Abstract Algebra I

A collection of notes on major definitions and results, proofs, and commentary based on the corresponding course at Illinois, as instructed by Rezk

Lecture Notes By

Dheeran E. Wiggins

Department of Mathematics
University of Illinois Urbana-Champaign

Disclaimer
The lecture notes in this document were based on Abstract Algebra I [500], as instructed by Charles Rezk [Department of Mathematics] in the Fall semester of 2024 [FA24] at the University of Illinois Urbana-Champaign. All non-textbook approaches, exercises, and comments are adapted from Rezk's lectures.

Textbook
Many of the exercises and presentations were selected from *Abstract Algebra, Third Edition*, by David S. Dummit and Richard M. Foote.

Author Information
Dheeran E. Wiggins is, at the time of writing [Fall, 2024], a second-year student at Illinois studying mathematics. All typesetting and verbiage are his own.

dheeran2@illinois.edu

This is a universal property. Whatever that means.

– Charles Rezk

Contents

On the Theory of Groups

Developing Structure | 1

We review some of the basic facts and notations of group theory. Most results are given without proof, but are worthwhile exercises if you do not remember their demonstrations. Some results are presented with a bit more (categorical) abstraction.

1.1 Review and Notations

We usually write a group in the form $(G, \cdot)$, where G is the *underlying* set and $\cdot : G \times G \to G$ is a *binary operation*.[1] We take these such that[2]

(i) the binary operation is *associative*, so $(xy)z = x(yz)$.
(ii) there exists a unique $e \in G$ which is an *identity*: $ex = x = xe$ for all $x \in G$.
(iii) for all $x \in G$, there exists a unique *inverse* $x^{-1} \in G$ such that

$$xx^{-1} = e = x^{-1}x.$$

1: That is, it takes $(x, y) \mapsto x \cdot y = xy$.

2: If we just have (i) and (ii), then $(G, \cdot)$ is a *monoid*. If we just have (i), then $(G, \cdot)$ is a *semigroup*. If none hold, then $(G, \cdot)$ is a *magma*.

Remark 1.1.1 We generally prefer juxtaposition over explicit use of the operation, when context suffices. We also, by abuse of notation, will refer to the underlying set G as the group.

Definition 1.1.1 (Abelian Group) *If we have $xy = yx$ for all $x, y \in G$, then G is called abelian.*[3]

3: An *additive* group is an abelian group written with $+$ as the binary operation.

Definition 1.1.2 (Order) *The order of a group is $|G|$, the cardinality of the underlying set G.*

Example 1.1.1 There are a few quintessential groups which we will need to be familiar with.

(a) $C_n := \{e, a, a^2, \ldots, a^{n-1}\}$.[4]
(b) $\mathbb{Z}/n\mathbb{Z} := \{0, 1, 2, \ldots, n-1\}$.[5]
(c) D_{2n} is the symmetries of a regular n-gon in space.[6]
(d) $\mathrm{Sym}(\Omega) = S_\Omega$ is the symmetric group of a set Ω; i.e., the set of permutations/bijections $\sigma : \Omega \to \Omega$.
(e) S_n is the symmetric group on n letters: $\mathrm{Sym}([n])$.
(f) $\mathrm{GL}_n(\mathbb{F})$ is $n \times n$ invertible matrices with entries in a field $\mathbb{F}$.
(g) $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$.

4: This is the finite cyclic group of order n, written multaplicatively.

5: This is the set of congruence classes modulo n, which is isomorphic to C_n, but is written additively.

6: $|D_{2n}| = 2n$.

Definition 1.1.3 (Subgroup) *Given a group G, a subgroup is a subset $H \subseteq G$ such that*

(i) $H \neq \varnothing$.[7]
(ii) $x \in H$ implies $x^{-1} \in H$.

7: We can equivalently write $e \in H$.

(iii) $x, y \in H$ *implies* $xy \in H$.

In this case, we write $H \leq G$.

Given a group G with a subset $S \subseteq G$,[8]

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H \leq G$$

is the "smallest subgroup" of G which contains S.[9]

8: Proving that this is, in fact, a group, is not very difficult.

9: That is, if $H \leq G$ such that $S \subseteq H$, then $\langle S \rangle \leq H$. This is called the subgroup generated by S.

Proposition 1.1.1 *We can equivalently write*

$$\langle S \rangle = \left\{ a_1, \ldots, a_k : \begin{array}{c} \textit{for all } i \in [k], \\ \textit{either } a_i \in S \\ \textit{or } a_i^{-1} \in S, \\ \textit{with } k \geq 0 \end{array} \right\},$$

where $k = 0$ *implies* $e \in S$.[10]

10: The contents of $\langle S \rangle$ are precisely the *words* written in S.

Sketch of Proof. Let $K :=$ the RHS. We need to show that (1) $K \leq G$ such that $S \subseteq K$, and (2) if $H \leq G$ and $S \subseteq H$, then $K \subseteq H$. □

Remark 1.1.2 If we have a group G and $S = \varnothing$, then $\langle \varnothing \rangle = \{e\}$.

We often say G is "generated" by the subset S if $\langle S \rangle = G$.

Definition 1.1.4 (Cyclic Group) *A group G is called cyclic is when there exists*[11] $a \in G$ *such that* $G = \langle \{a\} \rangle = \langle a \rangle$.

11: This "generator" a is *not* unique.

Example 1.1.2 Consider C_8. Note that we can write

$$C_8 = \langle a \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle.$$

Definition 1.1.5 (Cosets) *Let $H \leq G$. Then, a left coset of H in G is a subset of the form*

$$xH = \{xh : h \in H\},$$

for some $x \in G$.[12]

12: A *right coset* is written Hx, defined similarly. Note that $xH = Hx$ when G is abelian.

The collection of all left cosets partitions G into pairwise disjoint sets.[13]

13: The same is true for right cosets.

Proposition 1.1.2 *Given* $x, y \in G$, *with* $H \leq G$, *the following are equivalent:*

(i) $xH = yH$.
(ii) $x \in yH$.
(iii) $y \in xH$.
(iv) $xy^{-1} \in H$.
(v) $yx^{-1} \in H$.

Example 1.1.3 Let xH and yH be cosets. Suppose $z \in xH \cap yH$. We want to show that $xH = yH$. Well, $z \in xH \cap yH$ means $z = xh_1 = yh_2$ for some $h_1, h_2 \in H$. Well, this means $x = yh_2h_1^{-1}$ and $y = xh_1h_2^{-1}$. Hence, $x \in yH$ and $y \in xH$. In general, if $xh \in xH$, then $xh = yh_2h_1^{-1} \in yH$, so $xH \subseteq yH$.[14]

14: The other direction is the same, since the demonstration is symmetric.

Definition 1.1.6 (Index) *The index of $H \leq G$ is the cardinality of the set of left cosets:*[15]

$$|G : H| := |G/H|.$$

15: We write G/H for the set of left H cosets in G.

Remark 1.1.3 There exists a bijection[16]

$$G/H \xleftrightarrow{\text{bijection}} H\backslash G,$$

taking the prescription

$$xH \longmapsto Hx^{-1}.$$

16: We write $H\backslash G$ for the set of right H cosets in G.

Theorem 1.1.3 (Lagrange's Theorem) *There exists a bijection of sets*[17]

$$G \xleftrightarrow{\textit{bijection}} H \times G/H,$$

where we have the identity[18]

$$|G| = |H| \cdot |G : H|.$$

We pick for each coset a representative element.[19]

17: Take $H \leq G$.

18: This is the $H \times G/H \to G$ direction. From here, it is probably best to just show injectivity and surjectivity.

19: Note that this works for infinite sets.

Definition 1.1.7 (Group Homomorphism) *A group homomorphism is a function $\varphi : G \to H$ between groups which "preserves structure." That is,*

$$\varphi(xy) = \varphi(x)\varphi(y),$$

for all $x, y \in G$.

This definition, as you should know, implies $\varphi(e_G) = e_H$. Additionally, the same is true for inverses: $\varphi(x^{-1}) = \varphi(x)^{-1}$.[20]

20: Interestingly, for a monoid homomorphism $\varphi : M \to N$, we define

$$\varphi(xy) = \varphi(x)\varphi(y)$$

and $\varphi(e_M) = e_N$. That is, we actually need to ensure the identity preservation holds, because it is not implied by the operation preservation.

1.2 Groups Form a Category Grp

We can get some neat results about groups by now thinking from a categorical perspective.

Definition 1.2.1 (Category) *A category $\mathscr{C}$ consists of*[21]

(i) *a class* $\operatorname{ob}\mathscr{C}$ *of "objects."*
(ii) *a class* $\operatorname{Hom}(X, Y)$ *of "morphisms" for each pair* $X, Y \in \operatorname{ob}\mathscr{C}$.
(iii) *a "composition" operation given* $f \in \operatorname{Hom}(X, Y)$ *and* $g \in \operatorname{Hom}(Y, Z)$

21: Assume NBG instead of ZFC.

such that $g \circ f \in \mathrm{Hom}(X, Z)$.

(iv) identity morphisms $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ *such that*

(a) *given morphisms* f, g, h, *we have*

$$(h \circ g) \circ f = h \circ (g \circ f),$$

if these are all defined.

(b) $f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f$, *for all* $f \in \mathrm{Hom}(X, Y)$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[loop above, "\mathrm{id}_X"] \arrow[dr, "g\circ f"'] & Y \arrow[d, "g"] \arrow[loop above, "\mathrm{id}_Y"] \\ & Z \arrow[loop below, "\mathrm{id}_Z"] \end{tikzcd}$$

Figure 1.1: The identity and composition morphisms acting between $X, Y, Z \in \mathrm{ob}\,\mathscr{C}$.

Example 1.2.1 There are a few examples of *concrete* categories which we are already familiar with.

(a) The category Set has objects which are sets $S, T, \ldots$ and

$$\mathrm{Hom}(S, T) = \{\text{all functions } f : S \to T\}.$$

(b) The category Grp has objects which are groups and morphisms which are homomorphisms.
(c) The category Top has objects which are topological spaces and morphisms which are continuous maps.
(d) The category $\mathsf{Vect}_{\Bbbk}$ has objects which are $\Bbbk$-linear spaces and morphisms which are linear maps.

Definition 1.2.2 (Isomorphism) *An isomorphism is a morphism* $f : X \to Y$ *in* $\mathscr{C}$ *such that there exists a morphism* $g : Y \to X$ *such that* $g \circ f = \mathrm{id}_X$ *and* $f \circ g = \mathrm{id}_Y$.

Definition 1.2.3 (Inverse) *We call* g, *as above, the inverse of* f *and write* $f^{-1} := g$.

Proposition 1.2.1 *In a category, if an inverse exists, it is unique.*

Proof. Let $f \in \mathrm{Hom}(X, Y)$ and $g, g' \in \mathrm{Hom}(Y, X)$ such that $gf = \mathrm{id}_X = g'f$ and $fg = \mathrm{id}_Y = fg'$. Then,[22]

$$\begin{aligned} g'(fg) &= (g'f)g \\ g'\,\mathrm{id}_Y &= \mathrm{id}_X\, g, \end{aligned}$$

so $g' = g$. □

22: This is essentially the same method of proof that we would use if we were simply considering groups.

Example 1.2.2 Let M be a monoid. Then, we can define a category $\mathscr{C}$ with $\mathrm{ob}\,\mathscr{C} := \{X\}$ and $\mathrm{Hom}(X, X) := M$, where composition in $\mathscr{C}$ directly corresponds to multiplication in M.

Remark 1.2.1 In general, if $\mathscr{C}$ is a category and $X \in \mathrm{ob}\,\mathscr{C}$, then the set $\mathrm{Hom}(X, X)$ has the structure of a monoid. This is called the *endomorphism monoid* $\mathrm{End}(X)$.

Remark 1.2.2 The set $\mathrm{Iso}(X, X) \subseteq \mathrm{Hom}(X, X)$ of isomorphisms in $\mathscr{C}$ has the structure of a group called $\mathrm{Aut}(X)$, which is the *automorphism group*.

Definition 1.2.4 (Groupoid) *A groupoid is a category $\mathscr{C}$ such that every morphism is an isomorphism.*[23]

23: As an observation, a groupoid with one object is a group, in the same way that a category with one object is a monoid. Inverses is what we needed!

If $\mathscr{C}$ is a category, it contains a groupoid $\mathscr{C}^{\mathrm{core}}$ where $\mathrm{ob}\,\mathscr{C}^{\mathrm{core}} = \mathrm{ob}\,\mathscr{C}$,

$$\text{and} \quad \mathrm{Hom}_{\mathscr{C}^{\mathrm{core}}}(X, Y) := \left\{ f \in \mathrm{Hom}_{\mathscr{C}}(X, Y) : \begin{array}{c} f \text{ is an isomorphism} \\ \text{in } \mathscr{C} \end{array} \right\}$$

Remark 1.2.3 (Arrow Notation) We will use the following convention, when we remember:

(i) *injection*: $X \rightarrowtail Y$
(ii) *surjection*: $X \twoheadrightarrow Y$
(iii) *inclusion*: $X \hookrightarrow Y$
(iv) *bijection/isomorphism* $X \xrightarrow{\sim} Y$ or $X \xrightarrow{\simeq} Y$

Now, Grp is a category, so let us take a look at isomorphisms of groups.

Proposition 1.2.2 *A homomorphism $f : G \to H$ of groups is an isomorphism if and only if it is a bijection.*

Definition 1.2.5 (Isomorphic Groups) *Given groups G, H, we say G and H are isomorphic, written $G \simeq H$, if there exists an isomorphism $\varphi : G \xrightarrow{\sim} H$.*[24]

24: Note that these isomorphisms are usually not unique.

S_3 and D_6 are isomorphic groups.[25] If we label each of the vertices of $\triangle$ by $1, 2, 3$, counterclockwise starting from the RHS, then each symmetry $\alpha \in D_6$ can correspond via φ to $\varphi(\alpha) \in S_3$. The rotation $r = 120°$ gets

25: Remember, S_3 is the permutations of $\{1, 2, 3\}$ and D_6 is the symmetries of $\triangle$.

$$r \overset{\varphi}{\longmapsto} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

and the reflection $s = 180°$ gets

$$s \overset{\varphi}{\longmapsto} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Proposition 1.2.3 *We claim φ is an isomorphism of groups.*[26]

26: Note that our labeling is arbitrary, so relabeling the vertices gives a different isomorphism. There are actually *six* isomorphisms between these groups, one for each labeling.

