \lambda u, (123)u = \omega u$  where  $\lambda = \pm 1$  and  $\omega^3 = 1$ . Now,  $(23)u = (13)(12)(13)u$ . Say  $(13)u = \delta u$  (so  $\delta = \pm 1$ ). Then  $(23)u = \delta^2 \lambda u = \lambda u$ . Thus everything in the same conjugacy class of  $(12)$  maps  $u$  to the same scalar multiple of  $u$ . Also,  $u = (123)(132)u = \omega^2 u$ . So  $\omega^2 = 1 = \omega^3$  which implies  $\omega = 1$ . We can similar show all 3-cycles act trivially. So  $V_2$  is given by  $(1)u = u, (12)u = -u, (123)u = u$  (where everything in the same conjugacy class act the same on  $u$ ).

**Definition 4.7.** Let  $F$  be a field,  $V$  an  $F$ -vector space. Let  $GL_F(V) := End_F(V)^*$ . Let  $G$  be a group. A **(linear)  $F$ -representation** of  $G$  is a group homomorphism  $\rho : G \rightarrow GL_F(V)$  for some  $F$ -vector space  $V$ . The **degree** of  $\rho$  is  $\dim_F V$ .

**Remarks.**

1. Let  $\rho : G \rightarrow GL_F(V)$  be a representation of  $G$ . Define a left  $F[G]$ -module  $V_\rho$  by  $V_\rho = V$  as an  $F$ -vector space. For  $g \in G$  and  $v \in V$ , define  $gv := \rho(g)v$ . One can check that  $V_\rho$  is an  $F[G]$ -module.

$$\text{Composition: } g_1(g_2v) := \rho(g_1)(\rho(g_2)(v)) = (\rho(g_1)\rho(g_2))(v) = \rho(g_1g_2)(v) = (g_1g_2)v.$$

2. Conversely, let  $M$  be a left  $F[G]$ -module. For each  $g \in G$ , define  $\tilde{g} : M \rightarrow M$  by  $m \mapsto gm$ . Then  $\tilde{g} \in End_F(M)$  (as  $F \in Z(G)$  and thus  $F$  commutes with everything). Since  $(\tilde{g})^{-1} = \widetilde{g^{-1}}$ , we see  $\tilde{g} \in GL_F(M)$ . Define  $\rho : G \rightarrow GL_F(M)$  by  $g \mapsto \tilde{g}$ . It is easily checked that  $\rho$  is a group homomorphism.

This gives us a correspondence between  $F$ -representations of  $G$  and  $F[G]$ -modules.

**Definition 4.8.** Let  $\rho_i : G \rightarrow GL_F(V_i)$  for  $i = 1, 2$  be two  $F$ -representations of  $G$ . We say  $\rho_1$  is **isomorphic** (or **similar** or **equivalent**) to  $\rho_2$  if  $(V_1)_{\rho_1} \cong (V_2)_{\rho_2}$  as  $F[G]$ -modules. An  $F$ -representation  $\rho : G \rightarrow GL_F(V)$  is called **irreducible** if  $V_\rho$  is a simple  $F[G]$ -module. A **subrepresentation** of  $\rho$  is a representation  $\phi : G \rightarrow GL_F(W)$  where  $W$  is a subspace of  $V$  and  $\phi(g) = \rho(g)|_W$  for all  $g \in G$ . Equivalently,  $W_\phi$  is an  $F[G]$ -submodule of  $V_\rho$ .

In particular, if  $\rho_1$  is isomorphic to  $\rho_2$  then  $V_1 \cong V_2$  as  $F$ -vector spaces and thus have the same dimension.

**Notes.**

- The zero representation of  $G$  is  $\rho : G \rightarrow \{1\} = End_F(0)$ .
- Any degree 1 representation is irreducible (as  $\deg 1 \leftrightarrow \dim V = 1$  which has no subrepresentations).

**Examples.**

1. The trivial representation:  $\rho : G \rightarrow GL_F(F)$  where  $\rho(g) = 1$  for all  $g$ . This is a degree 1 representation and  $F_\rho$  is the  $F[G]$ -module  $F$  where  $gf = f$  for all  $g \in G$ .
2. The sign representation: Let  $G = S_n$  and define  $\rho : G \rightarrow GL_F(F) = End_F(F) = F^*$  by  $\sigma \mapsto (-1)^{sgn(\sigma)}$  where  $sgn(\sigma)$  is 1 if its an even permutation and -1 if its odd. This is a degree 1 representation and note  $\rho$  is nontrivial if and only if  $n > 1$  and  $\text{char } F \neq 2$ .

3. Let  $G = C_n$  and suppose  $w \in F$  where  $w$  is a primitive  $n^{\text{th}}$  root of unity. Define  $\rho_i : C_n \rightarrow GL_F(F) = F^*$  by  $a \mapsto \omega^i$ . Now  $\deg \rho_i = 1$  and thus the representation is irreducible. As we saw earlier, if  $\text{char } F \nmid n$ , then  $\rho_i \not\cong \rho_j$  for all  $0 \leq i \neq j \leq n-1$ .

4.  $G = S_3$ . Recall there were 2 degree 1 representations and 1 degree 2 representation. We've seen  $\rho_1$  is the trivial representation and  $\rho_2$  is the sign representation where  $\rho_1 \nmid \rho_2$  as long as  $\text{char } F \neq 2$ . Now let us figure out  $\rho_3$ . Let  $V$  be a 3-dimensional  $F$ -vector space with basis  $\{e_1, e_2, e_3\}$ . Define  $\rho : S_3 \rightarrow GL_F(V)$  by  $\sigma \mapsto \tilde{\sigma}$  where  $\tilde{\sigma}(e_i) = e_{\sigma(i)}$ . So  $\rho$  is a degree 3 representation of  $S_3$ . Since we've seen the only irreducible representations have degree 1 or 2, this is not irreducible. So there exists a subrepresentation. Let  $W = F(e_1 + e_2 + e_3) \subseteq V$ . Note  $\tilde{\sigma}$  fixes  $W$  for all  $\sigma \in S_3$ . So  $W$  is an  $F[S_3]$ -submodule of  $V_\rho$ . Consider the  $F[S_3]$ -module  $U = V/W \cong Fe_1 \oplus Fe_2 \oplus Fe_3 / F(e_1 + e_2 + e_3)$ . To show this is an irreducible representation, we can show it has no proper submodules. Note that  $\dim V = 2$ .

Claim:  $U$  is a simple  $F[S_3]$ -module if and only if  $\text{char } F \neq 3$ .

Proof: Suppose  $\text{char } F \neq 3$ . Note that  $U = F\bar{e}_1 \oplus F\bar{e}_2$  where  $\bar{e}_3 = -\bar{e}_1 - \bar{e}_2$ . Let  $u = r\bar{e}_1 + s\bar{e}_2 \neq 0$  in  $U$ .

Case 1:  $r \neq -s$ . Then  $(13)u + (123)u = r\bar{e}_3 + s\bar{e}_2 + r\bar{e}_2 + s\bar{e}_3 = -(r+s)\bar{e}_1$ . If  $r \neq -s$ , then  $\bar{e}_1 \in F[S_3]u$  which implies  $\bar{e}_2 = (12)e_1 \in F[S_3]u$ . So  $F[S_3]u = U$ .

Case 2:  $r = -s \neq 0$ . Then, as we can divide by  $r$ , it is enough to show for  $u = \bar{e}_1 - \bar{e}_2$ . Note  $(23)u + (123)u = \bar{e}_1 - \bar{e}_3 + \bar{e}_2 - \bar{e}_3 = 3(\bar{e}_1 + \bar{e}_2)$ . Since  $\text{char } F \neq 3$ , this says  $\bar{e}_1 + \bar{e}_2 \in F[S_3](\bar{e}_1 - \bar{e}_2)$ . If  $\text{char } F \neq 2$ , this says  $\bar{e}_1, \bar{e}_2 \in F[S_3](\bar{e}_1 - \bar{e}_2)$ . Now, suppose  $\text{char } F = 2$ . Then  $\bar{e}_1 - \bar{e}_2 = \bar{e}_1 + \bar{e}_2$  and  $(13)(\bar{e}_1 + \bar{e}_2) = \bar{e}_1 + 2\bar{e}_2 = \bar{e}_1$ . Thus  $\bar{e}_1, \bar{e}_2 \in F[S_3](\bar{e}_1 - \bar{e}_2)$  and therefore  $F[S_3]u = U$ .

We have just shown that  $F[S_3]u = U$  for all  $u \in U$ . Thus  $U$  is simple. The  $\text{char } F = 3$  case is left as an exercise.

Thus  $\rho_3 : G \rightarrow GL_F(F^2) = GL_F(F)$  defined by  $(12) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$  and  $(123) \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$  is the last representation.

**Definition 4.9.** Let  $\rho_1, \rho_2 : G \rightarrow GL_F(V_i)$  for  $i = 1, 2$  be two  $F$ -representations of  $G$ . The **direct sum**  $\rho_1 \oplus \rho_2$  is  $\rho_1 \oplus \rho_2 : F \rightarrow GL_F(V_1 \oplus V_2)$  defined by  $g \mapsto \rho_1(g) \oplus \rho_2(g)$ .

**Note.**  $(V_1 \oplus V_2)_{\rho_1 \oplus \rho_2} \cong (V_1)_{\rho_1} \oplus (V_2)_{\rho_2}$  as  $F[G]$ -modules.

**Remark.** If  $|G| < \infty$  and  $\text{char } F \nmid |G|$ , then every  $F$ -representation of  $G$  is a direct sum of irreducible representations.

**Example.** The regular representation. Let  $G$  be a group,  $F$  a field, and  $V$  an  $F$ -vector space of  $\dim |G|$ . Let  $\{e_g | g \in G\}$  be a basis for  $V$ . For  $h \in G$ , define the  $F$ -linear map  $\tilde{h} : V \rightarrow V$  by  $e_g \mapsto e_{hg}$ . Clearly  $\widetilde{h_1 h_2} = \widetilde{h_1} \widetilde{h_2}$  and  $\widetilde{h^{-1}} = \widetilde{h}^{-1}$ . So  $\tilde{h} \in GL_F(V)$  and  $\rho : G \rightarrow GL_F(V)$  defined by  $h \mapsto \tilde{h}$  is an  $F$ -representation of  $G$ , called the **regular representation** of  $G$ . Note that  $V_\rho \cong F[G]$ . If  $F[G]$  is semisimple, then every  $F[G]$ -module appears in any decompositions of  $F[G]$  into simple left  $F[G]$  modules. Thus every irreducible  $F$  representation of  $G$  appears in any decomposition of the regular representation into irreducible representations.