What about $\mathrm{Aut}(S_3)$? Well,

$$\mathrm{Aut}(G) = \left\{ \begin{array}{c} \text{set of isomorphisms} \\ \varphi : G \xrightarrow{\sim} G \end{array} \right\},$$

as a group under composition. Since S_3 is generated by its transpositions, the elements of $\mathrm{Aut}(S_3)$ sending transpositions to transpositions is equivalent to permuting the elements of S_3, so $\mathrm{Aut}(S_3) \simeq S_3$.[27]

27: There is some more leg work to be done here, but this is a good sketch of the proof.

1.3 Normality and Quotients

Definition 1.3.1 (Normal Subgroup) *A subgroup $H \leq G$ is normal if $xHx^{-1} = H$ for all $x \in G$. We write $H \trianglelefteq G$.* [28]

28: This is an equality of sets. The LHS is a shorthand for

$$xHx^{-1} = \{xhx^{-1} : h \in H\}.$$

This operation is called *conjugating* by x.

Example 1.3.1 In D_6, we have the elements $\{e, r, r^2, s, sr, sr^2\}$. Now, $\langle r \rangle \leq D_6$, which is $\{e, r, r^2\}$, and $\langle s \rangle \leq D_6$, which is $\{e, s\}$. Only $\langle r \rangle \trianglelefteq D_6$. Remember there is a relation $sr = r^{-1}s$, so $sr^{-1} = rs$. To show $\langle s \rangle \ntrianglelefteq H$, note that

$$rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr,$$

so

$$rHr^{-1} = \{e, sr\} \neq H.$$

Proposition 1.3.1 *A subgroup $N \leq G$ is normal if and only if $Nx = xN$ for all $x \in G$.*

Remark 1.3.1 That is, a subgroup is normal if and only if all left cosets are right cosets. This characterization of normality can be great for intuiting whether or not a subgroup is normal.

Definition 1.3.2 (Kernel) *If $\varphi : G \to H$ is a homomorphism, the kernel*

$$\ker(\varphi) := \{g \in G : \varphi(g) = e\}$$

is a normal subgroup of G.

Proof. This is a straightforward verification. □

Definition 1.3.3 (Quotient Group) *If $N \trianglelefteq G$, we can form the quotient group G/N, where*[29]

$$G/N := \{xN : x \in G\} = \text{set of all left cosets}.$$

29: The multiplication is defined by

$$xN \cdot yN := (xy)N.$$

We have to check that this is well-defined, but we will not. Notably, we need N to be *normal* in order for the operation to be well-defined.

If we write the operation in terms of set multiplication, we find

$$xNyN = x(yN)N = xyN,$$

as desired.

Definition 1.3.4 (Quotient Homomorphism) *There exists a surjective homomorphism $\pi : G \twoheadrightarrow G/N$, defined by $\varphi(x) := xN$.*[30]

30: Note that $\ker(\pi) = N$, so normal is *exactly* the right condition to form a quotient group.

Example 1.3.2 For instance, consider $(\mathbb{Z}, +)$. Given $n \geq 1$, the group $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Their quotient $\mathbb{Z}/n\mathbb{Z}$ is precisely the integers modulo n, as we hoped.[31] The elements of the quotient group are written

$$x + n\mathbb{Z} = \{x + ny : y \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

31: Sometimes, we will also write $\mathbb{Z}/n$, though I am not a fan of this notation.

1.4 Isomorphism Theorems

The isomorphism theorems are quite well-known, but we state the "homomorphism theorem" first, which is the building block of the others. In turn, the isomorphism theorems, while convoluted at first glance, are one of the many "universal" threads which appear in standard algebraic objects. We will return to variants of these theorems two more times.

Theorem 1.4.1 (Homomorphism Theorem) *Given $N \trianglelefteq G$ and $\pi : G \twoheadrightarrow G/N$, the quotient homomorphism, if $\varphi : G \to H$ is a homomorphism such that $\varphi(N) = \{e\}$, then there exists a unique homomorphism $\psi : G/N \to H$ such that $\psi \circ \pi = \varphi$.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\exists!", "\psi"'] & \end{tikzcd}$$

Figure 1.2: This diagram commutes if $\varphi(N) = \{e\}$, or equivalently, $N \subseteq \ker(\varphi)$.

Corollary 1.4.2 *Given $N \trianglelefteq G$, with $\pi : G \to G/M$, then*

$$\mathrm{Hom}(G/N, H) \longrightarrow \mathrm{Hom}(G, H)$$

via

$$\psi \longmapsto \psi \circ \pi$$

is injective, with image subset

$$\{\psi \in \mathrm{Hom}(G, H) : \psi(N) = \{e\}\}$$

Theorem 1.4.3 (First Isomorphism Theorem) *Given a homomorphism $\varphi : G \to H$, we have an isomorphism $G/\ker(\varphi) \simeq \varphi(G) \leq H$. That is, φ factors through an isomorphism.*[32]

32: The corresponding diagram has

$$\overline{\varphi}(xN) = \varphi(x) \in \varphi(G) \leq H,$$

where $N = \ker(\varphi)$.

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi", "\text{quotient}"'] & & H \\ & G/\ker(\varphi) \xrightarrow[\sim]{\overline{\varphi}} \varphi(H) \arrow[ur, hook, "\iota"', "\text{inclusion}"] & \end{tikzcd}$$

Figure 1.3: Commutative diagram of the first isomorphism theorem

Let us do some setup for the second theorem. Well, given $A, B \leq G$ as subgroups, we have the *product subset*[33]

$$AB := \{ab \in G : a \in A, b \in B\} \subseteq G.$$

33: We may hope that this is a subgroup, but it is not always.

Example 1.4.1 Let $G = D_6 = \{e, r, r^2, s, sr, sr^2\}$. Recall that $r^3 = e = s^2$ and $rs = sr^{-1}$. We have the subgroups $A := \langle s \rangle = \{e, s\}$ and $B := \langle sr \rangle = \{e, sr\}$. The product subset is then

$$AB = \{e, s, sr, r\} \not\leq D_6,$$

as $4 \nmid 6$.

Proposition 1.4.4 *Given any two subgroups $A, B \leq G$, then $AB \subseteq G$ is a subgroup if and only if $BA \subseteq AB$.*[34] *If this is the case, then $AB = BA$.*

34: This is not in most textbooks, and is surprisingly hard to find *anywhere*.

Proof. We begin with the forward direction. Suppose $AB \leq G$. Then, for $a \in A$ and $b \in B$, we have $a = ae, b = eb \in AB$. Hence, $ba \in AB$.[35] Thus, $BA \subseteq AB$. To show $AB \subseteq BA$, suppose $x \in AB$. We also have $x^{-1} \in AB$, so we can write $x^{-1} = ab$, for some $a \in A$ and $b \in B$. However, $(x^{-1})^{-1} = (ab)^{-1} = b^{-1}a^{-1} \in BA$. Thus, $AB \subseteq BA$, so $AB = BA$. Now, for the other, more interesting direction, suppose $BA \subseteq AB$. If $a \in A$ and $b \in B$, then $(ab)^{-1} = b^{-1}a^{-1} \in BA \subseteq AB$, so AB is closed under inverses. It is also certainly not empty with $e \in AB$. Suppose we have $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then, $BA \subseteq AB$ implies $b_1 a_2 = a_2' b_1'$ for some $a_2' \in A$ and $b_2' \in B$:

$$(a_1 b_1)(a_2 b_2) = a_1 b_1 a_2 b_2 = (a_1 a_2')(b_1' b_2) \in AB,$$

so it is closed under multiplication.[36] ☐

35: AB is closed under the operation.

36: There you go. Under specific conditions, AB is a subgroup.

Example 1.4.2 If $A, B \leq G$ and $B \trianglelefteq G$, then $BA \subseteq AB$ and so $AB \leq G$.[37]

37: This is pretty trivial, becasue if $a \in A$, then $aB = Ba$, since B is normal.

Definition 1.4.1 (Normalizer) *Given a subset $S \subseteq G$, the normalizer of S is*

$$\mathcal{N}_G(S) := \{x \in G : xSx^{-1} = S\},$$

where

$$xSx^{-1} = \{xsx^{-1} : s \in S\}.$$

Clearly, we have $\mathcal{N}_G(S) \leq G$.

Proposition 1.4.5 *If $H \leq G$, then $H \trianglelefteq \mathcal{N}_G(H)$.*[38]

38: This is a *very* easy exercise.

Remark 1.4.1 Note that $\mathcal{N}_G(H)$ is the *largest* subgroup of G which has H as a normal subgroup.[39]

39: Notably, $H \trianglelefteq G$ if $\mathcal{N}_G(H) = G$.

Corollary 1.4.6 *If we have $A, B \leq G$ and $A \leq \mathcal{N}_G(B)$, then $AB = BA$ is a subgroup of G.*

$$\begin{tikzcd}
& G & \\
& \mathcal{N}_G(B) \arrow[u, hook] & \\
& AB \arrow[u, hook] & \\
A \arrow[ur, hook] & & B \arrow[ul, hook, "\trianglelefteq"'] \\
& A \cap B \arrow[ul, hook, "\trianglelefteq"] \arrow[ur, hook] &
\end{tikzcd}$$

Figure 1.4: We have $\varphi(a(A \cap B)) = aB$.

Theorem 1.4.7 (Second/Diamond Isomorphism Theorem) *Let $A, B \leq G$ with $A \leq \mathcal{N}_G(B)$. Then,*

(i) $AB \leq G$.
(ii) $B \trianglelefteq AB$.
(iii) $A \cap B \trianglelefteq A$.
(iv) $A/(A \cap B) \simeq AB/B$.

(i) *Proof.* This is immediate from the corollary. ☐
(ii) *Proof.* We have that $A \leq \mathcal{N}_G(B)$ implies $B \trianglelefteq AB$. ☐
(iii) *Proof.* If $a \in A$ and $x \in A \cap B$, then $axa^{-1} \in A$, as A is a subgroup, and $axa^{-1} \in B$, as $a \in \mathcal{N}_G(B)$. ☐

(iv) *Proof.* We can define the isomorphism

$$\begin{aligned} A/(A \cap B) &\xrightarrow{\quad \psi \quad} AB/B \\ x(A \cap B) &\longmapsto xB. \end{aligned}$$

Apply the homomorphism theorem to the diagram of ψ, as $x \in A \cap B$ implies $x \in B$, so $xB = eB$.

$$\begin{tikzcd} A \arrow[r, tail, "x \mapsto x"] \arrow[d, "\pi"'] & AB \arrow[r, two heads, "x \mapsto xB"] & AB/B \\ A/(A \cap B) \arrow[urr, dashed, "\psi", "x(A \cap B) \mapsto xB"'] & & \end{tikzcd}$$

Figure 1.5: Diagram of the isomorphism $\psi : A/(A \cap B) \to AB/B$.

Now, we have

- ψ is *injective*: $\psi(x(A \cap B)) = eB$ implies $xB = eB$.[40]
- ψ is *surjective*: given an element $abB \in AB/B$, where $a \in A$ and $b \in B$, we have $abB = aB$, so $\psi(a) = a$.

□

40: That is, $x \in B$ when $x \in A \cap B$, so

$$x(A \cap B) = e(A \cap B).$$

1.5 Free Group

A free group is a construction $F(S)$, dependent on a given set S. We begin with a definition, and then we will construct it.

Definition 1.5.1 (Free Group) *A free group is a pair (F, ι) where F is a group and $\iota : S \to F$ is a function*[41] *such that, for every group G and function $\varphi : S \to G$, there exists a unique homomorphism $\Phi : F \to G$ so that $\Phi \circ \iota = \varphi$.*

41: The set S is a "set of generators."

$$\begin{tikzcd} S \arrow[r, "\varphi", "\text{function}"'] \arrow[d, hook, "\iota"'] & G \\ F \arrow[ur, dashed, "\Phi", "\exists!\ \text{hom.}"'] & \end{tikzcd}$$

Figure 1.6: Diagram characterizing the free group of S

Example 1.5.1 Consider $S := \{a\}$. Let F be $C_\infty := \{a^n : n \in \mathbb{Z}\}$ and $\iota : S \to F$ prescribed by $\iota(a) = a^1$. Then, (F, ι) is a free group.

Proof. Given a function $\varphi : S \to G$ prescribed by $\varphi(a) = g$, there exists a unique homomorphism $\Phi : F \to G$ defined by $\Phi(a^n) = g^n$. □

Remark 1.5.1 Note that if (F, ι) is a free group, then we get a bijection

$$\mathrm{Hom}_{\mathsf{Grp}}(F, G) \xrightarrow{\quad \sim \quad} \mathrm{Hom}_{\mathsf{Set}}(S, G),$$

where $\Phi \mapsto \Phi \circ \iota$.

Proposition 1.5.1 *If $(F, \iota : S \to F)$ and $(F', \iota' : S \to F')$ are free groups, then $F \simeq F'$. We claim we can even build the isomorphism.*[42]

42: The construction makes the statement a bit more precise. The general idea, though, is there is only one free group for a set S.

Proof. Via the universal property, we may construct homomorphisms in the correct directions. There exists a unique group homomorphism $\varphi : F \to F'$ such that the following diagram commutes:

$$\begin{tikzcd} & F \arrow[dd, dashed, "\varphi"] \\ S \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & \\ & F' \end{tikzcd}$$

That is, $\varphi \circ \iota = \iota'$. Similarly, we may construct a unique homomorphism $\psi : F' \to F$ such that the following diagram commutes:

$$\begin{tikzcd} & F' \arrow[dd, dashed, "\psi"] \\ S \arrow[ur, "\iota'"] \arrow[dr, "\iota"'] & \\ & F \end{tikzcd}$$

That is, $\psi \circ \iota' = \iota$. Now, we may compose these two homomorphisms into maps $\psi \circ \varphi : F \to F$ and $\varphi \circ \psi : F' \to F'$. By our construction, we may glean the relations

$$\psi \circ \varphi \circ \iota = \psi \circ \iota' = \iota$$

and

$$\varphi \circ \psi \circ \iota' = \varphi \circ \iota = \iota'.$$

Yet, we know id_F and $\mathrm{id}_{F'}$, the identity morphisms in Grp, also satisfy

$$(\mathrm{id}_F : F \xrightarrow{\sim} F) \circ \iota = \mathrm{id}_F$$

and

$$(\mathrm{id}_{F'} : F' \xrightarrow{\sim} F') \circ \iota' = \mathrm{id}_{F'}.$$

Thus, via the uniqueness of our universal property for free groups, we must have that $\psi \circ \varphi = \mathrm{id}_F$ and $\varphi \circ \psi = \mathrm{id}_{F'}$. Therefore, φ, ψ are inverse isomorphisms yielding $F \simeq F'$, as desired. □

Example 1.5.2 There is one easier example of a free group than we did before: $S = \varnothing$ implies $F \simeq \{e\}$.