**Recall.** If  $F = \overline{F}$  and  $\text{char } F \nmid |G|$ , then  $F[G] \cong n_1 I_1 \oplus \cdots \oplus n_t I_t$  where  $I_1, \dots, I_t$  are the distinct simple left ideals (up to isomorphism) and  $n_i = \dim_F I_i$ . Let  $\rho$  be the regular representation and  $\rho_1, \dots, \rho_t$  the distinct irreducible  $F$ -representations of  $G$  corresponding to  $I_i$ . Then  $\rho = n_1 \rho_1 \oplus \cdots \oplus n_t \rho_t$  where  $n_i = \deg \rho_i$ .

## 4.1 Characters

Let  $k$  be a field and  $R$  a finite dimensional  $k$ -algebra. Let  $M$  be a finitely generated left  $R$ -module. So  $\dim_k M < \infty$ . Let  $r \in R$  and define  $\tilde{r}_M : M \rightarrow M$  by  $m \mapsto rm$ . Since  $k \subseteq Z(R)$ , we see  $\tilde{r}_M \in \text{End}_k(M)$ . So  $\text{tr}(\tilde{r}_M) \in F$  is defined. Define the **character**  $\chi_M$  associated with  $M$  by  $\chi_M : R \rightarrow k$  where  $r \mapsto \text{tr}(\tilde{r}_M)$ .

**Remarks.**

1. Let  $B = \{u_1, \dots, u_n\}$  be a  $k$ -basis for  $R$ . Let  $r \in R$ . Then  $r = \sum a_i u_i$  for  $a_i \in k$ . It is easy to see  $\tilde{r} = \sum a_i \tilde{u}_{i,M}$  which implies  $\text{tr}(\tilde{r}_M) = \sum a_i \text{tr}(\tilde{u}_{i,M})$ . So  $\chi_M(r) = \sum_{i=1}^n a_i \chi_M(u_i)$ . So  $\chi_M$  is determined by  $\chi_M|_B$ .
2. If  $R = F[G]$  and  $M$  is a left  $R$ -module, since  $G$  is an  $F$ -basis for  $R$  we often consider  $\chi_M$  to be a function from  $G \rightarrow F$  as opposed to  $R \rightarrow F$ .  
**Note.** If  $\rho : G \rightarrow GL_F(V)$  is an  $F$ -representation of  $G$ , we define the character  $\chi_\rho$  associated to  $\rho$  by  $\chi_\rho := \chi_{V_\rho} : G \rightarrow F$ . Explicitly,  $\chi_\rho(g) = \text{tr}(\rho(g))$ .
3. If  $\text{char } k = 0$ , then  $\chi(1) = \dim_k M$ . If  $\rho : G \rightarrow GL_F(V)$ , then  $\chi_\rho(1) = \dim_F V = \text{deg } \rho$ .

**Proposition 4.10.** *Let  $R$  be a finite dimensional  $k$ -algebra. Let  $0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$  be a short exact sequence of finitely generated left  $R$ -modules. Then  $\chi_M = \chi_L + \chi_N$ .*

*Proof.* Let  $r \in R$  and consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \tilde{r}_L \downarrow & & \tilde{r}_M \downarrow & & \tilde{r}_N \downarrow & & \\ 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

Claim: This is a diagram of  $k$ -linear maps.

Proof: Let  $\ell \in L$ . Then  $f\tilde{r}_L(\ell) = f(r\ell) = r f(\ell) = \tilde{r}_M(f(\ell))$ . Similarly for the other square.

Since the rows split as  $k$ -vector spaces, we see  $M \cong L \oplus N$ . So we have

$$\begin{array}{ccc} M & \xrightarrow{f} & L \oplus N \\ \tilde{r}_M \downarrow & & \tilde{r}_L \oplus \tilde{r}_N \downarrow \\ M & \xrightarrow{f} & L \oplus N \end{array}$$

and  $\tilde{r}_L \oplus \tilde{r}_N$  corresponds to  $\begin{bmatrix} \tilde{r}_L & \\ & \tilde{r}_N \end{bmatrix}$ . This says  $\text{tr}(\tilde{r}_M) = \text{tr}(\tilde{r}_L) + \text{tr}(\tilde{r}_N)$  and thus  $\chi_M(r) = \chi_L(r) + \chi_N(r)$ .  $\square$

**Corollary 4.11.** 1. *If  $N \subseteq M$  are finitely generated  $R$ -modules, then  $\chi_M = \chi_N + \chi_{M/N}$ .*

2.  $\chi_{M \oplus N} = \chi_M + \chi_N$ .

3. *If  $M \cong N$  as  $R$ -modules, then  $\chi_M = \chi_N$ .*

**Examples.** The converse of 3 is not true in general.

1. Let  $k$  be a field,  $R = k[x]/(x^2) \cong k \oplus kx$  as  $k$ -vector spaces. Let  $M = R/(x) \oplus R/(x) \cong k \oplus k$  as  $k$ -vector spaces. Then  $M \not\cong R$  since  $xM = 0$  and  $xR = kx \neq 0$ .

Claim:  $\chi_M = \chi_R$ .

Proof: It is enough to show they agree on the basis  $\{1, x\}$ . Of course,  $\chi_M(1) = \dim M = 2 = \chi_R(1)$ . Also,  $\chi_M(x) = 0$  as multiplication by  $x$  is the 0 map and since  $\tilde{x}_R = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$  we see  $\chi_R(x) = \text{tr}(\tilde{x}_R) = 0$ .

2. Let  $R = \mathbb{F}_2, M = \mathbb{F}_2 \oplus \mathbb{F}_2$ . Then  $\chi_M(1) = 2 = 0$  but obviously  $M \not\cong 0$ .

**Exercise.** If  $R$  is semisimple and finitely generated over  $k$  and  $M$  is simple, then  $\chi_M \neq 0$ .

*Proof.* Note that  $M$  is isomorphic to a simple left ideal of  $R$ , say  $I_i$ , where  $R = n_1 I_1 + \dots + n_t I_t$ . Then  $\chi_M = \chi_i$ . Of course,  $\chi_i(1) = \dim_k I_i \neq 0$ .  $\square$

**Theorem 4.12.** *Let  $R$  be a finite dimensional  $k$ -algebra (for a field  $k$ ),  $\text{char } k = 0$ . Let  $M, N$  be finitely generated semisimple left  $R$ -modules. Then  $\chi_M = \chi_N$  if and only if  $M \cong N$  as  $R$ -modules.*

*Proof.* We've already shown  $\Leftarrow$ , thus we need only show  $\Rightarrow$ . Let  $J = J(R)$ . Since  $M, N$  are sums of simple modules,  $JM = JN = 0$ . Thus  $M, N$  are left  $R/J$ -modules. Since  $R/J$  is semisimple ( $R$  is Artinian and  $J(R/J) = 0$ ), we know  $R/J \cong R_1 \times \cdots \times R_t$ , where  $R_i$  is Artinian, simple with left simple modules  $I_i$ . Let  $I_1, \dots, I_t$  be the distinct simple  $R/J$ -modules. Then  $I_1, \dots, I_t$  are the distinct simple left  $R$ -modules. (Any simple  $R$  module is a simple  $R/J$  module and vice versa). Thus

$$M \cong m_1 I_1 \oplus \cdots \oplus m_t I_t \text{ and } N \cong n_1 I_1 \oplus \cdots \oplus n_t I_t$$

for  $m_i, n_i \geq 0$ . Thus it is enough to show  $m_i = n_i$  for all  $i = 1, \dots, t$ . Let  $e_i \in R$  be such that  $e_i + J$  is the identity of  $R_i$ . Then  $e_i I_j = 0$  for all  $i \neq j$  and  $e_i|_{I_i} = 1|_{I_i}$ . Consider  $(\tilde{e}_i)_M : M \rightarrow M$  defined by  $m \mapsto e_i m$ , a  $k$ -endomorphism. Choose a basis

for  $M$  by taking the union of bases for  $m_j I_j$  for  $j = 1, \dots, t$ . Then  $(\tilde{e}_i)_M =$

$$\begin{bmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & 1_{m_i \dim I_i} & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix}, \text{ where}$$

$1_{m_i \dim I_i}$  is the identity matrix of size  $m_i \dim I_i$ . So  $\chi_M(e_i) = \text{tr}((\tilde{e}_i)_M) = m_i \dim I_i$ . Similarly,  $\chi_N(e_i) = \text{tr}((\tilde{e}_i)_N) = n_i \dim I_i$ . As  $\text{char } k = 0$ , we have  $m_i = n_i$ .  $\square$

**Corollary 4.13.** *Let  $R$  be a semisimple finite dimensional  $k$ -algebra with  $\text{char } k = 0$ . Let  $I_1, \dots, I_t$  be the distinct left simple ideals. Let  $\chi_i = \chi_{I_i}$  for  $i = 1, \dots, t$ . Then  $\chi_1, \dots, \chi_t$  are distinct irreducible  $k$ -characters of  $R$ . Given any finitely generated left  $R$ -module  $M$ , there exist unique  $n_1, \dots, n_t \in \mathbb{Z}$  such that  $\chi_M = n_1 \chi_1 + \dots + n_t \chi_t$  (since characters are additive). If  $n_i > 0$ , say  $\chi_i$  is an **irreducible constituent** of  $\chi_M$ .*

**Example.** Let  $R$  be as above and  $k = \bar{k}$ . For  $R = n_1 I_1 \oplus \cdots \oplus n_t I_t$ , we know  $n_i = \dim_k I_i = \chi_i(1)$ . Thus  $\chi_R = \chi_1(1)\chi_1 + \cdots + \chi_t(1)\chi_t$ .