Theorem 1.5.2 *For every set S, there exists a free group $(F, \iota : S \to F)$.*

Proof. We begin by developing some terminology:

- We call elements $s \in S$ "symbols."
- Choose a new set S^* disjoint from S, but in bijective correspondence with S.[43]
- Let $S \coprod S^*$ be the set of "letters."
- Given $s^* \in S^*$, let $(s^*)^* := s \in S$.

43: This is via $s \in S \mapsto s^* \in S^*$.

Now, a *word* is a finite sequence

$$x = (x_1, x_2, \ldots, x_n)$$

of letters $x_i \in S \coprod S^*$, where $i \in [n]$ and $n \geq 0$. Note that the "empty word" corresponds to the $n = 0$ case, which we write as ().[44] The *length* of x is precisely n. A *reduced* word $x = (x_1, \ldots, x_n)$ is one such that $x_k^* \neq x_{k+1}$ for all $k \in [n-1]$. Let us define F as the set of all words. Then, let us take the function

$$\iota : S \to F : s \mapsto (s),$$

where (s) is a word of length 1 in F.[45] Given $x := (x_1, \ldots, x_m)$ and $y := (y_1, \ldots, y_n) \in F$, where $x_i, y_j \in S \coprod S^*$, define

$$x \cdot y := \begin{cases} (x_1, \ldots, x_{m-k}, y_{k+1}, \ldots, y_n), & k < \min(m,n) \\ (y_{m+1}, \ldots, y_n), & k = m < n \\ (x_1, \ldots, x_{m-n}), & k = n < m \\ (), & k = m = n, \end{cases}$$

where k is the largest integer such that $x_{m-j}^* = y_{j+1}$ for all $0 \leq j < k$ and $0 \leq k \leq \min(m,n)$.[46] □

44: That is, () is of length **0**.

45: Our goal is to define an operation via concatenation, but this may give us unreduced words. Our solution is simply to remove any problems, moving from the center of the concatenated word, out.

46: All cases except the first in the definition of the group law are morally "edge cases," but they should be written down.

At this point, we only know that $(F, \cdot)$ is a *magma*.

Proposition 1.5.3 *If G is a group and $\varphi : S \to G$ is a function, then there exists a unique function $\Phi : F \to G$ such that*[47]

(i) $\Phi((s)) = \varphi(s)$ *for all* $s \in S$.
(ii) $\Phi(x \cdot y) = \Phi(x)\Phi(y)$.

47: This is what we use to prove the universal property, even though we do not actually know that F is a group yet.

Proof. For existence, let us extend the definition of $\varphi : S \to G$ to $\varphi : S \coprod S^* \to G$, setting $\varphi(s^*) := \varphi(s)^{-1}$. Now, define

$$\Phi : F \to G : (x_1, \ldots, x_n) \mapsto \varphi(x_1)\varphi(x_2)\cdots\varphi(x_n).$$

This is a function which satisfies (1).[48] Now, given $x, y \in F$ of length m and n, respectively, let us compute

48: That is, it extends φ.

$$x \cdot y = (x_1, \ldots, x_{m-k}, y_{k+1}, \ldots, y_m),$$

where k is such that $x_{m-k}^* \neq y_{k+1}$, but $x_{m-j}^* = y_{j+1}$ for $j < k$. Then,

$$\Phi(x)\Phi(y) = \Phi(x_1)\cdots\Phi(x_{m-k})\Phi(x_{m-k+1})\cdots\Phi(x_m)\Phi(y_1)\cdots\Phi(y_k)$$

up to $\Phi(y_{k+1})\cdots\Phi(y_n)$. If $j < k$, then $x_{m-j}^* = y_{j+1}$, which is precisely

$$\varphi(x_{m-j}^*) = \varphi(x_{m-j})^{-1} = \varphi(y_{j+1}),$$

so

$$\begin{aligned} \Phi(x)\Phi(y) &= \varphi(x_1)\cdots\varphi(x_{m-k})\varphi(y_{k+1})\cdots\varphi(y_n) \\ &= \Phi(x \cdot y), \end{aligned}$$

proving (2). Now, why is this unique? Well, if $\Phi : F \to G$ satisfies (1) and (2), note that $() \cdot () = ()$ in F, so $\varphi(())\varphi(()) = \varphi(()) = e \in G$. Likewise,

$(s)(s^*) = () = (s^*)(s)$, then

$$\varphi((s))\varphi((s^*)) = e = \varphi((s^*))\varphi((s)) = \varphi((s^*)) = \varphi((s))^{-1}.$$

Now, we know, in general, a word x of length n is a product of a word (x_1) of length 1 and a word $(x_2, \dots, x_n)$ of length $n-1$ in F. Then, we have[49]

49: This is just (2).

$$\Phi((x_1)(x_2, \dots, x_n)) = \Phi((x_1))\Phi((x_2, \dots, x_n)),$$

and induction on n will show[50]

50: This shows that the formula we made is the unique correct one.

$$\Phi((x_1, \dots, x_n)) = \varphi((x_1)) \cdots \varphi((x_n)).$$

$\square$

Finally, we need to show that F is a group. The easy part is taking $() = e$, as it acts as an identity element. If $x = (x_1, \dots, x_n)$, then define $x^{-1} := (x_n^*, x_{n-1}^*, \dots, x_1^*)$.[51] We now need to show that $(F, \cdot)$ is associative.[52] Let $G := \mathrm{Sym}(F)$. Given $a \in S \coprod S^*$, let $\lambda_a : F \to F$ be defined by $\lambda_a(x) := (a) \cdot x$. Now, we have that

51: As an exercise, check that $x \cdot x^{-1} = () = x^{-1} \cdot x$.

52: We use a trick here. For some reason, many algebra texts, at this point, give a monologue about how difficult associativity is to show for F. Rezk strongly disagrees.

$$\lambda_a(x) = \begin{cases} (a, x_1, \dots, x_n), & a^* \neq x_1 \\ (x_2, \dots, x_n), & x^* = x. \end{cases}$$

We can calculate that $\lambda_a(\lambda_{a^*}(x)) = x$ and $\lambda_{a^*}(\lambda_a(x)) = x$. Hence, $\lambda_a, \lambda_{a^*} \in G = \mathrm{Sym}(F)$, as $\lambda_{a^*} = \lambda_a^{-1}$. This is nice, because we have just constructed a function

$$\begin{tikzcd} S \arrow[r, "a \mapsto \lambda_a"] \arrow[d, tail, "\iota"] & G \\ F \arrow[ur, "\Phi"] & \end{tikzcd}$$

Figure 1.7: This is by what we showed: there exists a unique function Φ such that $\Phi((s)) = \lambda_s$ and $\Phi(x \cdot y) = \varphi(x)\varphi(y)$.

We claim that Φ is an injection. Well, $\Phi(x)(())$ for $\Phi(x) \in G = \mathrm{Sym}(F)$ and $() \in F$, so plug this into $\Phi(x)$. Then, we have $\Phi(x) = \lambda_{x_1} \circ \cdots \circ \lambda_{x_n}$ and $(\lambda_{x_1} \circ \cdots \circ \lambda_{x_n})() = (x_1, \dots, x_n)$. We have $F \overset{\Phi}{\longleftrightarrow} (F) \leq G$ by $\Phi(x \cdot y) = \varphi(x)\varphi(y)$.[53]

53: This ending is more of a sketch, due to time constraints, but we get associativity because it isomorphic as a *magma* to the image of Φ in G.

1.6 Group Presentations and S_n

As notation, we will write $F(S)$ to be "*the* free group on the set S," and $\iota : S \rightarrowtail F(S)$ is *essentially* inclusion.

Definition 1.6.1 (Group Presentation) *A group presentation is a pair (S, R), where S is a set and $R \subseteq F(S)$.*

Now, given a presentation (S, R), we can form a group[54]

54: This is called the group *presented by* (S, R).

$$G := \langle S | R \rangle := F(S)/N,$$

where[55]

$$N := \left\langle \bigcup_{g \in F(S)} gRg^{-1} \right\rangle \trianglelefteq F(S).$$

55: The normal subgroup N is called the *normal closure*.

Definition 1.6.2 (Finitely Presentable) *We call a group G finitely presentable if there exist finite sets $S, R \subseteq F(S)$ such that $G \simeq \langle S | R \rangle$.*

Example 1.6.1 We have $\langle S | \varnothing \rangle \simeq F(S)$.

Example 1.6.2 Consider $\langle a | a^n \rangle$. In this case, $S = \{a\}$ and $R = \{a^n\} \subseteq F(S)$. Hence, $\langle a | a^n \rangle \simeq C_n$

Example 1.6.3 Now, consider $\left\langle a, b \middle| aba^{-1}b^{-1} \right\rangle$. This "forces" $aba^{-1}b^{-1} = e$, so $ab = ba$. This is isomorphic to $C_\infty \times C_\infty \simeq \mathbb{Z} \times \mathbb{Z}$.

Example 1.6.4 Here is a fun example. Consider

$$\left\langle a, b \middle| aba^{-1}b^{-2}, bab^{-1}a^{-2} \right\rangle.$$

Interestingly, this is isomorphic to $\{e\}$.[56]

56: This shows that a group can have multiple presentations.

Remark 1.6.1 Note that we can write any group as $G = \langle G | R \rangle = F(G)/N$, where $N = \ker(F(G) \to G)$, and set $R = N$.

Example 1.6.5 We have $\left\langle r, s \middle| r^n, s^2, srsr \right\rangle \simeq D_{2n}$.

How would we show something like that? Well, we have to construct an isomorphism from $F(r,s)/N \to D_{2n} \subseteq \mathrm{GL}_3(\mathbb{R})$.[57] We construct

57: Note that this is the *correct* direction, since the quotient is specifically built for constructing homomorphisms.

$$\begin{array}{ccc} F(r,s) & \overset{\varphi}{\xrightarrow{\hspace{6em}}\!\!\!\!\twoheadrightarrow} & D_{2n} \subseteq \mathrm{GL}_3(\mathbb{R}) \\[2em] r & \longmapsto & \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) & \\ \sin(2\pi/n) & \cos(2\pi/n) & \\ & & 1 \end{pmatrix} = R \\[2em] s & \longmapsto & \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix} = S \end{array}$$

Let $N := \left\langle \{grg^{-1}, gs^2g^{-1}, g(sr)^2g^{-1}\} \right\rangle$. We need to check that $N \subseteq \ker\varphi$, so we need to show $r^n, s^2, srsr \in \ker\varphi$. We get that gr^ng^{-1}, etc $\in \ker\varphi \trianglelefteq F(S)$, so $\left\langle \{gr^ng^{-1}, \dots\} \right\rangle \subseteq \ker\varphi$. Thus, we have a surjective homomorphism $\langle S | R \rangle \twoheadrightarrow D_{2n}$. We can complete this argument by showing that every element in the given presentation is equal to one of $e, r, \dots, r^{n-1}, s, sr, \dots, s, sr^{n-1}$. To do this, (1) we know in G we can

$$\begin{tikzcd} F(s,r) \arrow[r, two heads, "\varphi"] \arrow[d] & D_{2n} \\ F(s,r)/N \arrow[ur, dashed, "?", "\overline{\varphi}"'] & \end{tikzcd}$$

Figure 1.8: We need $\overline{\varphi}$.

always move s past a power of r.[58] Hence, we can reduce every element to the form $s^i r^j$. Then, (2) we use the relations $r^n = e$ and $s^2 = e$.

58: This is because $rs = sr^{-1}$.

Remark 1.6.2 It is very difficult to work with presentations. It is not a calculational tool that you can always find an answer for. This is why we need the tool of building homomorphisms.

Remark 1.6.3 (Word Problem) Given S, R finite and a presentation $G = \langle S|R \rangle$. Provide an algorithm to decide for each $w \in F(S)$, whether the image in G is id.

Theorem 1.6.1 *There exist finite group presentations which are undecidable.*[59]

59: That is, there is *not* an algorithm.

Example 1.6.6 The symmetric group S_n can be presented as

$$S_n = \left\langle s_1, s_2, \ldots, s_{n-1} \middle| \begin{array}{c} s_i s_i, \\ (s_i s_{i+1})^3, \\ (s_i s_j)^2 \text{ if } |i-j| \geq 2 \end{array} \right\rangle.$$

Proof. We leave out the proof, but the idea is to use $s_i = (i \ i+1)$.[60] □

60: See Rezk's notes.

Actions and Automorphisms | 2

Now that we have reviewed the structure of groups, we will begin to investigate the consequences of this structure within a broader context. Topics will vary, but include a discussion of group actions, the simplicity of A_n, and the automorphism groups $\mathrm{Inn}(G)$ and $\mathrm{Out}(G)$

2.1 Group Actions

Definition 2.1.1 (Group Action) *A group action is the triple $(G, X, G \times X \to X)$, where G is a group, X is a set, and $(g, x) \mapsto gx$, such that*

(i) $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$.
(ii) $e \cdot x = x$.

We say that "G acts on X." Some alternate notation is to define $\varphi_g(x) := gx$, then $\varphi_g : X \to X$ is a function.

Proposition 2.1.1 *Defining $\varphi : G \to \mathrm{Sym}(X)$ by $g \mapsto (\varphi_g : X \to X)$ is a homomorphism of groups.*[1]

Conversely, given a homomorphism $\varphi : G \to \mathrm{Sym}(X)$, define $gx := \varphi(g)(x)$. Then, this defines a group action $(G, X, (g, x) \mapsto \varphi(g)(x))$.

Example 2.1.1 Let $G = G$ and $X = G$. Then, define $g \cdot x$.[2]

Example 2.1.2 Taking $H \leq G$, let $G = G$ and $X = G/H$. We define the action by $g \cdot xH := (gx)H$, which corresponds to the homomorphism $G \to \mathrm{Sym}(G/H)$ with $g \mapsto (xH \mapsto gxH)$.[3]

Definition 2.1.2 (Transitive Action) *An action by G on X is transitive if for all $x, x' \in X$ there exists a $g \in G$ such that $g \cdot x = x'$* and $X \neq \varnothing$.

Definition 2.1.3 (Kernel of Action) *We define the kernel of the action*

$$\ker[G \xrightarrow{\varphi} \mathrm{Sym}(x)] := \{g \in G : g \cdot x = x \textit{ for all } x \in X\}.$$

Note that since we have any action corresponding to a homomorphism $\varphi : G \to \mathrm{Sym}(X)$, we have that the kernel of the action is *precisely* $\ker \varphi \trianglelefteq G$.