**Proposition 4.14.** *Let  $G$  be a group,  $F$  a field. Let  $\chi$  be an  $F$ -character of  $G$ . Then for all  $g, x \in G$ , we have  $\chi(g) = \chi(xgx^{-1})$ , that is,  $\chi$  is constant on conjugacy classes.*

*Proof.* Let  $\rho : G \rightarrow GL_F(V)$  be an  $F$ -representation of  $G$  with character  $\chi$ . Then  $\chi(xgx^{-1}) = \text{tr}(\rho(xgx^{-1})) = \text{tr}(\rho(x)\rho(g)\rho(x)^{-1}) = \text{tr}(\rho(g)) = \chi(g)$ .  $\square$

**Examples.** Let  $k = \bar{k}$  and  $\text{char } k = 0$ .

- $G = C_n = \langle a \rangle$ . Since  $G$  is abelian, all representations have deg 1. Then irreducible  $k$ -representations are  $\rho_i = C_n \rightarrow k^*$  defined by  $a \mapsto \omega^i$  for  $i = 0, \dots, n - 1$  where  $\omega$  is a fixed primitive  $n^{\text{th}}$  root of unity. The character  $\chi_i$  associated to  $\rho_i$  is  $\chi_i(a^j) = \omega^{ij}$ . Thus we can construct the **character table**:

	1	$a$	$a^2$
$\chi_0$	1	1	1
$\chi_1$	1	$\omega$	$\omega^2$
$\chi_2$	1	$\omega^2$	$\omega$

where the top row consists of representations for each conjugacy class and the first column consists of the irreducible characters.

2.  $G = V_4 = \{1, a, b, ab\}$ . Recall the representations are  $\rho_{ij} : G \rightarrow k^*$  defined by  $a^i \mapsto (-1)^i$  and  $b^j \mapsto (-1)^j$  for  $i, j \in \{0, 1\}$ .

		1	a	b	ab
$(\rho_{00} \leftrightarrow)$	$\chi_0$	1	1	1	1
$(\rho_{01} \leftrightarrow)$	$\chi_1$	1	-1	1	-1
$(\rho_{10} \leftrightarrow)$	$\chi_2$	1	1	-1	-1
$(\rho_{11} \leftrightarrow)$	$\chi_3$	1	-1	-1	1

3.  $G = S_3$ . Recall that there were two degree 1 representations: the trivial representation  $\rho_0$  and the signed representation  $\rho_1$  and one degree 2 representation:  $\rho_2 : S_3 \rightarrow GL_2(k)$  defined by  $(12) \mapsto \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$  and  $\begin{bmatrix} & -1 \\ 1 & -1 \end{bmatrix}$ . Thus the character table is given by:

	(1)	(12)	(123)	← as there only 3 conjugacy classes
$\chi_0$	1	1	1	
$\chi_1$	1	-1	1	
$\chi_2$	2	0	-1	← Remember we just want the trace of the matrices

Note that the first column is always just the degree of the representation.

4.  $G = Q_8 = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, ab = b^3a \rangle$ . Note that any normal subgroup of  $Q_8$  induces the homomorphism  $G \rightarrow G/H \rightarrow GL_F(V)$ . Let  $Z = Z(G) = \{\pm 1\}$ . Then  $G/Z \cong V_4$ . Recall that this has 4 degree 1 representations, namely  $\rho_{ij} : Q_8 \rightarrow k^*$  by  $a \mapsto (-1)^i$  and  $b \mapsto (-1)^j$  where  $i, j \in \{0, 1\}$ . As  $G$  is not abelian, we know there must exist a representation of degree  $\geq 2$ . Furthermore, as  $\sum_{i=1}^t n_i^2 = |G| = 8$ , we see there can exist only one more representation, which must have degree 2. Note that  $\begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$  and  $\begin{bmatrix} & \omega \\ \omega & \end{bmatrix}$  (where  $\omega$  is a primitive 4<sup>th</sup> root of unity (for  $k = \mathbb{C}, \omega = \pm i$ )) satisfy the relations of  $G$ . So define  $\rho_4 : Q_8 \rightarrow GL_2(k)$  by  $a \mapsto \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$  and  $b \mapsto \begin{bmatrix} & \omega \\ \omega & \end{bmatrix}$

Note that then  $c \mapsto \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \begin{bmatrix} & \omega \\ \omega & \end{bmatrix} = \begin{bmatrix} \omega & \\ & -\omega \end{bmatrix}$ . Thus our character table is given by

	1	-1	a	b	c
$\chi_0$	1	1	1	1	1
$\chi_1$	1	1	1	-1	-1
$\chi_2$	1	1	-1	1	-1
$\chi_3$	1	1	-1	-1	1
$\chi_4$	2	-2	0	0	0

For  $-1$ , just note that since  $-1 \in Z(G)$ ,  $-1$  is  $1 \in G/Z(G)$ . So  $\chi_i(-1) = \chi_i(1)$  for  $i = 0, \dots, 3$ . For  $\chi_4$ , we know  $-1 \mapsto -I$ , which has trace  $-2$ .

Let  $G$  be a finite group,  $k = \bar{k}$ , with  $\text{char } k \nmid |G|$ . Recall  $k[G] \cong B_1 \times \dots \times B_t$  with  $B_i$  simple and Artinian. Let  $e_i \in B_i$  be the identity element. Then  $\{e_1, \dots, e_t\}$  are uniquely determined by  $k[G]$ . Recall  $Z(k[G]) = Z(B_1) \times \dots \times Z(B_t)$  where  $Z(B_i) = Z(M_n(k)) = \{\lambda I_n \mid \lambda \in k\} = ke_i$ . Thus  $Z(k[G]) = ke_1 \times \dots \times ke_t$ . On the other hand, we know  $Z(k[G]) = kz_1 \oplus \dots \oplus kz_t$  where  $z_i = \sum_{g \in C_i} g$  where  $C_1, \dots, C_t$  are the distinct conjugacy classes of  $G$ .

Let  $\chi_1, \dots, \chi_t$  be the irreducible characters of  $G$  associated to the simple left ideals  $I_1, \dots, I_t$ , respectively and where  $B_i \cong n_i I_i$  (as  $k$ -vector spaces). Recall  $\dim_k I_i = n_i$ . Let  $m_i = |C_i|$  for  $i = 1, \dots, t$ .

**Theorem 4.15.** *With the above notation,*

1.  $e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$  for  $i = 1, \dots, t$ .

2.  $z_i = m_i \sum_{j=1}^t \frac{\chi_i(g)e_j}{n_j}$  for  $g \in C_i$ .

In particular, (1) says  $\text{char } k \nmid n_i$ .

*Proof.* Let  $\phi$  be the character associated to the regular representation of  $G$ . Recall

(a)  $\phi = n_1\chi_1 + \dots + n_t\chi_t$ .

(b)  $\phi(1) = |G|$ .

(c)  $\phi(g) = 0$  for all  $g \neq 1$  (as for  $V = \{e_h | e_h \in G\}$ ,  $\rho : G \rightarrow GL_k(V)$  defined by  $g \cdot e_h = e_{gh} \neq e_h$  if  $g \neq 1$ . Thus  $\text{tr}(\rho(g)) = 0$  if  $g \neq 1$ .)

1. Let  $e_i = \sum_{g \in G} a_{ig}g$  for  $a_{ig} \in k$ . Want to show  $a_{ig} = \frac{n_i\chi_i(g^{-1})}{|G|}$ . Let  $h \in G$  and consider  $\phi(e_i h^{-1}) = \sum_{g \in G} a_{ig}\phi(gh^{-1}) = a_{ih}|G|$  by (b) and (c). By (a),  $\phi(e_i h^{-1}) = \sum_{j=1}^t n_j\chi_j(e_i h^{-1})$ , where  $\chi_j(e_i h^{-1}) = \text{tr}(\widetilde{e_i h^{-1}}_{I_j}) = \text{tr}(\delta_{ij}\widetilde{h^{-1}}_{I_j}) = \delta_{ij}\chi_j(h^{-1})$  as  $\widetilde{e_i}$  annihilates  $I_j$  but is the identity on  $I_i$ . Thus  $a_{ih}|G| = \phi(e_i h^{-1}) = n_i\chi_i(h^{-1})$ . Thus  $a_{ih} = \frac{n_i\chi_i(h^{-1})}{|G|}$ .
2. Let  $g \in C_i, z_i = \sum_{j=1}^t b_{gj}e_j$ . Then  $\chi_j(z_i) = m_i\chi_j(g)$  as  $z_i = \sum_{h \in C_i} h$  and  $\chi_j(\sum_{\ell=1}^t b_{g\ell}e_\ell) = \sum_{\ell=1}^t b_{g\ell}\chi_j(e_\ell) = b_{gj}\chi_j(e_j) = b_{gj}\text{tr}(id_{I_j}) = b_{gj}n_j$ . Thus  $b_{gj} = \frac{m_i\chi_j(g)}{n_j}$  which implies  $z_i = m_i \sum_{j=1}^t \frac{\chi_j(g)e_j}{n_j}$ . [It should be noted here that we mean  $\overline{n_j} \in k$ , however, we will just say  $n_j$  for simplicity]  $\square$

**Corollary 4.16.** *With the above notation ( $|G| < \infty, \text{char } k \nmid |G|, k = \overline{k}$ ), let  $\chi_1, \dots, \chi_t$  be the irreducible characters of  $G$ . Then*

1. For  $i, j$  we have  $\sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}|G|$ .
2. For all  $g, h \in G$ , we have  $\sum_{i=1}^t \chi_i(g)\chi_i(h^{-1}) = \delta|C_G(g)|$ , where  $C_G(g) := \{x \in G | xg = gx\}$  and  $\delta = 1$  if  $g, h$  are in the same conjugacy class and  $\delta = 0$  otherwise.
3. If  $g \neq 1$ , then  $\sum_{i=1}^t \chi_i(1)\chi_i(g) = 0$ .

*Proof.* 1. By the Theorem,  $e_i = \frac{n_i}{|G|} \sum \chi_i(g^{-1})g$ . Apply  $\chi_j$  to both sides. Then  $\chi_j(e_i) = \delta_{ij}n_i$ . So  $\delta_{ij}n_i = \frac{n_i}{|G|} \sum \chi_i(g^{-1})\chi_j(g)$ . Thus  $\delta_{ij}|G| = \sum \chi_i(g^{-1})\chi_j(g)$ .

2. Plug 1 of the theorem into 2 of the theorem to get for  $g \in C_i, z_i = \frac{m_i}{|G|} \sum_{h \in G} (\sum_{j=1}^t \chi_j(g)\chi_j(h^{-1}))h$ . Comparing coefficients,  $\frac{m_i}{|G|} \sum_{j=1}^t \chi_j(g)\chi_j(h^{-1}) = 1$  if and only if  $h \in C_i$  (and 0 otherwise). Now,  $m_i = |C_i| = \frac{|G|}{|C_G(g)|}$ .

3. Follows from 2 by letting  $h = 1$ .  $\square$

**Definition 4.17.** *A  $k$ -class function on  $G$  is a function  $\phi : G \rightarrow k$  which is constant on conjugacy classes, that is,  $\phi(g) = \phi(xgx^{-1})$  for all  $x, g \in G$ . Let  $F_k(G)$  be the set of  $k$ -class functions of  $G$ .*

**Remark.**  $F_k(G)$  is a  $k$ -vector space in a natural way

$$(\phi + \psi)(g) = \phi(g) + \psi(g) \text{ and } (a\phi)(g) = a\phi(g) \text{ for all } g \in G, a \in k.$$

The  $\dim_k F_k(G)$  is the number of conjugacy classes. We can define an inner product (which is bilinear) on  $F_k(G)$  via

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g^{-1})\psi(g).$$

**Proposition 4.18.** *With the above notation, the set of irreducible characters on  $G$ ,  $\{\chi_1, \dots, \chi_t\}$ , is an orthonormal basis for  $F_k(G)$ .*

*Proof.* We've shown  $\langle \chi_i, \chi_k \rangle = \delta_{i,j}$ . Since  $\dim_k F_k(G) = t$ , we see that it is a basis.  $\square$



**Examples.**

1.  $G = A_4$  (where  $\text{char } k \neq 2, 3$ ). First, we need to find the conjugacy classes. Let  $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ . Then  $H \triangleleft A_4$  and the conjugacy classes are  $\{1\}, H \setminus \{1\}, (123)H, (132)H$ . Thus there are 4 irreducible characters. Note that  $G/H \cong C_3$ , which gives us 3 degree 1 representations. Since  $\sum n_i^2 = |G|$ , we see there is only one other, which has degree 3. Now, we can fill out the character table:

	(1)	(12)(34)	(123)	(132)	
$\chi_1$	1	1	1	1	
$\chi_2$	1	1	$\omega$	$\omega^2$	
$\chi_3$	1	1	$\omega^2$	$\omega$	
$\chi_4$	3	-1	0	0	$\leftarrow$ for this row, recall $\chi_4(1) = \deg \rho_4$ and $0 = \sum_{i=1}^t \chi_i(g)\chi_i(1)$ .

Since  $(12)(34) \in H$ , it acts like (1) on  $\chi_1, \chi_2, \chi_3$ .

What is a representation with character  $\chi_4$ ? Let  $V = ke_1 \oplus ke_2 \oplus ke_3 \oplus ke_4 / k(e_1 + e_2 + e_3 + e_4) \cong k\bar{e}_1 \oplus k\bar{e}_2 \oplus k\bar{e}_3$ , where  $\bar{e}_4 = -\bar{e}_1 - \bar{e}_2 - \bar{e}_3$ . Now, make  $V$  into a  $k[A_4]$ -module by defining  $\sigma\bar{e}_i = \bar{e}_{\sigma(i)}$  for all  $\sigma \in A_4, i = 1, 2, 3$ . This is well-defined as  $\sigma e_i = e_{\sigma(i)}$  is well-defined and  $\sigma$  fixes  $e_1 + e_2 + e_3 + e_4$ . Thus  $V$  gives rise to a degree 3 representation of  $A_4$ . Let  $\chi$  be the associated character.

Claim:  $\chi = \chi_4$  (that is,  $\chi$  is irreducible)

Proof: If  $\chi \neq \chi_4$ , then it is reducible. Thus it is a sum of irreducible characters, which implies  $\chi = \chi_1 + \chi_2 + \chi_3$ .

Then,  $\chi((12)(34)) = \chi_1 + \chi_2 + \chi_3 = 3$ . However,  $\chi((12)(34)) = \text{tr}(\rho((12)(34))) = \text{tr} \begin{bmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{bmatrix} = -1$ .

This shows that, since  $\chi$  is irreducible,  $V$  is simple.

2.  $G = S_4$ . Here, the conjugacy classes are (1), (12), (12)(34), (123), (1234). Note that  $H$  above is still normal in  $S_4$ . Here,  $|S_4/H| = 6$ . Since every element of  $S_4$  has order  $\leq 4$ , we see  $S_4/H \cong S_3$ .

	(1)	(12)	(12)(34)	(123)	(1234)	
$\chi_1$	1	1	1	1	1	
$\chi_2$	1	-1	1	1	-1	
$\chi_3$	2	0	2	-1	0	
$\chi_4$	3	1	-1	0	-1	$\leftarrow V$ , the $k[A_4]$ -module above is also a simple $k[S_4]$ -module
$\chi_5$	3	-1	-1	0	1	$\leftarrow$ Use the fact that $\sum_{i=1}^t \chi_i(1)\chi_i(g) = 0$ .

For  $\chi_1, \chi_2, \chi_3$ , note that (12)(34) maps to 1 in  $S_4/H$  and (1234) maps to a transposition in  $S_4/H$ .

By HW6# 6, if  $k = \mathbb{C}$ , we see  $\frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}$ .

**Corollary 4.19.** Suppose  $k = \mathbb{C}$ . With the above notation,  $\frac{1}{|G|} \sum_{g \in G} |\chi_i(g)|^2 = 1$  and  $\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = 0$  for  $i \neq j$ .

Let  $g_i \in C_i$  for  $i \in [t]$  and  $m_i = |C_i|$ . Then  $\sum_{i=1}^t m_i \chi_j(g_i)\overline{\chi_\ell(g_i)} = \delta_{j\ell}|G|$ .

**Facts.** Let  $G$  be a finite group,  $\rho : G \rightarrow GL_{\mathbb{C}}V$  a finite dimensional representation with associated character  $\chi$ . Say  $\deg \rho = n$ . Then  $GL_{\mathbb{C}}V = GL_n(\mathbb{C})$ .

1. For all  $g \in G, |\chi(g)| \leq \chi(1)$ .
2.  $\chi(g) = \chi(1)$  if and only if  $g \in \ker \rho$ .

*Proof.* 1. Let  $\lambda_1, \dots, \lambda_n$  be the eigenvalues of  $\rho(g)$ . Then  $\lambda_1, \dots, \lambda_n$  are roots of unity. So  $|\chi(g)| = |\lambda_1 + \dots + \lambda_n| \leq |\lambda_1| + \dots + |\lambda_n| = n \cdot 1 = \chi(1)$ .

2. The backward direction is clear. So assume  $\chi(g) = \chi(1)$ . Then, by (1),  $\lambda_1 + \dots + \lambda_n = n$ . By Cauchy Schwarz,  $|\lambda_1 + \dots + \lambda_n| = |\lambda_1| + \dots + |\lambda_n|$  if and only if  $\lambda_i = \lambda_j$  for all  $i, j$ . Then  $n\lambda_1 = n$  which implies  $\lambda_1 = 1$ . Thus  $\lambda_i = 1$  for all  $i$ . Since the minimal polynomial divides  $x^n - 1$ ,  $\rho(g)$  is diagonalizable and since it is similar to the identity matrix, it is in fact the identity matrix.  $\square$

### Examples.

1. Recall  $(12)(34) \in H \triangleleft A_4$  and  $\chi_i((12)(34)) = \chi_i(1)$  for  $i = 1, 2, 3$ .
2. Let  $F = \mathbb{R}, G = C_4 = \langle g \rangle$ . Then

$$\mathbb{R}[G] = \mathbb{R} \cdot 1 \oplus \mathbb{R}g \oplus \mathbb{R}g^2 \oplus \mathbb{R}g^3 = \mathbb{R}[x]/(x^4 - 1) \cong \mathbb{R}[x]/(x - 1) \oplus \mathbb{R}[x]/(x + 1) \oplus \mathbb{R}[x]/(x^2 + 1).$$

Let  $\rho_1 : G \rightarrow \mathbb{R}^*$  be defined by  $g \mapsto 1$ ,  $\rho_2 : G \rightarrow \mathbb{R}^*$  be defined by  $g \mapsto -1$ , and  $\rho_3 : G \rightarrow \mathbb{R}^*$  be defined by  $g \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ . Then  $\rho_i$  is a representation of the  $i^{\text{th}}$  summand on the right hand side of the above equation.

Now, let  $\phi : G \rightarrow GL_4(\mathbb{R})$  be defined by  $g \mapsto \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 0 & -1 \\ & & 1 & 0 \end{bmatrix}$ . Then  $\phi = \rho_1 \oplus \rho_2 \oplus \rho_3$ . Also, if we define

$\rho : C_4 \rightarrow GL_4(\mathbb{R})$  by  $g \mapsto \begin{bmatrix} & & & 1 \\ & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{bmatrix}$ . Then  $\rho \cong \phi$ .

## 4.2 Integral Extensions

Our goal is to work towards proving Burnside's Theorem, which says *Every group of order  $p^a q^b$  (for  $p, q$  primes) is solvable.*

**Definition 4.20.** Let  $R \subset S$  be commutative rings,  $u \in S$ . Then  $u$  is **integral** over  $R$  if  $f(u) = 0$  for some monic polynomial  $f(x) \in R[x]$ . We say  $S$  is **integral over  $R$**  if every element of  $S$  is integral over  $R$ .

**Remark.** If  $E/F$  is a field extension, then  $\alpha \in E$  is integral over  $F$  if and only if  $\alpha$  is algebraic over  $F$ .

**Proposition 4.21.** Let  $R \subset S$  be commutative rings,  $u \in S$ . TFAE

1.  $u$  is integral over  $R$ .
2.  $R[u]$  is a finitely generated  $R$ -module
3. There exists a faithful  $R[u]$ -submodule  $M$  of  $S$  which is finitely generated as an  $R$ -module. (Recall faithful means  $\text{Ann}_{R[u]} M = 0$ )

**Note.** The above are also equivalent to "There exists a finitely generated  $R$ -submodule  $M$  of  $S$  such that  $1 \in M$  and  $uM \subseteq M$ ."