Definition 2.1.4 (Stabilizer Subgroup) *Given an action by G on X and*

1: We would need to check that φ_g is a bijection and a group homomorphism:

$$\varphi_g \circ \varphi_h = \varphi_{gh}.$$

2: This is called the *left action* of G on itself.

3: This is the *left coset action*.

$x \in X$, the stabilizer[4]

$$\mathrm{stab}(x) = G_x := \{g \in G : g \cdot x = x\} \leq G.$$

4: This is *not* the kernel. Look carefully.

Example 2.1.3

(a) For any set X, we can take the *tautological action* by $G := \mathrm{Sym}(X)$, so $g \cdot x := g(x)$.[5]
(b) Another example is the action on *right cosets*, where we take $X := H\backslash G = \{Hx\}$. Then, we define the action by $g \cdot Hx := Hxg^{-1}$.[6]
(c) We also have the *conjugation action*, where we take $X := G$ and

$$\mathrm{conj}_g(x) := gxg^{-1},$$

with $g, x \in G$, so $\mathrm{conj}_g \in \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$.[7]
(d) The *trivial* action for a G-set X is $g \cdot x = x$ for all $g \in G$, $x \in X$.

5: In this case,

$$\varphi = \mathrm{id}_G : G \to \mathrm{Sym}(X).$$

6: Convince yourself that we need g^{-1}. Otherwise, it will not work.

7: The operator conj defines a homomorphism from $G \to \mathrm{Sym}(G)$ via $G \xrightarrow{\mathrm{conj}} \mathrm{Aut}(G)$.

Exercise 2.1.1 Prove that

$$\bigcap_{x \in X} \mathrm{stab}(x) = \ker[G \xrightarrow{\varphi} \mathrm{Sym}(x)].$$

Definition 2.1.5 (Faithful Action) *An action is faithful if* $\ker \varphi = \{e\}$.

Definition 2.1.6 (Free Action) *An action is free if* $\mathrm{stab}(x) = \{e\}$ *for all* $x \in X$.[8]

8: The trivial group acting on the empty set is an example of an action which is free but not faithful.

Proposition 2.1.2 *If X is a G-set, then if $x, y \in X$ such that $y = g \cdot x$ for some $g \in G$. Then, $G_x \simeq G_y$. In fact,*[9]

$$G_y = gG_xg^{-1} := \{gag^{-1} : a \in G_x\}.$$

9: That is, the isomorphism is given by $\gamma : a \mapsto gag^{-1}$, conjugation.

Proof. We must first show that γ is well-defined. That is, if $a \in G_x$, then $\gamma(a) = gag^{-1} \in G_y$. In fact, $gag^{-1} \cdot y = ga \cdot x = g \cdot (ax) = g \cdot x = y$. This actually shows that $gG_xg^{-1} \leq G_y$. Since $x = g^{-1} \cdot y$, the same argument give $g^{-1} \cdot G_y(g^{-1})^{-1} \subseteq G_x$, which shows that γ has an inverse function given by sending $b \mapsto g^{-1}bg$. $\square$

2.2 Applications of Actions and Orbits

Theorem 2.2.1 (Cayley) *Every group G is isomorphic to a subgroup of some* $\mathrm{Sym}(X)$ *for some set X. Furthermore, if G is finite, then we can choose* $|X| < \infty$.[10]

10: It turns out, this is not very useful. It is, however, historically important.

Proof. We have the left action by G on $X = G$, given by

$$\varphi : G \to \mathrm{Sym}(X),$$

where $\varphi(g)(x) = gx$. This is a faithful action; i.e., the kernel of φ is trivial.[11] Thus, $\varphi : G \xrightarrow{\sim} \varphi(G) \leq \mathrm{Sym}(X)$. $\square$

11: It is also free.

Proposition 2.2.2 *Let $|G| < \infty$, and let p be the smallest prime such that $p \mid |G|$. Then, any subgroup $H \leq G$ with $|G : H| = p$ is a normal subgroup.*[12]

12: You already know this for $p = 2$.

Proof. The proof is that there is the left action by G on $X = G/H$. We have a homomorphism $\varphi : G \to \mathrm{Sym}(G/H) \simeq S_p$. Let $K := \ker \varphi \leq G$. Note that $K \leq H$, as if $\varphi(g) = \mathrm{id}$, then $\varphi(g)(eH) = gH = eH$, so $g \in H$. We know, by the first isomorphism theorem, that $G/K \simeq \varphi(G) \leq S_p$. We also know that

$$|\varphi(G)| = |G/K| = |G : K| = |G : H| = |H : K| = p|H : K|.$$

Now, $\varphi(G) \leq S_p$ so $|\varphi(G)|$ dives $p!$, so $|H : K|$ divides $(p-1)!$. Yet, Lagrange actually tells us that $|H : K| = |H|/|K| \mid |G|$. We know that p is the smallest prime factor dividing $|G|$. Hence, $|H : K| = 1$, so $K = \ker \varphi = H \trianglelefteq G$. $\square$

Definition 2.2.1 (Orbit) *Given a G-set X, we can define a relation $\sim$ on X by the recipe $x \sim y$ if and only if there exists a $g \in G$ such that $g \cdot x = y$ under the action.*[13] *The orbit $G \cdot x$ is an equivalence class of this relation:*

$$G \cdot x := \{g \cdot x : g \in G\}.$$

13: Show that this is an equivalence relation on X.

Note that the equivalence relation partitions X into pairwise disjoint and non-empty subsets (the orbits).

Definition 2.2.2 (Transitive Action) *An action is transitive if there is exactly one orbit.*[14]

14: This is equivalent to the prior definition.

Remark 2.2.1 Recall that if $x \sim y$, then G_x and G_y are conjugate subgroups of G.

Theorem 2.2.3 (Orbit/Stabilizer) *For any action G on X, and for any $x \in X$, there is a bijection*

$$G/\operatorname{stab}(x) \xrightarrow[\text{bijection}]{g\operatorname{stab}(x) \mapsto g \cdot x} G \cdot x.$$

As a consequence, for any orbit $\mathcal{O} \subseteq X$, we have that $|\mathcal{O}| = |G : \operatorname{stab}(x)|$, for any $x \in \mathcal{O}$.[15]

15: We essentially proved this on the second problem set.

Proposition 2.2.4 *If X is a G-set, with $|X| < \infty$, then*

$$|X| = \sum_{k=1}^{r} |G : \operatorname{stab}(x)|,$$

where $x_1, \ldots, x_r \in X$ are representative elements of the distinct orbits of the *action.*[16]

16: In other words, $G \cdot x_i \cap G \cdot x_j = \varnothing$ if $x_i \neq x_j$, and

$$\bigcup_{i=1}^{r} G \cdot x_i = X.$$

Proof. X is partitioned into pairwise disjoint sets via the orbits, and using the orbit/stabilizer theorem, we have a way to count. □

2.3 Cauchy's Theorem

Definition 2.3.1 (Fixed Set of Action) *Define*

$$X^G := \{x \in X : g \cdot x = x \text{ for all } g \in G\}.$$

Example 2.3.1 Let us consider actions by $G := C_p$, where p is prime. Suppose X is a G-set, $|X| < \infty$. The orbits can have size 1 or p. Let m be the number of orbits of size 1, and write n as the size of orbits of size p. Then, $|X| = m + pn$. That is,

$$|X| = m + pn \equiv m = \left|X^G\right| \pmod{p}.$$

Theorem 2.3.1 (Cauchy) *Let G be a finite group, and let p be a prime such that $p \mid |G|$. Then there exists a $g \in G$ with $|g| = p$.*[17]

17: We give a more recent proof, due to McKay, which is a lot more clever than the standard proof you will see in algebra texts.

Proof. Consider the set

$$X := \{(g_1, \ldots, g_p) \in G^p : g_1 \cdots g_p = e\}.$$

Then, we have that $|X| = |G|^{p-1} =: n^{p-1}$. This is because g_p is the inverse of $(g_1 \cdots g_{p-1})^{-1}$. In particular, $p \mid |X|$. Now, define a function

$$\begin{aligned} X &\xrightarrow{\varphi} X \\ (g_1, \ldots, g_p) &\longmapsto (g_2, \ldots, g_p, g_1). \end{aligned}$$

We need to verify that $(g_1, \ldots, g_p) \in X$ implies $\varphi(g_1, \ldots, g_p) \in X$. Well, if $g_1 g_2 \cdots g_p = e$, then conjugating by g^{-1} tells us that $g_2 \cdots g_p g_1 = e$.[18] Also, if we compose $\varphi^p = \mathrm{id}$, so if $H = C_p = \langle \varphi \rangle$, then we get an action by H on X. Explicitly,

18: In fact, φ^{-1} also takes X into X. Thus, φ is actually a permutation of the set X.

$$\begin{aligned} H = \langle \varphi \rangle &\longrightarrow \mathrm{Sym}(X) \\ \varphi &\longmapsto \varphi. \end{aligned}$$

Now, recall that if $H = C_p$ acts on a finite set, then $|X| \equiv \left|X^H\right| \pmod{p}$. Now, in our case, we have that

$$\left|X^H\right| \equiv |X| \equiv 0 \pmod{p}.$$

What is X^H? Since H is cyclic, the fixed set

$$X^H = \{x \in X : \varphi(x) = x\},$$

which is precisely the set

$$X^H = \{(g_1, \dots, g_p) \in G^p : g \in G, g^p = e\}$$

Since $(e, \dots, e) \in X^H$, we have that $\left|X^H\right| \geq p$, so any $g \in G$ with $g \neq e$ has $(g, \dots, g) \in X^H$ with order p.

$\square$

2.4 A Note on Cycles and A_n

Given $G := \mathrm{Sym}(X)$, and given a sequence $x_1, \dots, x_k$ of distinct elements in X, define[19]

$$\sigma := (x_1\ x_2\ \cdots\ x_k) \in G,$$

where

$$\sigma(x) = \begin{cases} x, & \text{if } x \notin \{x_1, \dots, x_l\} \\ x_{i+1}, & \text{if } x = x_i, i \in [k-1] \\ x, & \text{if } x = x_k. \end{cases}$$

19: Note that we can cylically permute the elements of σ freely, as long as we do not change the cyclic order. Also, $(x_1) = \mathrm{id}$.

Any cycles $\sigma = (x_1, \dots, x_k)$, $\tau = (y_1, \dots, y_\ell)$ are *disjoint* if the sets

$$\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_\ell\} = \varnothing.$$

If so, then $\sigma\tau = \tau\sigma$.

Proposition 2.4.1 *If $|X| < \infty$, then every $g \in \mathrm{Sym}(X)$ is equal to a product of disjoint, nontrivial cycles. Furthermore, this representation is unique up to reordering the cycles.*

Proof Outline. The idea is that $H = \langle g \rangle \leq \mathrm{Sym}(X)$ acts tautologically on X. We know that when we have a group action, we can decompose it into the orbits of the action by H on X.[20] $\square$

20: These are basically the cycles.

For instance, consider $g \in S_9$ defined by

$$\begin{tikzcd}
1 \arrow[d] & 5 \arrow[l] & 2 \arrow[d] & 7 \arrow[l] & 6 \arrow[d, leftrightarrow] \\
3 \arrow[r] & 8 \arrow[u] & 4 \arrow[ur] & & 9
\end{tikzcd}$$

In this case, we can decompose[21] $g = (1\ 3\ 8\ 5)(2\ 4\ 7)(6\ 9)$.

21: The picture gives us all the information about the disjoint cycles that we need.

We also have the *cycle conjugation formula*. If we have

$$\sigma = (x_1\ x_2\ \cdots x_k) \in \mathrm{Sym}(x)$$

and $g \in \mathrm{Sym}(X)$, then

$$g(x_1\ x_2\ \cdots\ x_k)g^{-1} = (g(x_1)\ g(x_2)\ \cdots\ g(x_k)).$$

Now, given sgn : $S_n \to \{\pm 1\}$.[22] Then,

$$\ker(S_n \xrightarrow{\text{sgn}} \{\pm 1\}) =: A_n \leq S_n.$$

22: This is the sign homomorphism. One "formula" is

$$\text{sgn}(\sigma) = \det[e_{\sigma(1)} \cdots e_{\sigma(n)}].$$

Theorem 2.4.2 *A_n is simple if $n \geq 5$.*[23]

23: A group is called *simple* if it only has two normal subgroups.

Proof. Use the cycle conjugation formula to show that any nontrivial $N \trianglelefteq A_n$ contains every element of A_n. □

Example 2.4.1 One example of a simple group is C_p for prime p.

2.5 Category Set_G of G-Sets

Now, fix a group G. We can define a category of G-sets called Set_G. We define the objects $\operatorname{ob}\mathsf{Set}_G$ to be $(X, G \xrightarrow{\varphi} \text{Sym}(x))$ and the morphisms $\text{Hom}_{\mathsf{Set}_G}((X,\varphi),(X',\varphi'))$ to be functions of sets $f : X \to X'$ such that for all $g \in G$ and $x \in X$, then[24]

$$f(\varphi(g)(x)) = \varphi'(g)(f(x)).$$

24: If we write both actions as $g \cdot x$, then the condition is

$$f(g \cdot x) = g \cdot f(x).$$

Given this language, we can now talk about isomorphisms of G-sets.

Proposition 2.5.1 *If we have*

$$f \in \text{Hom}_{\mathsf{Set}_G}((X,\varphi),(X',\varphi'))$$

is an isomorphism if and only if it is a bijection $X \to X'$.[25]

25: Note that there are categories, such as the category of topological spaces, where the isomorphisms are *not* simply bijections.

Proposition 2.5.2 *Fix G. Any transitive G-set is isomorphic in Set_G to an object of the form G/H for some $H \leq G$.*[26] *We also have that H is unique up to conjugation in G; i.e., there is a bijective correspondence between transitive G-sets up to isomorphism and subgroups of G up to conjugacy.*

26: Here, G/H is precisely the set of left cosets with the standard left coset action.

Proof. If X is a transitive G-set, pick an element $x \in X$, and let

$$H := \text{stab}(x) \leq G.$$

Then, define a function

$$\begin{aligned} G/H &\xrightarrow{f} X \\ gH &\longmapsto g \cdot x. \end{aligned}$$

We claim that f is a well-defined bijection. Now, we show that f is a morphism in Set_G. Well, for all $g \in G$, $f(g \cdot aH) = g \cdot f(aH)$, and $f(g \cdot aH) = f(g \cdot aH) = ga \cdot x$, and $g \cdot f(aH) = g \cdot (a \cdot x)$.[27] Note that we can show that if $f : G/H \to X$ is any isomorphism of G-sets, then let $x_0 := f(eH)$. We can calculate that $\text{stab}(x_0) = H$. If $g \in G$ and

27: This last statement is true, so f is a morphism by symmetry.