*Proof.* (1)  $\Rightarrow$  (2) There exists an equation of the form  $u^n + r_1 u^{n-1} + \dots + r_n = 0$ ,  $r_i \in R$ . Then  $u^{n+k} \in R \cdot 1 + \dots + Ru^{n-1}$  for all  $k \geq 0$ . So  $R[u] = R \cdot 1 + \dots + Ru^{n-1}$ , a finitely generated  $R$ -module.

(2)  $\Rightarrow$  (3) Let  $M = R[u]$ .  $M$  is faithful as  $1 \in M$ . Of course  $uR[u] \subseteq R[u]$ .

(3)  $\Rightarrow$  (1) “determinant trick.” Recall: Let  $R$  be a commutative ring,  $A \in M_n(R)$ . Define the adjoint of  $A$  by  $\text{adj}A = (b_{ij})_{n \times n}$  where  $b_{ij} = (-1)^{i+j} \det(A_{ji})$  where  $A_{ji}$  is the  $(n-1) \times (n-1)$  matrix obtained by deleting the  $j^{\text{th}}$  row and  $i^{\text{th}}$  column. Also,  $A \cdot (\text{adj}A) = (\det A)I_n = (\text{adj}A) \cdot A$  (p 511). Let  $M = Rx_1 + \dots + Rx_n \subseteq S$ ,  $\text{Ann}_R M = 0$ ,  $uM \subseteq M$ .

For  $j, i = 1, \dots, n$  there exists  $r_{ij} \in R$  such that  $ux_i = \sum r_{ij}x_j$ , that is,  $uI_n \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  for  $A \in M_n(R)$ .

Then  $(uI_n - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$ . Say  $B := uI_n - A$ . Multiply both sides by  $\text{adj}B$ . Then  $0 = \text{adj}(B)B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} =$

$(\det B)I \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  which implies  $(\det B)M = 0$ . But  $M$  is faithful and  $\det B \in R[u]$ . Thus  $\det B = 0$ . One can show

$\det B$  has the form  $u^n + t_1u^{n-1} + \dots + t_n$  for  $t_i \in R$ . Thus  $u^n + t_1u^{n-1} + \dots + t_n = 0$  which implies  $u$  is integral over  $R$ .  $\square$

**Corollary 4.22.**  $S/R$  as above,  $u \in S$ . Then TFAE

1.  $u$  is integral over  $R$ .
2.  $R[u]$  is a finitely generated  $R$ -module.
3.  $R[u]$  is integral over  $R$ .

*Proof.* Let  $\beta \in R[u]$  and  $M = R[u]$  from theorem. Then  $\beta M \subseteq M$  (that is,  $M$  is an  $R[\beta]$ -module),  $1 \in M$ . By (2),  $M$  is a finitely generated  $R$ -module. By (3) of the theorem,  $\beta$  is integral.  $\square$

**Exercise.**  $S/R$  as above and  $u_1, \dots, u_n \in S$ . Then TFAE

1.  $u_1, \dots, u_n$  are integral over  $R$ .
2.  $R[u_1, \dots, u_n]$  is a finitely generated  $R$ -module.
3.  $R[u_1, \dots, u_n]$  is integral over  $R$ .

**Corollary 4.23.**  $R \subseteq S$  as above.

1. If  $S$  is finitely generated as an  $R$ -module, then  $S$  is integral over  $R$ .
2. If  $S$  is integral over  $R$ , then  $S$  is finitely generated over  $R$  as an algebra if and only if  $S$  is finitely generated over  $R$  as a module.

**Examples.**

1. Let  $K$  be a field,  $R = k[t^2, t^3]$ ,  $S = k[t]$ . Then  $t$  is integral over  $R$  (it is a root of  $x^2 - t^2 \in R[t]$ ) and so  $S$  is integral over  $R$ . Note that  $S$  is contained in the field of fractions. Also,  $S$  is integral over  $R$  and finitely generated as an  $R$ -algebra. Thus  $S$  is finitely generated as an  $R$ -module ( $S = R + Rt$ ).
2. Let  $S = \mathbb{Z}[\frac{3+\sqrt{5}}{2}]$  and  $R = \mathbb{Z}[\sqrt{5}]$ . Note  $S \subseteq Q(R) = \mathbb{Q}(\sqrt{5})$ . Note  $\frac{3+\sqrt{5}}{2}$  is integral over  $R$  as it is a root of  $x^2 - 3x + 1 \in \mathbb{Z}[x]$ . Thus  $S$  is integral over  $R$  and finitely generated as an  $R$ -module.

**Corollary 4.24.** Let  $R \subseteq S$  as above. Let  $T = \{\alpha \in S \mid \alpha \text{ is integral over } R\}$ . Then  $T$  is a subring of  $S$  which is integral over  $R$ .  $T$  is called the **integral closure** of  $R$  in  $S$ . If  $T = R$ , then  $T$  is said to be **integrally closed** in  $S$ .

*Proof.* Follows from above exercise as  $\alpha\beta, \alpha \pm \beta \in R[\alpha, \beta]$  which is integral over  $R$  when  $\alpha, \beta$  are integral.  $\square$

**Example.** Let  $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ is integral over } \mathbb{Z}\}$ . Then  $A$  is a ring. The elements of  $A$  are called **algebraic integers**. Note  $A$  is integral over  $\mathbb{Z}$ , but not finitely generated over  $\mathbb{Z}$  (as either a module or algebra, by the corollary).

**Definition 4.25.** Let  $R$  be a commutative domain. Let  $Q$  be its field of fractions. The **absolute integral closure** of  $R$ , denoted  $R^+$ , is  $R^+ = \{\alpha \in \overline{Q} : \alpha \text{ is integral over } R\}$  where  $\overline{Q}$  is some algebraic closure of  $Q$ .

**Theorem 4.26** (Hochster-Heneke, 1993). If  $\text{char } R = p$ , then  $R^+$  is a Cohen-Macaulay  $R$ -algebra.

**Definition 4.27.** Let  $R$  be a domain. Say  $R$  is **integrally closed** (or **normal**) if  $R$  is integrally closed in its field of fractions.

**Proposition 4.28.** Let  $R$  be a UFD. Then  $R$  is integrally closed.

*Proof.* Let  $\frac{a}{b} \in Q(R)$  be integral over  $R$ . WLOG, assume  $\gcd(a, b) = 1$ . So  $(\frac{a}{b})^n + r_1(\frac{a}{b})^{n-1} + \dots + r_{n-1}(\frac{a}{b}) + r_n = 0$  where  $r_i \in R$ . Multiply by  $b^n$  to get  $a^n + \underbrace{r_1ba^{n-1} + \dots + r_{n-1}b^{n-1}a + r_nb^n}_{b \text{ divides these}} = 0$ . Thus  $b \mid a^n$ . But  $\gcd(a^n, b) = 1$ . So  $b$  is a unit of  $R$  which implies  $\frac{a}{b} \in R$ . □

**Note.** This says that PIDs are integrally closed.

**Corollary 4.29.** The only rational algebraic integers are integers.

**Remark.** Let  $R \subseteq S$  be commutative rings,  $I$  an ideal of  $S$ . Then  $\phi : R/(I \cap R) \rightarrow S/I$  defined by  $r + I \cap R \mapsto r + I$  is an injective ring homomorphism. So we can consider  $R/(I \cap R)$  as a subring of  $S/I$ , where multiplication is defined by  $\bar{r} \cdot \bar{s} = \overline{rs}$  (that is,  $(r + I \cap R)(s + I) = rs + I$  is well-defined).

**Lemma 4.30.** If  $S$  is integral over  $R$  and  $I$  is an ideal of  $S$ , then  $S/I$  is integral over  $R/I \cap R$ .

*Proof.* Let  $s \in S$ . Then  $s^n + r_1s^{n-1} + \dots + r_n = 0$  for  $r_i \in R$ . By the remark, modding out by  $I$  gives  $\bar{s}^n + \bar{r}_1\bar{s}^{n-1} + \dots + \bar{r}_n = 0$  where  $\bar{r}_i \in R/(I \cap R)$ . □

**Proposition 4.31.** Let  $S$  be integral over  $R$ . Let  $p \in \text{Spec } S$ . Then  $p$  is maximal in  $S$  if and only if  $p \cap R$  is maximal in  $R$ .

*Proof.* By lemma,  $S/p$  is integral over  $R/p \cap R$ . Also,  $S/p$  and  $R/p \cap R$  are domains (as  $p, p \cap R$  are prime). Thus it is enough to prove:

Claim: If  $S$  is integral over  $R$  and both are domains, then  $S$  is a field if and only if  $R$  is a field.

*Proof:*

$\Leftarrow$  Suppose  $R$  is a field. Let  $u \in S \setminus \{0\}$ . Then  $u$  is integral over  $R$  which implies  $u$  is algebraic over  $R$ . Since  $R[u] \subseteq S$  is a domain and is a finite dimensional  $R$ -vector space,  $R[u]$  is a field. Thus  $u^{-1} \in R[u] \subseteq S$ .

$\Rightarrow$  Suppose  $S$  is a field. Let  $u \in R \setminus \{0\}$ . Then  $u^{-1} \in S$  is integral over  $R$ . Then  $(u^{-1})^n + r_1(u^{-1})^{n-1} + \dots + r_n = 0$  for  $r_i \in R$  and multiplication by  $u^{n-1}$  gives  $u^{-1} + r_1 + \dots + r_n u^{n-1} = 0$ . Thus  $u \in R$ . □

Suppose  $R \supseteq S$  are commutative rings,  $Q$  a multiplicatively closed subset of  $R$ . Since localization is exact,  $R_W \subseteq S_W$  (as rings).

**Proposition 4.32.** If  $S/R$  is integral,  $W$  is a multiplicatively closed subset of  $R$ , then  $S_W$  is integral over  $R_W$ .

*Proof.* Let  $\frac{s}{w} \in S_W$ . Since  $S/R$  is integral, there exists an equation of the form  $s^n + r_1s^{n-1} + \dots + r_1s + r_n = 0$ , for  $r_i \in R$ . Divide by  $w^n$  to get  $(\frac{s}{w})^n + \frac{r_1}{w}(\frac{s}{w})^{n-1} + \dots + \frac{r_{n-1}}{w^{n-1}}(\frac{s}{w}) + \frac{r_n}{w^n} = 0$ . Thus  $\frac{s}{w}$  is integral over  $R_W$ . □

**Remark.** Let  $N_1, N_2$  be  $R$ -submodules of  $M$  and  $W$  a multiplicatively closed subset. Then  $(N_1 \cap N_2)_W = (N_1)_W \cap (N_2)_W$ .

**Lying Over (LO) Theorem.** (Cohen - Seidenberg) *Let  $S/R$  be an integral extension. Given  $p \in \text{Spec}R$ , there exists  $P \in \text{Spec}S$  such that  $P \cap R = p$ .*

*Proof.* Let  $W = R - p$ , a multiplicatively closed subset of  $R$ . Then  $p_W$  is the unique maximal ideal of  $R_W$ . As noted,  $S_W$  is integral over  $R_W$ . Let  $P \in \text{Spec}S$  be such that  $P_W$  is maximal in  $S_W$  (as maximal ideals of  $S_W$  correspond to maximal ideals of  $S$ ). By a previous proposition,  $P_W \cap R_W$  is maximal in  $R_W$ . Since  $p_W$  is unique,  $p_W = P_W \cap R_W = (P \cap R)_W$ . Note  $P \cap R \in \text{Spec}R$ . By the one-to-one correspondence between primes of  $R$  which do not intersect  $W$  and  $\text{Spec}R_W$ , we have  $P \cap R = p$ .  $\square$

**Incomparable (INC) Theorem.** *Let  $S/R$  be integral and  $P_1, P_2 \in \text{Spec}S$  such that  $P_1 \cap R = P_2 \cap R$ . Then  $P_1, P_2$  are incomparable (that is,  $P_1 \not\subset P_2$  and  $P_2 \not\subset P_1$ ).*

*Proof.* Let  $p \in P_1 \cap R = P_2 \cap R \in \text{Spec}R$ . Localize at  $W = R - p$ . Then  $(P_1)_W, (P_2)_W \in \text{Spec}S_W$  and are  $\neq S$ . Also  $(P_1)_W \cap R_W = p_W = (P_2)_W \cap R_W$ . Therefore, it is enough to show in the case that  $P_1 \cap R = P_2 \cap R$  is maximal in  $R$ . Then  $P_1, P_2$  are maximal in  $S$ . Hence  $P_1 \not\subset P_2$  and  $P_2 \not\subset P_1$ .  $\square$

**Going Up (GU) Theorem.** *Let  $S/R$  be integral and  $p \subset q$  primes of  $R$ . Let  $P \in \text{Spec}S$  such that  $P \cap R = p$ . Then there exists  $Q \in \text{Spec}S$  such that  $P \subset Q$  and  $Q \cap R = q$ .*

*Proof.* By localizing at  $Q = R - q$ , we can reduce to the case that  $q$  is maximal. Thus it is enough to prove in the case that  $(R, q)$  is quasilocal. Let  $Q$  be any maximal ideal of  $S$  containing  $P$ . Then  $Q \cap R$  is maximal in  $R$  which says  $Q \cap R = q$ .  $\square$

**Theorem 4.33.** *Let  $S/R$  be an integral extension. Then  $\dim S = \dim R$ .*

*Proof.* Let  $Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_n$  be a chain of primes of  $S$ . Intersect with  $R$  to get  $Q_0 \cap R \subset Q_1 \cap R \subset \dots \subset Q_n \cap R$ , a chain of primes in  $R$ . By the INC Theorem, these are still proper containments. Thus  $\dim R \geq \dim S$ . Let  $p_0 \subsetneq p_1 \subsetneq \dots \subsetneq p_n$  be a chain of primes of  $R$ . By the LO Theorem, there exists  $Q_0 \in \text{Spec}S$  such that  $Q_0 \cap R = p_0$ . Now use the GU Theorem  $n$  times to get  $Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_n$  where  $Q_i \cap R = p_i$ . Then  $\dim S \geq \dim R$ .  $\square$

Setup: Let  $G$  be a finite group,  $k = \bar{k}$  a field,  $\text{char } k \nmid |G|$ . Then  $k[G]$  is semisimple and thus  $k[G] = B_1 \times \dots \times B_t$  where  $B_i$  are Artinian simple rings. Let  $e_i$  be the identity of  $B_i$ . Let  $C_1, \dots, C_t$  be the conjugacy classes of  $G$  and  $z_i = \sum_{g \in C_i} g$ . We've proved  $Z(k[G]) = ke_1 \times \dots \times ke_t$  as rings and  $Z(k[G]) = kz_1 \oplus \dots \oplus kz_t$  as  $k$ -modules. If  $R$  is a commutative ring, then  $R[G] = \bigoplus_{g \in G} Rg$  and one can show that  $Z(R[G]) = Rz_1 \oplus \dots \oplus Rz_t$ . Now, assume  $\text{char } k = 0$ . Then  $\mathbb{Z} \subseteq k$  and as  $k$  is a field, this says  $\mathbb{Q} \subseteq k$ .

**Remark.** If  $\text{char } k = 0, k = \bar{k}$ , then  $Z(\mathbb{Z}[g]) = \mathbb{Z}z_1 \oplus \dots \oplus \mathbb{Z}z_t \subseteq kz_1 \oplus \dots \oplus kz_t = Z(k[G])$ .

**Theorem 4.34.** *Let  $\text{char } k = 0$  and  $\chi_1, \dots, \chi_t$  be the irreducible characters of  $G$  where  $\chi_i$  correspond to  $B_i$ . Let  $m_i = |C_i|$ . Then for all  $i, j \in [t], g \in C_j$  we have  $\frac{m_j \chi_i(g)}{\chi_i(1)} \in k$  is integral over  $\mathbb{Z}$ . Thus  $z_i \in Ae_1 + \dots + Ae_t$ , where  $A$  is the integral closure of  $\mathbb{Z}$  in  $k$ .*

*Proof.* Recall that  $z_j = m_j \sum_{i=1}^t \frac{\chi_i(g)e_i}{\chi_i(1)}$ . Now  $z_j \in Z(\mathbb{Z}[G]) = \mathbb{Z}z_1 + \dots + \mathbb{Z}z_t$ , which is a ring and a finitely generated  $\mathbb{Z}$ -module. Thus  $z_j$  is integral over  $\mathbb{Z}$ . Also,  $z_j \in Z(k[G]) = ke_1 + \dots + ke_t$ . Say  $z_j = \sum_{i=1}^t \alpha_i e_i$  for  $\alpha_i \in k$ . Let  $f(x) \in \mathbb{Z}[x]$  be monic such that  $f(z_i) = 0$ . Then

$$0 = f(z_i) = f(\alpha_1 e_1 + \dots + \alpha_t e_t) = f(\alpha_1) e_1 + \dots + f(\alpha_t) e_t$$

as  $e_i e_j = \delta_{ij} e_i$ . as  $e_1, \dots, e_t$  are linearly independent over  $k$ , we must have that  $f(\alpha_i) = 0$  for all  $i$ . Thus  $\alpha_i \in A$  for all  $i$ . Thus  $z_i \in Ae_1 + \dots + Ae_t$ .  $\square$

**Lemma 4.35.** Let  $A$  be the integral closure of  $\mathbb{Z}$  in  $k$  and  $\chi$  be any character of  $G$ . Then  $\chi(g) \in A$  for all  $g \in G$ .

*Proof.* Note that  $\chi(g) = \sum \lambda_i$ , where  $\lambda_i$  are the eigenvalues of  $\rho(g)$  for  $\rho : G \rightarrow GL_k(V)$  a representation associated to  $\chi$ . Recall  $\lambda_i$  is a root of unity. Thus  $\lambda_i \in A$  for all  $i$ . Since  $A$  is a ring,  $\chi(g) \in A$ .  $\square$

**Theorem 4.36.** With the above notation,  $n_i \mid |G|$  for all  $i = 1, \dots, t$ .

*Proof.* Recall that  $e_i = \frac{n_i}{|G|} \sum_{j=1}^t m_j \chi_i(g_j^{-1}) z_j$  where  $g_i \in C_i$ . Thus  $\frac{|G|}{n_i} e_i = \sum_{j=1}^t m_j \chi_i(g_j^{-1}) z_j$ , where  $m_j \chi_i(g_j^{-1}) \in A$ . Thus  $\frac{|G|}{n_i} e_i \in Az_1 + \dots + Az_t \subseteq Ae_1 + \dots + Ae_t$ . Since the  $e_i$ 's are linearly independent, we must have  $\frac{|G|}{n_i} \in A \cap \mathbb{Q} \subseteq \mathbb{Z}$  as  $\mathbb{Z}$  is integrally closed. Thus  $n_i \mid |G|$ .  $\square$

### 4.3 Representations of Products of Groups

Let  $\rho_i : G_i \rightarrow GL_k(V_i)$ , for  $i = 1, 2$ , be  $k$ -representations of  $G_i$ . Define the **tensor product**  $\rho_1 \otimes \rho_2$  by  $\rho_1 \otimes \rho_2 : G_1 \times G_2 \rightarrow GL_k(V_1 \otimes V_2)$  by  $(g_1, g_2) \mapsto \rho(g_1) \otimes \rho(g_2)$ . This is easily seen to be a representation of  $G_1 \times G_2$  of degree  $(\deg \rho_1)(\deg \rho_2)$ . Now  $\chi_{\rho_1 \otimes \rho_2}(g_1, g_2) = \text{tr}_k(\rho_1(g_1) \otimes \rho_2(g_2)) = \text{tr}_k(\rho_1(g_1)) \text{tr}_k(\rho_2(g_2)) = \chi_{\rho_1}(g_1) \chi_{\rho_2}(g_2)$  (Exercise). Generally, we will write  $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \chi_{\rho_2}$ . Let  $\rho_i, \rho'_i$  be representations of  $G_i$  for  $i = 1, 2$ . Then

$$\langle \chi_{\rho_1 \otimes \rho_2}, \chi_{\rho'_1 \otimes \rho'_2} \rangle = \langle \chi_{\rho_1}, \chi_{\rho'_1} \rangle_{G_1} \langle \chi_{\rho_2}, \chi_{\rho'_2} \rangle_{G_2}$$

(Exercise).