$g \cdot x_0 = x_0$, then $f^{-1}(g \cdot x_0) = f^{-1}(x_0)$, and we can pull the g out to give us $g \cdot eH = g \cdot f^{-1}(x_0) = eH$, so $g \in H$.[28] □

28: Use the same argument, but backwards, to show the other direction of inclusion.

Whereas the orbit/stabilizer gives us a way to count, this proposition about Set_G gives us a way to *classify*.

2.6 Conjugation Action

Recall that if we have $g, x \in G$, then $\mathrm{conj}_g(x) = gxg^{-1}$. This gives a group action $G \to \mathrm{Sym}(G)$.

Definition 2.6.1 (Conjugacy Class) *The orbits of the conjugation action are*[29]

$$\mathrm{Cl}(x) := \{gxg^{-1} : g \in G\},$$

called the conjugacy classes.

29: Recall that these partition G by subsets.

Definition 2.6.2 (Centralizer) *The stabilizer of the conjugation action is*

$$\mathscr{C}_G(x) := \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\},$$

called the centralizer subgroup.[30]

30: We have that $\mathscr{C}_G(x) \leq G$.

Remark 2.6.1 The kernel of $\mathrm{conj} : G \to \mathrm{Sym}(G)$ is precisely

$$\mathscr{Z}(G) := \{g \in G : gx = xg \text{ for all } x \in G\} \trianglelefteq G,$$

the center of G.[31]

31: This is precisely the intersection of all the centralizers.

Now, recalling the orbit/stabilizer theorem, we know that

$$|\mathrm{Cl}(x)| = |G : \mathscr{C}_G(x)|.$$

Example 2.6.1 We have that $\mathrm{Cl}(e) = \{e\}$, and $\mathscr{C}_G(e) = G$.

Example 2.6.2 Now, if G is abelian, then $\mathscr{C}_G(x) = G$ and $\mathrm{Cl}(x) = \{x\}$. It is not very informative in this case.

Let $G := D_{2n}$. We can write

$$D_{2n} = \left\langle r, s \middle| r^n, s^2, (sr)^2 \right\rangle = \{e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}.$$

Since there are two generators r, s, all we need is the following:[32]

32: Note that D_{4n} always has a center of order 2.

$$\begin{aligned}
\mathrm{conj}_r(r^k) &= r^k \\
\mathrm{conj}_r(sr^k) &= sr^{k-2} \\
\mathrm{conj}_s(r^k) &= r^{-k} \\
\mathrm{conj}_s(sr^k) &= sr^{-k}.
\end{aligned}$$

Remark 2.6.2 The general method for D_{2n} is to conjugate each element by r and s, via the formulae computed, after chasing the conjugation diagrams.[33]

33: We can use the orbit/stabilizer theorem to deduce the order of the centralizers. In D_{4n+2}, it is typical to have all reflections in the same conjugacy class.

Theorem 2.6.1 (Class Equation) *Let $|G| < \infty$. Then,*

$$|G| = |\mathfrak{Z}(G)| + \sum_{k=1}^{r} |G : \mathscr{C}_G(g_k)|,$$

where $g_1, \ldots, g_k$ are representative elements of distinct conjugacy classes of G, which are not contained in $\mathfrak{Z}(G)$.[34]

34: Recall that $g \in \mathfrak{Z}(G)$ if and only if $\mathrm{Cl}(g) = g$. Note that each term on the RHS divides $|G|$, and

$$1 < |G : \mathscr{C}_G(g_k)| < |G|.$$

Proof. There are two types of orbits $\mathbb{O}$ of conj:

- $|\mathbb{O}| = 1$ if and only if $|G : \mathscr{C}_G(x)| = 1$ if and only if $x \in \mathfrak{Z}(G)$.
- $|\mathbb{O}| \geq 2$ if and only if $|\mathbb{O}| = |G : \mathscr{C}_G(x)|$ for any $x \in \mathbb{O}$.

Now, for any group action on X, we have

$$|X| = \sum_{|\mathbb{O}|=1} |\mathbb{O}| + \sum_{|\mathbb{O}|\geq 2} |\mathbb{O}|,$$

and grouping view counting and our observations above yields the class equation. □

Despite this being a seemingly silly result, we can actually get some nifty results out of it.

Definition 2.6.3 (p-group) *A p-group is a finite group with $|G| = p^d$, where $d \geq 1$.*

Theorem 2.6.2 *Every p-group has a non-trivial center.*

Proof. Use the class equation:we know that $|G| = p^d$, and the indices $m_i \mid p^d$, and $1 < m_i < p^d$, so $p \mid |G|$ and $p \mid m_i$ for all i. Thus, $p \mid |\mathfrak{Z}(G)|$, which means the center is nontrivial.[35] □

35: This tells us that p-groups can "de-structured" by using this fact about their centers.

Corollary 2.6.3 *If we have $|G| = p^2$, then G is abelian.*

Proof. For any group G, if $G/\mathfrak{Z}(G)$ is cyclic, then G is abelian.[36] Now, if $|G| = p^2$, then $|\mathfrak{Z}(G)| \in \{p, p^2\}$, by the theorem, so $|G/\mathfrak{Z}(G)| \in \{1, p\}$, so $G/\mathfrak{Z}(G)$ is cyclic. □

36: Why is this true? Well, pick $\langle \overline{g} \rangle \in G/\mathfrak{Z}(G)$. Lift $\overline{g}$ to an element $g \in G$. We claim that every element y of G can be written as $y = g^k x$, where $x \in \mathfrak{Z}(G)$, and $k \in \mathbb{Z}$. Thus, if we have $g^k x g^\ell x' = g^\ell x' g^k x$.

2.7 Automorphism Groups

Recall that an *endomorphism* of a group G is a homomorphism $\varphi : G \to G$, and an *automorphism* is an isomorphism $\varphi : G \to G$. Note that in general,

$$\underbrace{\mathrm{Aut}(G)}_{\text{group}} \subseteq \underbrace{\mathrm{End}(G)}_{\text{monoid}} = \mathrm{Hom}_{\mathsf{Grp}}(G, G).$$

Now, recall that we have a homomorphism

$$\mathrm{conj} : G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G),$$

and $\ker(\mathrm{conj}) = \mathfrak{Z}(G)$.

Definition 2.7.1 (Inner Automorphisms) *The image*[37]

$$\mathrm{conj}(G) =: \mathrm{Inn}(G) \leq \mathrm{Aut}(G),$$

is the inner automorphism group, and by the first isomorphism theorem, $\mathrm{Inn}(G) \simeq G/\mathfrak{Z}(G)$.

37: That is, the image of conjugation is the *group* of inner automorphisms.

Example 2.7.1 If G is abelian, then $\mathrm{Inn}(G) = \{\mathrm{id}\}$.[38]

38: Once again, abelian groups make our tools useless.

Example 2.7.2 Let $G := D_6$. What is $\mathrm{End}(D_6)$? Fix H. Well, there is a bijection

$$\left\{\begin{matrix}\text{homomorphisms}\\ D_6 \xrightarrow{\varphi} H\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}(R, S) \in H \times H\\ R^3 = S^2 = SRSR = e\end{matrix}\right\}.$$

Suppose $H = D_6$. Then, $R^3 = e$ implies $R \in \{e, r, r^2\}$ and $S^2 = e$ implies $S \in \{e, s, sr, sr^2\}$, such that $(SR)^2 = e$.[39]

39: There will be 10 distinct endomorphisms. What if we were, instead, checking for automorphisms? We know that if $\varphi \in \mathrm{Aut}(G)$, then $R \in \{r, r^2\}$ and $S \in \{s, sr, sr^2\}$, so we have an upper bound

$$|\mathrm{Aut}|(D_6) \leq 6.$$

We also have $\mathrm{Inn}(D_6) \simeq D_6/\mathfrak{Z}(G)$, which is of order 6. Thus, there exists an isomorphism

$$D_6 \xrightarrow{\sim} \mathrm{Aut}(D_6),$$

via conj.

Proposition 2.7.1 *Let $\varphi \in \mathrm{Aut}(G)$. Then, with $g \in G$, we can write*

$$\varphi \,\mathrm{conj}_g\, \varphi^{-1} = \mathrm{conj}_{\varphi(g)}\,.$$

As such, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. Let $x \in G$. Then,

$$\begin{aligned}(\varphi \,\mathrm{conj}_g\, \varphi^{-1})(x) &= \varphi(\mathrm{conj}_g(\varphi^{-1}(x)))\\ &= \varphi(g\varphi^{-1}(x)g^{-1})\\ &= \varphi(g)\varphi(\varphi^{-1}(x))\varphi(g)^{-1}\\ &= \varphi(g)x\varphi(g)^{-1} = \mathrm{conj}_{\varphi(g)}(x).\end{aligned}$$

$\square$

Definition 2.7.2 (Outer Automorphisms) *Seeing as the inner automorphisms form a normal subgroup, we can form the outer automorphism group*[40]

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\,\mathrm{Inn}(G).$$

40: Note that there are not "outer automorphisms." Rather, $\mathrm{Out}(G)$ contains equivalence classes of automorphisms.

Recall that $\mathrm{Inn}(G) \simeq G/\mathfrak{Z}(G)$. How do you find "outer automorphisms" of G? We want to *embed* G as a normal subgroup in some H. Take $G \trianglelefteq H$. We get[41]

$$\begin{tikzcd} H \arrow[r, "\kappa"] & \mathrm{Aut}(G) \\ h \arrow[r, mapsto] & \mathrm{conj}_h\big|_G. \end{tikzcd}$$

41: That is, $\kappa(h)(g) = hgh^{-1}$.

Proposition 2.7.2 *The kernel of κ, as above, is*

$$\ker\kappa = \mathscr{C}_H(G) := \{h \in H : hx = xh \text{ for all } x \in G\},$$

the centralizer of G in H.[42]

42: This is immediate from the definiton.

Proposition 2.7.3 *We can also write*

$$\kappa^{-1}(\mathrm{Inn}(G)) = \mathscr{C}_H(G)G \trianglelefteq H.$$

Proof. Note that $\kappa(\mathscr{C}_H(G)) = \{\mathrm{id}\}$ and $\kappa(G) \subseteq \mathrm{Inn}(G)$. Suppose $z \in H$, so that $\kappa(z) \in \mathrm{Inn}(G)$. Then, there exists a $g \in G$ such that $\kappa(z) = \kappa(g) = \mathrm{conj}_g$. If we take

$$\kappa(zg^{-1}) = \kappa(z)\kappa(g)^{-1} = \mathrm{id},$$

so $y = zg^{-1} \in \mathscr{C}_H(G)$. Thus, $z = yg \in \mathscr{C}_H(G)G$, which means $\kappa^{-1}(\mathrm{Inn}(G)) = \mathscr{C}_H(G)G$. □

$$\begin{tikzcd} H \arrow[r, "\kappa"] \arrow[d, two heads] & \mathrm{Aut}(G) \arrow[d, two heads, "\pi"] \\ H/\mathscr{C}_H(G)G \arrow[r, tail] & \mathrm{Aut}(G)/\,\mathrm{Inn}(G) = \mathrm{Out}(G) \end{tikzcd}$$

Figure 2.1: We have that

$$H/\mathscr{C}_H(G)G \simeq K \leq \mathrm{Out}(G).$$

Consider

$$H := D_{16} = \left\langle r, s \middle| r^8, s^2, (sr)^2 \right\rangle.$$

Then, $G = \langle r^2, s\rangle \trianglelefteq H$.[43] Now, $\kappa : H \to \mathrm{Aut}(G)$, and

43: As an exercise, show that $G \simeq D_8$.

$$\ker(\kappa) = \mathscr{C}_H(G) = \{e, r^4\} \subseteq G.$$

Doing this shows that

$$\kappa^{-1}(\mathrm{Inn}(G)) = \mathscr{C}_H(G)G = G.$$

Thus, we have an injective homomorphism $\kappa : H/G \rightarrowtail \mathrm{Out}(G)$, where $H/G \simeq \left\langle r \middle| r^2 \right\rangle$ and $\mathrm{Out}(G) \simeq D_8$. Thus, $\mathrm{conj}_r\big|_G$ defines an "outer automorphism" of $G \simeq D_8$.

Proposition 2.7.4 *Let us look at another standard example, S_n. Well, $\mathfrak{Z}(S_n) = \{e\}$ if $n \neq 2$.*[44]

44: In the case where $n = 2$, S_n is abelian, so the center is certainly not trivial.

Proof. Let $\sigma \in \mathfrak{Z}(S_n)$. Then, $\sigma(a\ b)\sigma^{-1} = (a\ b)$, but we also know that $\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b))$. This implies that $\sigma(a) \in \{a, b\}$. If there exists a $c \notin \{a, b\}$, the same argument gives us $\sigma(a) \in \{a, c\}$. Since we can run this for any two elements, $\sigma(a) = a$. □

Remark 2.7.1 Because of the above, if $n \geq 3$, we have that $\mathrm{Inn}(S_n) \simeq S_n$.

Remark 2.7.2 We have that $\mathrm{Out}(S_n) = \{e\}$ unless $n = 6$, in which case $\mathrm{Out}(S_6) \simeq C_2$.[45]

45: We omit proof for when $n \neq 6$. However, note that $\varphi \in \mathrm{Aut}(G)$ preserves a lot of structure. For instance, $\varphi(\mathrm{Cl}(g)) = \mathrm{Cl}(\varphi(g))$, and if $\varphi \in \mathrm{Inn}(G)$, then

$$\varphi(\mathrm{Cl}(g)) = \mathrm{Cl}(G).$$

In the case of the symmetric group, let

$$T := \mathrm{Cl}((1\ 2)) \subseteq S_n.$$

Then, $\varphi(T)$ is a conjugacy class of elements of order 2. We would then show that if $\varphi(T) = T$, then φ is innner, and then we count the sizes of conjugacy classes of elements of order 2 in S_n. We can show that the only class with the same size is T.

Example 2.7.3 In the alternating group A_n, we can show that $\mathfrak{Z}(A_n) = \{e\}$ if $n \neq 3$. The proof is very similar to $\mathfrak{Z}(S_n)$. In fact, $A_n \trianglelefteq S_n$, so we can show that $\mathscr{C}_{S_n}(A_n) = \{e\}$ if $n \geq 5$. As a consequence, we get an injective homomorphism $S_n/A_n \simeq C_2 \rightarrowtail \mathrm{Out}(A_n)$, meaning there always exists a non-trivial automorphism of A_n for all n.

2.8 Automorphisms of Cyclic Groups

Recall that if G is abelian, then $\mathrm{Inn}(G) = \{\mathrm{id}\}$, so $\mathrm{Aut}(G) = \mathrm{Out}(G)$. Consider $G = C_\infty = \langle a | \varnothing \rangle \simeq (\mathbb{Z}, +)$. Then, the endomorphisms in

$$\mathrm{End}(C_\infty) = \mathrm{Hom}(C_\infty, C_\infty) \xrightarrow{\sim} \mathbb{Z},$$

where we just take $\varphi \mapsto n$, taking $\varphi(a) = a^n$.

Remark 2.8.1 Define $\varphi_n \in \mathrm{End}(C_\infty)$ such that $\varphi_n(a) = a^n$, meaning $\varphi_n(a^k) = a^{nk}$. Then, since $\mathrm{End}(C_\infty)$ is a monoid, $\varphi_m \circ \varphi_n(a) = \varphi_m(a^n) = a^{mn} = \varphi_{mn}(a)$. Thus, we have an isomorphism of *monoids* $\mathrm{End}(C_\infty) \simeq (\mathbb{Z}, \cdot)$. Thus, $\mathrm{Aut}(C_\infty) \simeq \{\pm 1\}$.

Example 2.8.1 Let $C_n = \langle a | a^n \rangle \simeq (\mathbb{Z}/n, +)$. Well, $\mathrm{End}(C_n) = \mathrm{Hom}(C_n, C_n) \xrightarrow{\sim} \mathbb{Z}/n$. Then, we can take $\varphi \mapsto [k]$, where $\varphi(a) = a^k$.[46]

46: This k is only defined *up to* modulo n. Like before, we have an isomorphism of monoids, where $(\mathbb{Z}/n, \cdot) \simeq \mathrm{Hom}(C_n, C_n)$. As a consequence, $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n)^\times$, the group of units.

For instance,

$$\begin{aligned}
\mathrm{Aut}(C_2) &= (\mathbb{Z}/2)^\times = \{[1]\} \\
\mathrm{Aut}(C_3) &= (\mathbb{Z}/3)^\times = \{[1], [2]\} \\
\mathrm{Aut}(C_4) &= (\mathbb{Z}/4)^\times = \{[1], [3]\} \\
\mathrm{Aut}(C_5) &= (\mathbb{Z}/5)^\times = \{[1], [2], [3], [4]\} \\
\mathrm{Aut}(C_6) &= (\mathbb{Z}/6)^\times = \{[1], [6]\}.
\end{aligned}$$

Additionally, $|(\mathbb{Z}/7)^\times| = 6$, and $(\mathbb{Z}/8)^\times \simeq V_4$.

Proposition 2.8.1 *In general,*

$$|\mathrm{Aut}(C_n)| = |(Z/n)^\times| = \varphi(n),$$

where φ is Euler's totient function.[47]

47: Recall that the totient counts the number of elemenets $\{0, \ldots, n-1\}$ which are relatively prime to n.

Given this work, you might wonder if we could generalize this work on cyclic groups to abelian groups.

Example 2.8.2 Consider

$$G := \underbrace{C_p \times C_p \times \cdots \times C_p}_{m \text{ products}},$$

where $|G| = p^m$. Then,[48]

$$\mathrm{Aut}(G) \simeq \mathrm{GL}_m(\mathbb{Z}/p).$$

This is, of course, not abelian if $m \geq 2$.

48: This is partially because G is isomorphic to the vector space $(\mathbb{Z}/p)^m$, under addition.

Example 2.8.3 The automorphism group

$$\mathrm{Aut}(C_2 \times C_2) \simeq \mathrm{GL}_2(\mathbb{Z}/2) \simeq S_3.$$

Sylow Theorems and Products | 3

Recall that a *p-group* is a group of order p^a, where $a \geq 1$ and p is prime.

3.1 Sylow Theorems

Definition 3.1.1 (p-Sylow Subgroup) *A subgroup $P \leq G$ such that P is a p-group and $p \nmid |G : P|$ is called p-Sylow.*

Note that this is actually equivalent to saying that $|G| = p^a m$, where $p \nmid m$, and $|P| = p^a$ where $a \geq 1$.

Remark 3.1.1 We have a notation for the set

$$\mathrm{Syl}_p(G) := \{P \leq G : P \text{ is a } p\text{-Sylow subgroup}\}.$$

Now, G acts on $\mathrm{Syl}_p(G)$ via conjugation, as for $g \in G$ and $P \in \mathrm{Syl}_p(G)$, we have that $gPg^{-1} = P' \in \mathrm{Syl}_p(G)$.[1]

1: The notation for cardinality here is

$$n_p(G) := \left|\mathrm{Syl}_p(G)\right|.$$

Now, fix a finite group G and a prime p such that $p \mid |G|$.

Theorem 3.1.1 (Sylow I) *There exists a p-Sylow subgroup of G.*

Theorem 3.1.2 (Sylow II) *Any two p-Sylow subgroups of G are conjugate.*[2] *Thus, a p-Sylow subgroup $P \trianglelefteq G$ if and only if $n_p(G) = 1$.*

2: That is, $\mathrm{Syl}_p(G)$ is a single G-orbit.

Theorem 3.1.3 (Sylow III) *If $P \in \mathrm{Syl}_p(G)$, then*

$$n_p = |G : \mathcal{N}_G(P)|$$

and $n_p \equiv 1 \pmod{p}$.

We will give proofs for the Sylow theorems, but we will start with some applications.

Remark 3.1.2 Fix primes $p < q$. Suppose $|G| = pq$. Then, $n_p \in \{1, q\}$. Similarly, $n_q = 1$.[3]

3: We can have $n_p = q$ if and only if $q \equiv 1 \pmod{p}$, and $n_q = p$ if and only if $p \equiv 1 \pmod{q}$, which does not work.

Proposition 3.1.4 *If $|G| = pq$, then there exists $P \leq G$ such that $|P| = p$, and $A \trianglelefteq G$ such that $|Q| = q$. If we also have that $p \nmid q - 1$, then G is cyclic.*

Proof. In this case, $n_p = 1$, so $P \trianglelefteq G$. Also, because p, q are primes, $P = \langle x \rangle$, $Q = \langle y \rangle$, and $P \cap Q = \{e\}$. Thus, $xy = yx$, so the group is abelian. Why? Well,

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in PP = P$$

and

$$(xyx^{-1})y^{-1} \in QQ = Q,$$

so $xyx^{-1}y^{-1} = \{e\}$. Thus, $z = xy$ has order pq, where $z^k = x^k y^k$, and $= e$ if and only if $x^k = y^{-k} \in P \cap Q = \{e\}$, so $p \mid k$, $q \mid k$. As such, we must have $pq \mid k$. □

Example 3.1.1 (Groups of Order 30) Let $|G| = 30 = 2 \cdot 3 \cdot 5$. We can write that[4]

4: We use Sylow III.

$$n_2 \in \{1, 3, 5, 15\}$$
$$n_3 \in \{1, 10\}$$
$$n_5 \in \{1, 6\}.$$

We claim that we cannot have $n_3 = 10$ and $n_5 = 6$, as $n_3 = 10$ implies G has $2 \cdot 10$ elements of order 3, and $n_5 = 6$ implies G has $4 \cdot 6$ elements of order 5.[5] Choose $|P| = 3$ and $|Q| = 5$. One of these is normal in G. Consider

5: That is too many elements.

$$PQ = \{xy : x \in P, y \in Q\}.$$

We have that $PQ \leq G$, since either P or Q is normal. Thus, $|PQ| = 15$, meaning $|G : PQ| = 2$, and $PQ \trianglelefteq 2$. Yet, $3 \nmid 5 - 1$, so by the previous proposition, PQ is *cyclic*. Thus, every G of order 30 has a normal subgroup $C_{15} \simeq N \trianglelefteq G$.

Example 3.1.2 (Groups of Order 12) If $|G| = 12 = 3 \cdot 2^2$, then

$$n_3 \in \{1, 4\}$$
$$n_2 \in \{1, 3\}.$$

If G has no normal 3-Sylow subgroup, then it is isomorphic to A_4.[6]

6: We omit the proof for brevity. Check Rezk's notes. The idea is that if $n_3 = 4$, then we have an action by G on the set $\mathrm{Syl}_3(G)$ which has size 4. Thus, there is a homomorphism

$$G \xrightarrow{\varphi} \mathrm{Sym}(\mathrm{Syl}_3(G)) \simeq S_4.$$

The exercise here is to show that φ is injective, and $\varphi(G) = A_4$.

Now, let us prove the Sylow theorems.

Proof of Sylow I. We claim $(*)$ that

(i) there exists a proper $H < G$ such that $p \nmid |G : H|$ or
(ii) there exists $N \trianglelefteq G$ such that $|N| = p$.

We will use the claim $(*)$ to prove Sylow I, proceeding by induction on $|G|$. For the *base case*, $|G| = p$ implies $P = G$. For the *inductive step*, by the claim, either (i) or (ii). If (i), then by induction, there exists $P \leq H$ which is p-Sylow in H. Then, $|H| = p^a m'$, where $m' \mid m$. Thus, $P \in \mathrm{Syl}_p(G)$. If (ii), then consider $\overline{G} := G/N$. Then, $\left|\overline{G}\right| = p^{a-1}m < |G|$, and via induction, there exists $\overline{P} \leq \overline{G}$, where $\left|\overline{P}\right| = p^{a-1}$. Write $\pi : G \twoheadrightarrow \overline{G}$ for the canonical quotient homomorphism. Let $P := \pi^{-1}(\overline{P})$. Then $P \leq G$, and $|P| = \left|\overline{P}\right||N| = p^a$, so $P \in \mathrm{Syl}_p(G)$. □

Proof of Claim (∗). Via the class equation, we will show that if not (i), then (ii). Not (i) implies that for all $H < G$, $p \mid |G : H|$. In particular, $p \mid |G : \mathscr{C}_G(x_k)|$ for all $k \in [r]$. The class equation implies that $p \mid |\mathfrak{Z}(G)|$. By *Cauchy*, there exists an $x \in \mathfrak{Z}(G)$ such that $|x| = p$. Set $N := \langle x \rangle \trianglelefteq G$. □

Lemma 3.1.5 *Let $H, K \leq G$. We have an action K onto G/H by $k \cdot gH := kyH$. Then, this action has a fixed point if and only if there exists $x \in G$ such that $K \subseteq xHx^{-1}$.*

Proof. Suppose there exists $xH \in G/H$ such that $k \cdot x = xH$ for all $k \in K$. Then, for all $k \in K$, $kx \in xH$, which means $k = kxx^{-1} \in xHx^{-1}$. Thus, $K \subseteq xHx^{-1}$. Conversely, if $x \in G$ such that $K \subseteq xHx^{-1}$, then for all $k \in K$, $k \in xHx^{-1}$. As such, $kx \subseteq xH$, meaning $kxH = xH$. Thus, xH is a fixed point of the action K onto G/H. □

Proposition 3.1.6 *If $P \in \mathrm{Syl}_p(G)$, and $Q \leq G$ such that Q is a p-group, then there exists an $x \in G$ such that $Q \subseteq xPx^{-1}$.*[7]

7: Equivalenetly, $x^{-1}Qx \subseteq P$.

Proof. We have $Q, P \leq G$ and $|P| = p^a$ and $|G| = p^b \leq p^a$. Remember that $|G : P| = m$, where $p \nmid m$. Consider the action of Q onto G/P. We want to show that this has a fixed point, which by the lemma, would show that $Q \subseteq xPx^{-1}$. We do some counting:

$$|G/P| = \sum_{i=1}^{d} |\mathbb{O}_i|,$$

where each $\mathbb{O}_i \subseteq G/P$ is an orbit of the Q-action. Then, each $|\mathbb{O}_i| \mid |Q| = p^b$. In other words, we have

$$|\mathbb{O}_i| \in \{1, p, p^2, \ldots, p^b\}.$$

Then, $|G/P| = m$, so there exists an i such that $p \nmid |\mathbb{O}_i|$, so $\mathbb{O}_i = \{xP\}$, which is a fixed point. □

Corollary 3.1.7 *If Q is also p-Sylow, then $|Q| = \left|xPx^{-1}\right| = p^a$, so $Q = xPx^{-1}$. This is Sylow II.*

Corollary 3.1.8

$$\bigcup_{P \in \mathrm{Syl}_p(G)} P = \{y \in G : |y| = p^k, k \geq 0\}.$$

Proof of Sylow III. Sylow II tells us that $\mathrm{Syl}_p(G)$ is a transitive G-set. Well, the orbit/stabilizer gives us that[8]

8: Let $P \in \mathrm{Syl}_p(G)$.

$$n_p = \left|\mathrm{Syl}_p(G)\right| = |G : \mathscr{N}_G(P)|.$$

Suppose $P \in \mathrm{Syl}_p(G)$. Then, P inherits an action onto $\mathrm{Syl}_p(G)$, where for $x \in P$ and $Q \in \mathrm{Syl}_p(G)$, x acts on Q by xQx^{-1}. What are the fixed points of the action? Define

$$c := \left|\{Q : Q \in \mathrm{Syl}_p(G) \text{ is fixed by } P\}\right|.$$

Well, $c \geq 1$, as P is fixed by P, and $c \equiv n_p \pmod p$, as $|P| = p^a$ implies orbits of any P-action have sizes $1, p, p^2, \ldots, p^a$. We will show that $c = 1$. Suppose Q is a p-Sylow subgroup such that

$$xQx^{-1} = Q$$

for all $x \in P$. Then, P normalizes Q.[9] Yet, $Q \trianglelefteq \mathcal{N}_G(Q) \leq G$. Furthermore, Q is a p-Sylow subgroup in $\mathcal{N}_G(Q)$. Well, Sylow II tells us that if Q is a normal p-Sylow subgroup, then it is the *only* p-Sylow subgroup in $\mathcal{N}_G(Q)$. Thus, $P = Q$.[10] □

9: That is, $P \leq \mathcal{N}_G(Q)$.

10: See Rezk's notes for an outer automorphism of S_6.

3.2 Ascending Chain Condition

We now begin our discussion of *finitely generated* groups.

Definition 3.2.1 (Finitely Generated) *A group G is finitely generated if there exists a finite subset $S \subseteq G$ such that $G = \langle S \rangle$.*

We can make some observations about finite generation:

- $|G| < \infty$ implies G is finitely generated.
- $|S| < \infty$ implies the free group $F(S)$ is finitely generated.[11]
- $G \simeq H$ implies G is finitely generated if and only if H is finitely generated.
- G being finitely generated and $N \trianglelefteq G$ implies G/N is finitely generated.[12]

11: This is clear from the reduced word construction of $F(S)$.