**Conclusion.**  $\rho_1 \otimes \rho_2$  is irreducible if and only if  $\rho_1, \rho_2$  are irreducible. Moreover, if  $\{\chi_1, \dots, \chi_s\}$  is the set of irreducible characters of  $G_1$  and  $\{\phi_1, \dots, \phi_t\}$  is the set of irreducible characters for  $G_2$ , then  $\{\chi_i \phi_j\}$  is the set of irreducible characters of  $G_1 \times G_2$  (Use the fact that  $\sum n_i^2 = |G|$  to show that this must be all of them).

Another Version of...

**Lemma 4.37 (Schur's Lemma).** Let  $|G|$  be a finite group, char  $k \nmid |G|$ ,  $k = \bar{k}$ . Let  $\rho : G \rightarrow GL_k(V)$  be an irreducible representation of  $G$  and  $\chi$  its associated character. Then for all  $g \in Z(G)$ , we have

1.  $\rho(g) = \lambda I$  for some  $\lambda \in k^*$ .
2.  $|\chi(g)| = \chi(1)$  if  $k = \mathbb{C}$ .

*Proof.* Write  $k[G] = B_1 \times \dots \times B_t$  where  $B_i$  are simple, Artinian, and  $e_i \in B_i$  is the identity. Then  $Z(k[G]) = ke_1 \times \dots \times ke_t$ . If  $g \in Z(G)$ , then  $g \in Z(k[G])$ . Write  $\alpha_1 e_1 + \dots + \alpha_t e_t = g$ ,  $\alpha_i \in k$ . Now  $V$  is an irreducible  $k[G]$ -module. WLOG, say  $V$  is a simple  $B_1$ -module (if not, reindex the  $B_i$ 's). Then  $e_1 v = v$  for all  $v \in V$  and  $e_j v = 0$  for all  $j > 1$ . Then  $gv = \alpha_1 v$  for all  $v \in V$  and thus  $\rho(g) = \alpha_1 I_V$ .  $\square$

**Theorem 4.38.** Under the "standard notation" above,  $n_i \mid |G : Z(G)|$  for all  $i$ .

*Proof.* (Tate) Let  $n = n_1$ ,  $\chi = \chi_1$  with  $\rho : G \rightarrow GL_k(V)$ , a representation associated to  $\chi$ . Let  $m$  be a positive integer and consider  $\rho_m := \rho \otimes \dots \otimes \rho : \underbrace{G \times \dots \times G}_{:=G_m} \rightarrow GL_k(V \otimes \dots \otimes V)$ . As  $\rho$  is irreducible, so is  $\rho_m$ . Define a map  $\gamma : Z(G) \rightarrow k^*$  by

$g \mapsto \alpha$  where  $\rho(g) = \alpha I$ . It is easily seen that  $\gamma$  is a group homomorphism. Let  $D = \{(g_1, \dots, g_m) \in Z(G_m) \mid \lambda(g_1 \dots g_m) = 1\}$ . Let  $H = \ker \gamma$  and  $g_1, \dots, g_{m-1} \in Z(G)$ . Note  $(g_1, \dots, g_m) \in D$  if and only if  $g_1, \dots, g_m \in H$  which is if and only if  $g_m \in g_1^{-1} \dots g_{m-1}^{-1} H$ . Thus  $|D| = |Z(G)|^{m-1} |H|$  (as there are  $|Z(G)|^{m-1}$  choices for  $g_1, \dots, g_{m-1}$  and  $|H|$  choices for  $g_m$ ). Now  $D \triangleleft G_m$  as  $D \subseteq Z(G_m)$  and  $D \subseteq \ker \rho_m$  (To see this, let  $(g_1, \dots, g_m) \in D$ . Then  $\rho(g_1, \dots, g_m) = \rho(g_1) \otimes \dots \otimes \rho(g_m) = \alpha_{g_1} I_V \otimes \dots \otimes \alpha_{g_m} I_V = (\alpha_{g_1} \dots \alpha_{g_m}) I_{V \otimes \dots \otimes V} = \gamma(g_1) \dots \gamma(g_m) I_{V \otimes \dots \otimes V} = \gamma(g_1 \dots g_m) I_{V \otimes \dots \otimes V} = I_{V \otimes \dots \otimes V}$ ). Thus  $\bar{\rho}_m : G_m/D \rightarrow GL_k(V \otimes \dots \otimes V)$  defined by  $(\bar{g}_1, \dots, \bar{g}_m) \mapsto \rho(g_1) \otimes \dots \otimes \rho(g_m)$  is a well defined irreducible representation of  $G_m/D$ . By the previous theorem,  $\deg \bar{\rho}_m \mid |G_m/D|$  which implies  $n^m \mid |G|^m / (|Z(G)|^{m-1} \cdot |H|)$ . So  $\frac{|G|^m}{n^m |Z(G)|^{m-1} |H|} \in \mathbb{Z}$ .

Then  $\underbrace{\frac{|Z(G)|}{|H|}}_{\in \mathbb{Z}} \underbrace{\left(\frac{|G|}{n|Z(G)|}\right)^m}_{\in \mathbb{Q}} \in \mathbb{Z}$  for all  $m$ . By HW7#5, we see  $\frac{|G|}{n|Z(G)|}$  is integral over  $\mathbb{Z}$  which says  $n \mid [G : Z(G)]$  as  $\mathbb{Z}$  is integrally closed in  $\mathbb{Q}$ .  $\square$

**Lemma 4.39.** *Let  $G$  be a finite group,  $\rho : G \rightarrow GL_n(\mathbb{C})$  an irreducible representation, and  $\chi$  its associated character. Let  $C$  be a conjugacy class of  $G$  such that  $\gcd(|C|, n) = 1$ . Then for all  $g \in C$ , either  $\chi(g) = 0$  or  $|\chi(g)| = 1$ .*

*Proof.* Let  $m = |C|$ . Then there exists  $r, s \in \mathbb{Z}$  such that  $rm + sn = 1$ . Then for all  $g \in C$ , we have  $\frac{rm\chi(g)}{n} + s\chi(g) = \frac{\chi(g)}{n}$ . Let  $A$  be the integral closure of  $\mathbb{Z}$  in  $\mathbb{C}$ . We've seen  $\chi(g) \in A$  for all  $g \in G$ . By a previous proposition, we have also shown  $\frac{m\chi(g)}{n} \in A$  for  $g \in C$ . Thus  $\frac{\chi(g)}{n} \in A$  for all  $g \in C$ . Let  $\chi(g) = \lambda_1 + \dots + \lambda_n$  where  $\lambda_i$  are  $k^{th}$  roots of unity. Let  $\omega$  be a primitive  $k^{th}$  root of unity and  $L = \mathbb{Q}(\omega)$ . Then  $\lambda_i \in L$  for all  $i$ . Let  $H = Gal(L/\mathbb{Q})$  and  $\sigma \in H$ . Note  $\sigma(A \cap L) \subseteq A \cap L$ . Also,  $\sigma(\lambda_i) = \lambda_j$ . Let  $\alpha = \frac{\chi(g)}{n} = \frac{\lambda_1 + \dots + \lambda_n}{n}$ . Then  $|\alpha| \leq 1$ . Note  $|\sigma(\alpha)| = \frac{|\sigma(\lambda_1) + \dots + \sigma(\lambda_n)|}{n} \leq 1$  for all  $\sigma \in H$  and  $\sigma(\alpha) \in A$ . Consider  $N = N_{\mathbb{Q}}^L : L \rightarrow \mathbb{Q}$  where  $N(\beta) = \prod \sigma(\beta) \in \mathbb{Q}$ . So  $N(\alpha) = \prod_{\sigma \in H} \sigma(\alpha) \in \mathbb{Q} \cap A = \mathbb{Z}$ . So  $|N(\alpha)| = \prod |\sigma(\alpha)| \leq 1$ . Thus  $N(\alpha) = 0$  or  $1$ . Now  $N(\alpha) = 0$  implies  $\frac{\chi(g)}{n} = \alpha = 0$ . Thus  $\chi(g) = 0$ . If  $N(\alpha) = 1$ , then  $|\alpha| = 1$  which says  $\lambda_1 = \dots = \lambda_n$  so that  $\chi(g) = \lambda n$  and  $|\chi(g)| = n = \chi(1)$ .  $\square$

**Theorem 4.40.** *Let  $G$  be a finite simple group,  $C$  a conjugacy class of  $G$ . Then  $|C| \neq p^a$  for  $p$  prime and  $a > 0$ .*

*Proof.* Assume  $G$  is not abelian (as otherwise  $|C| = 1$ ). Suppose there exists  $C$  such that  $|C| = p^a$  for  $a > 0$ . Let  $\chi_1, \dots, \chi_t$  be the irreducible  $\mathbb{C}$ -characters of  $G$  and  $\rho_i : G \rightarrow GL_{n_i}(\mathbb{C})$  the irreducible representations associated with  $\chi_i$ . Let  $\rho_1$  be the trivial representation.

Claim 1: If  $p \nmid n_i$  for  $i > 1$ , then  $\chi_i(g) = 0$  for all  $g \in C$ .

*Proof:* Let  $G_i = \{g \in G \mid \rho_i(g) = \lambda I, \text{ some } \lambda \in \mathbb{C}\}$ . It is easy to see  $G_i \triangleleft G$ . But  $G$  is simple, so  $G_i = \{1\}$  or  $G_i = G$ . Suppose  $G_i = G$ . Note  $\ker \rho_i \triangleleft G$  and  $\rho_i \neq 1$ . Thus  $\ker \rho_i = \{1\}$ . So  $G \cong \rho_i(G) = \{\lambda_g I \mid g \in G\}$  as  $G_i = G$ , but this is abelian, a contradiction. Thus  $G_i = \{1\}$  and  $\rho_i(g) \neq \lambda I$  for all  $\lambda \in \mathbb{C}$  and  $g \neq 1$ . Thus  $|\chi_i(g)| < \chi_i(1)$  by HW7. By the lemma,  $\chi_i(g) = 0$  for all  $g \in C$ .

Claim 2:  $p \mid n_i$  for some  $i > 1$ .

*Proof:* By an orthogonality relation, for  $g \in C$ , we have  $\sum_{i=1}^t \chi_i(1)\chi_i(g) = 0$ . So  $0 = 1 + \sum_{i=2}^t \chi_i(1)\chi_i(g)$ . Since  $0 \neq 1$ , there exists  $j \geq 2$  such that  $\chi_j(g) \neq 0$ . Thus  $p \mid n_j$ .

Reorder the characters such that  $p \mid n_i$  for  $i = 2, \dots, s$  and  $p \nmid n_i$  for  $i = s+1, \dots, t$ . Thus by Claim 1,  $1 + \sum_{j=2}^s \chi_j(1)\chi_j(g) = 0$ . Since  $p \mid n_j$ , we have  $\frac{1}{p} = -\sum_{j=2}^s \left(\frac{n_j}{p}\right) \chi_j(g) \in A \cap \mathbb{Q} = \mathbb{Z}$ , a contradiction.  $\square$

**Corollary 4.41** (Burnside). *Let  $G$  be a group of order  $p^a q^b$ . Then  $G$  is solvable.*

*Proof.* We will show that  $G$  is not simple. We've seen the case where  $b = 0$ . So assume  $a, b \geq 1$ . Let  $P$  be a Sylow- $p$  subgroup. Let  $z \in Z(P) \setminus \{1\}$ . Then  $C_G(z) \supseteq P$  which implies  $[G : C_G(z)] = q^c$ , for some  $c$ . Of course,  $[G : C_G(z)] = |C|$ , where  $C$  is the conjugacy class of  $z$ . By the theorem, if  $G$  is simple, then  $c = 0$  which implies  $z \in Z(G) \setminus \{1\}$  and so  $G$  has a nontrivial subgroup. So  $G$  is not simple. Let  $H \triangleleft G$ . By induction,  $H$  and  $G/H$  are solvable, which implies  $G$  is solvable.  $\square$

## 4.4 Injective Modules

**Definition 4.42.** *An  $R$ -module  $E$  is injective if given*

$$\begin{array}{ccc}
 & E & \\
 & \uparrow & \swarrow \text{---} \\
 0 & \longrightarrow M & \longrightarrow N
 \end{array}
 \quad \text{exact}$$

there exists a map  $N \rightarrow M$  such that the diagram commutes.

**Theorem 4.43 (Baer's Criterion).** *Let  $E$  be a left  $R$ -module. Then  $E$  is injective if and only if given a diagram*

$$\begin{array}{ccc} & E & \\ & \uparrow & \nearrow \exists h \\ 0 & \longrightarrow I & \longrightarrow R \end{array} \quad \text{exact}$$

where  $I$  is a left ideal, there exists  $h : R \rightarrow E$  making the diagram commute.

*Proof.* The forward direction is clear from the definition. So suppose we are given a diagram

$$\begin{array}{ccc} & E & \\ & \uparrow f & \\ 0 & \longrightarrow M & \xrightarrow{i} N \end{array} \quad \text{exact}$$

where WLOG we may assume  $M \subset N$  and so  $i$  is just the inclusion map. Let  $\Lambda = \{(K, f_K) \mid M \subseteq K \subseteq N, K \text{ a left } R\text{-module}, f_K : K \rightarrow E, f_K|_M = f\}$ . Partially order in the obvious way. Then  $\Lambda \neq \emptyset$  and  $(M, f) \in \Lambda$ . By Zorn's Lemma, there exists  $(K, f_K)$  maximal in  $\Lambda$ .

Claim:  $K = N$ .

*Proof:* Suppose not. Choose  $x \in N \setminus K$ . Let  $I = (K :_R x) = \{r \in R \mid rx \in K\}$ . Then  $I$  is a left ideal of  $R$ . Define  $\phi : I \rightarrow E$  such that  $i \mapsto f_K(ix)$ . This is  $R$ -linear. By hypothesis, there exists  $\tilde{\phi} : R \rightarrow E$  such that  $\tilde{\phi}|_I = \phi$ . Define  $g : K + Rx \rightarrow E$  by  $k + rx \mapsto f_K(k) + \tilde{\phi}(r)$ . To show  $g$  is well-defined, suppose  $k + rx = 0$ . Then  $r \in I$ . So  $\tilde{\phi}(r) = \phi(r) = f_K(rx)$ . Then  $g(k + rx) = f_K(k) + f_K(rx) = f_K(k + rx) = f_K(0) = 0$ . Thus  $(K + Rx, g) \in \Lambda$ , a contradiction to the maximality of  $(K, f_K)$ . □

**Definition 4.44.** *Let  $R$  be commutative,  $M$  an  $R$ -module. Say  $M$  is **divisible** if for all  $m \in M$  and for all non-zero-divisors  $r \in R$ , there exists  $m' \in M$  such that  $rm' = m$ .*

**Examples.**

1. Every vector space over a field is divisible.
2. If  $R$  is a domain, then  $Q$ , the field of fractions of  $R$ , is divisible.
3. Sums, products, quotients of divisible modules are divisible.
4. Submodules of divisible modules are *not* always divisible. For example,  $\mathbb{Q}$  is a divisible  $\mathbb{Z}$ -module, but  $\mathbb{Z}$  is not.
5. In particular,  $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}$  are divisible  $\mathbb{Z}$ -modules.

**Proposition 4.45.** *Let  $R$  be commutative. Every injective module is divisible. If  $R$  is a PID, then the converse holds.*

*Proof.* Let  $E$  be injective,  $e \in E$ , and  $r \in R$  a non-zero-divisor. Consider the diagram

$$\begin{array}{ccc} & E & \\ & \uparrow f & \nearrow \\ 0 & \longrightarrow R & \xrightarrow{r} R \end{array} \quad \text{exact}$$



where  $r : R \rightarrow R$  is multiplication by  $r$  and  $f(1) = e$ . As  $E$  is injective, we have a map from  $R \rightarrow E$ , say its defined by  $1 \mapsto e'$ . Then, by commutivity,  $re' = e$ . Now, suppose  $R$  is a PID and  $E$  is a divisible module. Let  $I = (a)$  be an ideal of  $R$  and consider the diagram

$$\begin{array}{ccc}
 & E & \\
 & \uparrow f & \swarrow \\
 0 & \longrightarrow (a) & \xrightarrow{r} R
 \end{array}
 \quad \text{exact}$$

If  $a = 0$ , done. Otherwise, let  $e = f(a)$ . As  $a$  is a non-zero-divisor ( $R$  is a domain), there exists  $e'$  such that  $ae' = e$ . Define  $\tilde{f} : R \rightarrow E$  by  $1 \mapsto e'$ . Then  $\tilde{f}(ra) = r\tilde{f}(a) = rae' = re = rf(a) = f(ra)$ . So  $\tilde{f}|_{(a)} = f$ . By Baer's Criterion,  $E$  is injective.  $\square$

**Corollary 4.46.** Any  $\mathbb{Z}$ -module  $M$  can be embedded into an injective  $\mathbb{Z}$ -module.

*Proof.* Consider  $0 \rightarrow K \rightarrow \bigoplus_{\alpha \in I} \mathbb{Z} \rightarrow M \rightarrow 0$ , which is exact (let  $|I|$  be the number of generators of  $M$  as a  $\mathbb{Z}$ -module). So  $M \cong \bigoplus \mathbb{Z}/K \subseteq \bigoplus \mathbb{Q}/K$ . By the above,  $\bigoplus \mathbb{Q}/K$  is a divisible  $\mathbb{Z}$ -module and so it is injective. Thus  $M$  embeds into an injective module.  $\square$

**Proposition 4.47.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Let  $E$  be an injective left  $R$ -module. Then  $\text{Hom}_R(S, E)$  is an injective left  $S$ -module.

*Proof.* Recall  $\text{Hom}_R(S, E)$  is a left  $S$ -module via  $(sf) : S \rightarrow E$  where  $s' \mapsto f(s's)$  for  $s \in S, f \in \text{Hom}_R(S, E)$ . Note  $sf$  is  $R$ -linear. So it is enough to show that if  $0 \rightarrow M \rightarrow N$  is an exact sequence of  $S$ -modules,  $\text{Hom}_S(N, \text{Hom}_R(S, E)) \rightarrow \text{Hom}_S(M, \text{Hom}_R(S, E))$  is surjective. By Hom- $\otimes$  adjointness and the fact that  $S \otimes_S M = M$ , we have the following diagram

$$\begin{array}{ccc}
 \text{Hom}_S(N, \text{Hom}_R(S, E)) & \xrightarrow{\sigma} & \text{Hom}_S(M, \text{Hom}_R(S, E)) \\
 \downarrow \cong & & \downarrow \cong \\
 \text{Hom}_R(S \otimes_S N, E) & \longrightarrow & \text{Hom}_R(S \otimes_S M, E) \\
 \downarrow \cong & & \downarrow \cong \\
 \text{Hom}_R(N, E) & \longrightarrow & \text{Hom}_R(M, E) \longrightarrow 0 \text{ exact}
 \end{array}$$

Note that both squares commute by the "naturality" of the isomorphisms. The bottom row is exact as  $E$  is an injective  $R$ -module. So, we have  $\sigma$  is surjective.  $\square$

**Theorem 4.48.** Let  $R$  be a ring,  $M$  a left  $R$ -module. Then there exists an injective  $R$ -module  $E$  and an injective  $R$ -module homomorphism  $M \rightarrow E$ .

*Proof.* Of course, there exists a ring homomorphism  $\phi : \mathbb{Z} \rightarrow R$ . As  $M$  is a  $\mathbb{Z}$ -module, there exists an injective  $\mathbb{Z}$ -module  $I$  with  $M \subseteq I$ . By the above proposition,  $\text{Hom}_{\mathbb{Z}}(R, I)$  is an injective left  $R$ -module. Define  $g : M \rightarrow \text{Hom}_{\mathbb{Z}}(R, I)$  by  $m \mapsto f_m$  where  $f_m : R \rightarrow I$  is defined by  $r \mapsto rm \in M \subseteq I$ . We need to show  $g$  is  $R$ -linear. It is enough to show  $rf_m = f_{rm}$ . For  $r' \in R$ , we have  $(rf_m)(r') = f_m(r'r) = r'rm = f_{rm}(r')$ . Also,  $g$  is injective as  $m = 0$  if and only if  $f_m = 0$ .  $\square$