12: If $G = \langle S \rangle$, then $G/N = \langle \overline{S} \rangle$, and we have the canonical map $\pi : G \twoheadrightarrow G/N$, where $\overline{S} = \pi(S)$.

Remark 3.2.1 Note that there is absolutely *no reason* for subgroups to preserve this property, generally. Keep this in mind; it is a common pitfall students make when studying finitely generated groups.

Proposition 3.2.1 *If S is a set and $G = F(S)$ is the free group on S, then G is finitely generated if and only if $|S| < \infty$.*

Proof. We have that $|S| < \infty$ implies $F(S)$ is finitely generated.[13] Conversely, we claim that if $F(S) = \langle T \rangle$ for some $T \subseteq F(S)$, $|T| < \infty$, and then $|S| < \infty$. We can write

$$T = \{x_1, \ldots, x_n\} \subseteq F(S),$$

where each x_k is a reduced word in symbols on S. If $S_k \subseteq S$ is the finitely subset of symbols such that x_k is a reduced word in S_k, then let

$$S' := \bigcup_{k=1}^{n} S_k \subseteq S, |S'| < \infty.$$

13: This is easy: take $F(S) = \langle S \rangle$.

We have that $F(S) = \langle T \rangle = \langle S' \rangle$. Therefore, $S = S'$ is finite. $\square$

Example 3.2.1 Consider $G := F(a, b)$, the free group on 2 elements. Write $x_n := a^n b a a^{-n} \in G$, for any $n \in \mathbb{Z}$. Let $H := \langle x_n, n \in \mathbb{Z} \rangle \subseteq G$. We claim that H is *not* finitely generated.

Proof. Let S be the set of symbols $\{X_n, n \in \mathbb{Z}\}$. Define a homomorphism[14]

$$\begin{aligned} F(S) &\xrightarrow{\varphi} G \\ X_n &\longmapsto x_n = a^n b^{a-n}. \end{aligned}$$

14: Remember, it is easy to build homomorphisms out of free groups.

Note that $\varphi(F(S)) = H$, meaning we have a surjective homomorphism $\varphi : F(S) \twoheadrightarrow H$, and we claim that $\varphi : F(S) \xrightarrow{\sim} H$. By the proposition, H cannot be finitely generated. Why is φ injective? A typical element w in $F(S)$ can be written as

$$w := X_{k_1}^{c_1} X_{k_2}^{c_2} \cdots X_{k_r}^{c_r} \text{ with } r \geq 0, k_i \in \mathbb{Z}, c_i \in \{\pm 1\},$$

so that if $k_i = k_{i+1}$, then $c_i = c_{i+1}$.[15] We compute

15: This condition is what makes it a reduced word. Note that this is a *unique* expression.

$$\varphi(w) = a^{k_1} b^{c_1} a^{-k_1} \cdot a^{k_2} b^{c_2} a^{-k_2} \cdot \cdots \cdot a^{k_{r-1}} b^{c_{r-1}} a^{-k_{r-1}} a^{k_r} b^{c_r} a^{-k_r}.$$

The question is: is this e? Cancellation can occur only if $k_i = k_{i+1}$ and $c_i = -c_{i+1}$. However, this cannot happen, so if $\varphi(w) = e$, then $w = ()$.[16]

16: Thus, the kernel is trivial, meaning φ is an injection.

$\square$

Remark 3.2.2 Without proof, we note that every subgroup of a free group is a free group.

Now, moving towards the *ascending chain condition*, let $(P, \leq)$ be a poset.

Definition 3.2.2 (Ascending Chain Condition) *We say that $(P, \leq)$ has the ascending chain condition (ACC) if for every $\mathbb{Z}_+$-indexed sequence $\{x_k \in P\}_{k=1}^{\infty}$ such that $x_k \leq x_{k+1}$ for all $k \in \mathbb{Z}_+$, then there exists an $N \in \mathbb{Z}_+$ such that $x_k = x_N$ for all $k \geq N$.*

Equivalently, $(P, \leq)$ does *not* have the ACC if there exists a sequence in P of the form

$$x_1 < x_2 < x_3 < \cdots \rightsquigarrow \{x_k \in P\}_{k \in \mathbb{Z}_+},$$

where $x_k < x_{k+1}$ for all k.

Definition 3.2.3 (ACC for Subgroups) *A group G has the ACC for subgroups if* $(\mathrm{Subgroups}(G), \leq)$ *has the ACC.*

Proposition 3.2.2 *Let G be a group. Then, the following are equivalent:*

(i) G has ACC for subgroups.
(ii) Every subgroup of G is finitely generated.

Proof. We start with (i) $\Rightarrow$ (ii). We will show that $\neg$(ii) $\Rightarrow$ $\neg$(i).[17] If G' is not finitely generated, then we can choose a sequence of elements $x_k \in G'$, $k \in \mathbb{Z}_+$, such that

$$x_k \in G' \setminus \langle x_1, \ldots, x_{k-1} \rangle .$$

Let $H_k := \langle x_1, \ldots, x_k \rangle \subseteq G' \leq G$; i.e.,

$$H_1 < H_2 < H_3 < \cdots \leq G,$$

so we are done. Now, conversely, suppose every subgroup of G is finitely generated. Consider an ascending chain

$$H_1 \leq H_2 \leq H_3 \leq \cdots \leq G.$$

Let $H := \bigcup_{k=1}^{\infty} H_k$. Then, $H \leq G$. By hypothesis, H is finitely generated, so $H = \langle y_1, \ldots, y_m \rangle$, and each $y_i \in H_{k_i}$ for some k_i. Now, defining $k := \max(k_1, \ldots, k_i)$ implies $\{y_1, \ldots, y_m\} \subseteq H_k$. Thus, $H \subseteq H_k \subseteq H$, meaning $H_k = H$.[18] □

17: That is, every subgroup is not finitely generated, then ACC fails.

18: As such, G has the ACC for subgroups.

Proposition 3.2.3 *Let $N \trianglelefteq G$. The following are equivalent:*

(i) G has the ACC for subgroups.
(ii) Both N and G/N have the ACC for subgroups.

Proof. Start with (i) $\Rightarrow$ (ii). Suppose G has the ACC for subgroups. Then, it is immediate that N does too. Suppose

$$\overline{H}_1 \leq \overline{H}_2 \leq \cdots \leq G/N.$$

We have the quotient homomorphism $\pi : G \twoheadrightarrow G/N$. Let

$$H_k := \pi^{-1}(\overline{H}_k),$$

so via the ACC, there exists an N such that $H_k = H_N$ for all $k \geq N$. Well, then $\pi(H_k) = \pi(H_N)$, and so the $\overline{H}_k$ stabilize. Conversely, consider a chain

$$H_1 \leq H_2 \leq \cdots \leq G.$$

Then, we get a new chain

$$H_1 \cap N \leq H_2 \cap N \leq \cdots \leq N,$$

and

$$H_1 N/N \leq H_2 N/N \leq \cdots \leq G/N,$$

where $H_k N/N = \pi(H_k)$. By hypothesis, there exists an n for all $k \geq n$, $H_k \cap N = H_n \cap N$ and $H_k N/N = H_n N/N$. Therefore, $H_k = H_n$ for all $k \geq n$.[19] □

19: Suppose $x \in H_k$. Then, $xN \in H_k N/N = H_n N/N$, so $xN \in H_n N$. Thus, there exists $k \in N$ such that $xn \in H_n$. We have that $x = yk^{-1}$, $y \in H_n$, so

$$y^{-1}x = n^{-1} \in H_k \cap N = H_n \cap N.$$

Theorem 3.2.4 *Every subgroup of a finitely generated abelian group is finitely generated.*

Proof. Suppose G is an abelian group which has a generated set of size n. We proceed by induction on n that G has the ACC for subgroups. In the $n = 0$ case, $G = \{e\}$. Now, for a proper base case $n = 1$, we have $G = \langle x \rangle$.

Since subgroups of cyclic groups are cyclic, the base case holds. Now, for $n \geq 2$,

$$G = \langle x_1, x_2, \ldots, x_n \rangle .$$

Let $H = \langle x_1, \ldots, x_{n-1} \rangle$, and by induction, H has the ACC for subgroups. Well, $G/H = \langle \overline{x}_n \rangle$,[20] so it has the ACC for subgroups, meaning G has the ACC for subgroups.[21] □

20: Since G is abelian, $H \trianglelefteq G$.

21: Thus, by the equivalence, every subgroup of G is finitely generated.

3.3 Torsion and Products

Hereafter, assume G is abelian.

Definition 3.3.1 (Torsion) *An element $a \in G$ is torsion if $|a| < \infty$. We write*

$$G_{tors} := \{a \in G : |a| < \infty\}$$

for the set of torsion elements.

Proposition 3.3.1 *Since G is abelian, $G_{tors} \leq G$ is a subgroup.*[22]

22: This is easy, but we *need* G to be abelian.

Definition 3.3.2 (Torsion Group) *We say that a group G is a torsion group if it is abelian and $G_{tors} = G$.*

Example 3.3.1 For instance, $C_{m_1} \times \cdots \times c_{m_r}$. In fact, any finite abelian group is torsion.

Example 3.3.2 Take the group $G := (\mathbb{Q}/\mathbb{Z}, +)$. This group is countably infinite and abelian. However, it is a torsion group. Every element

$$x = \frac{a}{b} + \mathbb{Z} \in G,$$

and take the "bth power" yields

$$bx = b\left(\frac{a}{b} + \mathbb{Z}\right) = a + \mathbb{Z} = 0 + \mathbb{Z},$$

which means $|x|$ divides b.

Definition 3.3.3 (Torsion Free) *An abelian group G is torsion free if its torsion group is trivial: $G_{tors} = \{e\}$.*

Proposition 3.3.2 *If G is abelian, then G/G_{tors} is torsion free.*

Proof. Suppose $\overline{x} \in G/G_{\text{tors}}$, where $|\overline{x}| = n < \infty$. Let $x \in G$ such that $\pi(x) = \overline{x}$. Well, $x^n \in G_{\text{tors}}$, so $|x^n| = m$ for some $m < \infty$, which means $x^{mn} = e$. Thus, $x \in G_{\text{tors}}$, meaning $\overline{x} = \overline{e}$.[23] □

23: If you kill the torsion elements, the elements that are left are torsion free.

Proposition 3.3.3 *If G is abelian, finitely generated, and torsion, then G is finite.*

Proof. Suppose $G = \langle a_1, \dots, a_n \rangle$, where $|a_i| = m_i < \infty$. Since G is abelian, every $x \in G$ can be written as

$$x = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$$

for some $k_i \in \mathbb{Z}$, where $k_i \in \{0, 1, \dots, m_i\}$. Thus, $|G| \leq m_1 m_2 \cdots m_k$. □

Corollary 3.3.4 *Both $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}$ are not finitely generated.*[24]

24: Recall that finite generatoin is preserved by taking quotients.

Definition 3.3.4 (Direct Product) *We define the direct product*

$$G = G_1 \times \cdots \times G_n := \{(g_1, \dots, g_n) : g_i \in G_i\}.$$

Definition 3.3.5 (Projection Homomorphism) *We get the projection homomorphism*

$$\pi_k : G \to G_k,$$

where

$$\pi_k : (g_1, \dots, g_n) \mapsto g_k.$$

Proposition 3.3.5 *For any group H and product $G := G_1, \times \cdots \times G_n$, then there is a bijection*

$$\mathrm{Hom}(H, G) \xrightarrow{\sim} \mathrm{Hom}(H, G_1) \times \cdot \times \mathrm{Hom}(H, G_n),$$

where $\varphi : H \to G$ becomes $(\varphi_1, \dots, \varphi_n)$, taking $\varphi_k := \pi_k \circ \varphi : G \to G_k$, and we also get

$$\varphi(h) = (\varphi_1(h), \dots, \varphi_n(h)).$$

Remark 3.3.1 (Free/Co Product) Given $G_1, \dots, G_n$, there exists a group[25]

$$G' := G_1 * \cdots * G_n$$

called the coproduct, such that

$$\mathrm{Hom}(G', H) = \mathrm{Hom}(G_1, H) \times \cdots \times \mathrm{Hom}(G_n, H).$$

25: We will not constrct this here, but the construction parallels that of the free group.

Example 3.3.3 We have that $V_4 = C_2 \times C_2$, the Klein 4-group.

Remark 3.3.2 We can regard G_k as a subgroup of $G := G_1 \times \cdots \times G_n$. For specifically, we have an injective homomorphism

$$G_k \xrightarrow{\iota_k} G,$$

where
$$\iota_k : x \mapsto (e, \dots, x, e).$$

We have $\widetilde{G_k} := \iota_k(G_k) \trianglelefteq G$.

Theorem 3.3.6 *Let G be a group with normal subgroups $G_1, \dots, G_N \trianglelefteq G$ such that*

(i) $G_1 G_2 \cdots G_n = G$.
(ii) $G_k \cap (G_1 G_2 \cdots G_{k-1}) = \{e\}$ *for all* $k \in \{2, \dots, n\}$. *Then,*

$$\begin{aligned} G_1 \times G_2 \times \cdots G_n &\xrightarrow{\varphi} G \\ (g_1, g_2, \dots, g_n) &\longmapsto g_1 g_2 \cdots g_n \end{aligned}$$

is an isomorphism of groups.

Sketch of Proof. We have $G_i, G_j \trianglelefteq G$. We claim that if $G_i \cap G_j = \{e\}$, then for all $x \in G_i$ and $y \in G_j$, we have $xy = yx$.[26] Well, (ii) inplies if $i > j$, then
$$G_i \cap (G_1 G_2 \cdots G_{i-1}) = \{e\},$$
and we use this to prove φ is a homomorphism. Note that we *need* the second property for injectivity. □

26: We can write
$$xyx^{-1}y^{-1} = (xyx^{-1})y \in G_j G_j.$$
On the other hand,
$$xyx^{-1}y^{-1} = x(y^{-1}x^{-1}y) \in G_i G_i.$$
Thus, the commutator is in the intersection, so it is trivial, giving us the result.

Proposition 3.3.7 *Let $G = G_1 \times \cdots \times G_k$. Let $g \in G$. Then,*
$$|g| = \operatorname{lcm}(|g_1|, \dots, |g_k|),$$
or ∞ if any $|g_i| = \infty$.

Proof. We have the formula
$$g^n = (g_1^n, g_2^n, \dots, g_k^n),$$
so $g^n = e_G$ if and only if $g_i^n = e_{G_i}$ for $i \in [k]$. In other words, the order of G_i divides n for all $i \in [n]$.[27] □

27: By definition, the smallest of these is the lcm.

Proposition 3.3.8 *Let*
$$G := C_{m_1} \times C_{m_2} \times \cdots \times C_{m_k},$$
where $C_{m_i} := \langle x_i \,|\, x_i^{m_i} \rangle$. Then, if
$$x = x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k}, a_i \in \mathbb{Z},$$
then
$$|x| = \operatorname{lcm}\left(\frac{m_1}{d_1}, \frac{m_2}{d_2}, \dots, \frac{m_k}{d_k},\right)$$
where $d_i := \gcd(m_i, a_i)$.

Corollary 3.3.9 *If* $m = m_1 m_2 \cdots m_k$, *then*

$$C_{m_1} \times \cdots \times C_{m_k} \simeq C_m,$$

if and only if $\gcd(m_i, m_j) = 1$ *for all* $i \neq j$.

We have a nice consequence. If

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i are distinct primes, then[28]

$$C_m \simeq C_{p_1^{e_1}} \times C_{p_2^{e_2}} \times \cdots \times C_{p_k^{e_k}}.$$

28: We call the decomposition the *primary decomposition*.

Remark 3.3.3 We have a classification of finitely generated abelian groups, which states that all such groups are isomorphic to a finite product of cyclic groups.[29]

29: This is nontrivial, and we will discuss it later when we have developed more structural tools.

3.4 Extensions and Semidirect Products

Let H, K, G be groups.

Definition 3.4.1 (Group Extension) *We say* G *is an extension*[30] *of* K *by* H *if there exists* $H' \trianglelefteq G$ *such that* $H' \simeq H$ *and* $G/H' \simeq K$.

30: Dummit and Foote do not use this language, but it is common in the literature.

Definition 3.4.2 (Split Extension) *A split extension is an extension, as above, if there exists* $K' \leq G$ *so that*

$$K' \xhookrightarrow{\iota} G \xrightarrow{\pi} G/H' \simeq K$$

is an isomorphism: $K' \simeq G/H$.

We have an alternate formulation of extensions. We have a homomorphism

$$H \overset{j}{\rightarrowtail} G \overset{p}{\twoheadrightarrow} K$$

Figure 3.1: This sort of thing is called a *short exact sequence* of groups.

such that j is injective, p is surjective, and $\ker p = j(H)$.[31]

31: Note: $H' = j(H)$ and $G/H' \xrightarrow{\sim} K$.

Remark 3.4.1 (Extension Problem) Given H, K, find all groups G which is an extension of K by H. This is hard, but we can give such a classification by group cohomology.

Example 3.4.1 If $G := H \times K$, then we have the trivial extension of K by H, where $H' := H \times \{e\}$. Then, the projection map $\pi : G/H' \xrightarrow{\sim} K$ via $(h, k) \mapsto k$. Alternatively, we also have a trivial extension of H by K.

Trivial extensions are *always* split.

Example 3.4.2 Consider $H = K = C_2$. Let $G_1 := C_2 \times C_2 = H \times K$, which is the trivial extension of K by H. Let $G_2 := C_4 = \langle a | a^4 \rangle$. Then, $H = \langle a^2 \rangle$, and $G/H \simeq \langle a | a^2 \rangle = K$.[32]

32: The latter extension G_2 is *not* split.

Example 3.4.3 Let $H := C_3$ and $K := C_2$. We have one extension

$$G_1 := C_6 := \langle a | a^6 \rangle,$$

and we have $H = \langle a^2 \rangle \simeq C_3$, so the quotient gives us $G/H = \langle a | a^2 \rangle \simeq C_2$. Let $K' := \langle x^3 \rangle$. Then, $K' \xrightarrow{\sim} C_6/\langle a^2 \rangle$.[33] Now, let $G_2 = S_3 \simeq D_6$. Then, $H = \langle r \rangle \simeq C_3$ and $G_2/H \simeq C_2$. This is a split extension. For instance, take $K' = \langle s \rangle, \langle sr \rangle, \langle sr^2 \rangle$.

33: Thus, G_1 is a split exttension. In fact, since $C_6 \simeq C_3 \times C_2$, so it is a trivial extension.

Example 3.4.4 Similarly, let us write $H = c_2$ and $K = C_3$. We still have a trivial extension of $G_1 \simeq C_2 \times C_3 \simeq C_6$.[34]

34: It turns out this is the *only* extension of C_3 by C_2.

It turns out, split extensions correspond *exactly* to *semidirect* products.

Theorem 3.4.1 *To identify G as a split extension, it is enough to find subgroups $H, K \leq G$ such that*[35]

(i) $H \trianglelefteq G$.
(ii) $G = HK$.
(iii) $H \cap K = \{e\}$.

35: This is an equivalency.

Proof. Condition (i) gives us $\pi(K) := kH$, taking the $K \to G \to G/H$ short exact sequence, as before. Thus, $\ker \pi = H \cap K$. Finally, π is surejctive if and only if $G = KH$.[36] □

36: That is, the second two conditions force π to be an isomorphism.

In particular, every $g \in G$ can be written uniquely as $g = hk$ for unique $H \in H$ and $K \in K$. That is, there is a bijection $G \xrightarrow{\sim} H \times K$ where $hk \mapsto (h, k)$.

Remark 3.4.2 We get a homomorphism

$$\begin{aligned} K &\xrightarrow{\alpha} \mathrm{Aut}(H) \\ k &\longmapsto \alpha_k \end{aligned}$$

defined by $\alpha_k(h) := khk^{-1} \in H$.[37]

37: That is,

$$\alpha_k = \mathrm{conj}_k \big|_H \in \mathrm{Aut}(H).$$

Remark 3.4.3 We can reconstruct the group structure on G from H, K, α.

Let $g_1 = h_1k_1, g_2 = h_2k_2 \in G$, where $h_i \in H$ and $k_i \in K$. Well,

$$\begin{aligned} g_1g_2 &= h_1k_1 \cdot h_2k_2 \\ &= h_1k_1h_2k_1^{-1}k_1k_2 \\ &= h_1 \cdot \alpha_{k_1}(h_2) \cdot k_1k_2 \\ &= h \cdot k, \end{aligned}$$

where $h = h_1\alpha_{k_1}(h_2) \in H$ and $k = k_1k_2 \in K$.[38]

38: We can actually proceed in reverse. Proving the construction is *exceptionally* tedious. At least, as an exercise, check that G is a group as defined.

Theorem 3.4.2 *Given groups H, K and $\alpha \in \mathrm{Hom}_{\mathsf{Grp}}(K, \mathrm{Aut}(H))$. Let $H := H \times K$ as a set. Define a product on G by*

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1\alpha_{k_1}(h_2), k_1k_2).$$

Then,

(i) G is a group with identity (e, e) and inverse

$$(h, k)^{-1} = (\alpha_{k^{-1}}(h^{-1}), k^{-1}).$$

(ii) G is a split extension of K by H with

$$H \xrightarrow{\sim} H' := \{(h, e) : h \in H\} \leq G$$

and

$$K \xrightarrow{\sim} K' := \{(e, k) : k \in K\} \leq G.$$

We have $H' \trianglelefteq G$, $H' \cap K' = \{e\}$, $G = H'K'$, and for $h \in H'$ and $k \in K'$, we have $khk^{-1} = \alpha_k(h)$.

Definition 3.4.3 (Semidirect Product) *We call $(G, \cdot)$, as above, the semidirect product of H and K using α, and we write*[39]

$$G = H \rtimes_\alpha K.$$

Every split extension of K by H arises as a semidirect product.

39: Dummit and Foote do not include α in the notation, which makes no sense.

Exercise 3.4.1 If $\alpha(K) = \{\mathrm{id}\} \subseteq \mathrm{Aut}(H)$, then $H \rtimes_\alpha K = H \times K$.

Example 3.4.5 (Infinite Dihedral Group) let $H := F(a) = \langle a | \rangle \simeq C_\infty$. let $K := \langle b | b^2 \rangle \simeq C_2$. Define

$$\alpha : K \to \mathrm{Aut}(H) = \{\mathrm{id}, \mathrm{inv}\}$$

by $\alpha(b) = \mathrm{inv}$. Then, considering $G = H \times K$ as a set is

$$\{a^n e_k : n \in \mathbb{Z}\} \quad \text{or} \quad \{a^n b : n \in \mathbb{Z}\}$$

Then if $\alpha_b = \mathrm{inv}$, we have $\alpha_b(a) = a^{-1}$. Thus, there is a presentation

$$G \simeq \langle a, b | b^2, bab^{-1}a \rangle \simeq D_\infty.$$

Example 3.4.6 Note that we have $D_{2n} \simeq C_n \rtimes_\alpha C_2$, where we have

$$C_2 \to \mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

If you chase through the definition, we have $C_n := \langle r | r^n \rangle$ and $K := \langle s | s^2 \rangle$, where we have $\alpha : s \mapsto (r \mapsto r^{-1})$.

Example 3.4.7 Let $G = C_8 \rtimes_\alpha C_2$. We could have

$$\alpha : C_2 \to \mathrm{Aut}(C_8) \simeq (\mathbb{Z}/8\mathbb{Z})^\times.$$

There are *four different* semidirect products here.

Example 3.4.8 (Groups of Order 30) We have that $G \simeq N \rtimes_\alpha H$ for some $\alpha : C_2 \to \mathrm{Aut}(C_{15})$.[40] Let us present $H = \langle a | a^2 \rangle$ and $N = \langle b | b^{15} \rangle$. Since $\mathrm{Aut}(C_{15}) \simeq (\mathbb{Z}/15\mathbb{Z})^\times$, we know this group is of order eight. We have four different αs:[41]

$$\alpha_a : b \mapsto b, b^4, b^{-4}, b^{-1}.$$

For each of these, we can deduce a presentation:[42]

$$\begin{aligned} G_1 &= \langle a, b | a^2, b^{15}, aba^{-1} = b \rangle \simeq C_{30} \\ G_2 &= \langle a, b | a^2, b^{15}, aba^{-1} = b^4 \rangle \\ G_3 &= \langle a, b | a^2, b^{15}, aba^{-1} = b^{-4} \rangle \\ G_4 &= \langle a, b | a^2, b^{15}, aba^{-1} = b^{-1} \rangle \simeq D_{30}. \end{aligned}$$

Well, for G_4, the conjugacy classes are

$$\{e\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \ldots, \{b^7, b^{-7}\}$$

and

$$\{a, ab^{-2}, ab^{-4}, ab^{-6}, \ldots, ab^{-1}, \ldots\}.$$

On the other hand, for G_2,

$$\{e\}, \{b, b^4\}, \{b^2, b^8\}.\{b^3, b^{12}\}, \{b^5\}, \{b^6, b^9\}, \{b^{10}\}, \{b^{11}, b^{14}\}, \{b^7, b^{13}\}$$

Interestingly, $\mathfrak{X}(G_2) = \{e, b^5, b^{10}\}$.[43] For the as, we get

$$\{a, ab^3, ab^6, ab^9, ab^{12}\}, \{ab, ab^4, ab^7, ab^{10}, ab^{13}\},$$

$$\{ab^2, ab^{15}, ab^8, ab^{11}, ab^{14}\}.$$

The hard question is to determine whether $G_2 \simeq G_3$. In G_3, we have $ab = b^{-4}a$ and $ba = ab^{-4}$. Then, $bab^{-1} = ab^{-5}$, so we get a class

$$\mathrm{Cl}(a) = \{ab^{-5}, ab^{-10}, a\}.$$

It *looks like* these conjugacy classes are of size three. Then, note that

$$\mathrm{Cl}(b^3) = \{b^3, ab^3a^{-1} = b^{-12} = b^3\},$$

so $\mathfrak{X}(G_3) = \langle b^3 \rangle$. Thus, $G_2 \not\simeq G_3$.[44]

40: We use what we have learned about groups of order 30 from the Sylow theorems.

41: Note that there is an isomorphism of rings $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, so their groups of units is isomorphic to $C_2 \times C_4$.

42: We can try to use conjugacy classes to distinguish these groups.

43: Note that

$$bab^{-1} = ab^4b^{-1} = ab^3,$$
$$b(ab^i)b^{-1} = ab^{i+3}.$$

44: Thus, there are four distinct groups of order 30 up to isomorphism, and they are all semidirect products $C_{15} \rtimes C_2$, distinguished by their centers.

On the Theories of Rings and Modules

Ring Structure 4

Now, we need to distinguish between the standard definitions of rings, those having unity and not. To avoid a clash with Dummit and Foote, who take the classical approach, we define rings to *not inherently* have unity.

4.1 Basic Definitions

Definition 4.1.1 (Ring) *A ring is a triple $(R, +, \cdot)$ such that $(R, +)$ is an additive group, $\cdot : R^2 \to R$ is associative, and multiplication distributes over addition from either side.*

Definition 4.1.2 (Ring With Unity) *A ring with unity is a ring R with $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.*

Definition 4.1.3 (Commutative Ring) *A commutative ring R has $a \cdot b = b \cdot a$ for all $a, b \in R$.*

Proposition 4.1.1 (Easy Facts) *We have some easy facts about rings.*[1]

(i) $a \cdot 0 = 0 = 0 \cdot a$.
(ii) $(-a)b = -(ab) = a(-b)$.
(iii) $(-a)(-b) = ab$.
(iv) *If $1 \in R$, it is unique, and*

$$(-1)a = -a = a(-1).$$

1: If you do not know how to prove these immediately, sit down and do them. They are easy exercises.

Example 4.1.1 (Trivial Ring) The best ring is $R := \{0\}$, which is commutative and unital.[2]

2: This is the *only* ring in which $1 = 0$. You will find that some people disallow such a ring. This is stupid. We need the zero ring if we use categories.

Definition 4.1.4 (Unit) *Let $1 \in R$. A unit is an element in $a \in R$ such that there exists $b \in R$ so that $ab = 1 = ba$, and $a^{-1} = b$.*[3]

3: Such an inverse b is unique.

Definition 4.1.5 (Group of Units) *We write*

$$R^\times := \{a \in R : a \text{ is a unit}\}.$$

We have that $R^\times$ is a group under multiplication, which is a quick proof.

Example 4.1.2 (Matrix Ring) Say R is a ring and $n \geq 1$. Let $S := \mathbb{M}_n(R)$. Then, S is a ring via the matrix operations. The corresponding group of units, $S^\times =: \mathrm{GL}_n(R)$, the group of invertible $n \times n$ matrices over R.[4]

4: Assume $1 \in R$.

Definition 4.1.6 (Zero Divisor) *An element $0 \neq a \in R$ is a zero divisor if there exists $b \in R$ such that $ab = 0$ or $ba = 0$.*

Definition 4.1.7 (Non Zero Divisor) *We say $0 \neq a \in R$ is a non zero divisor (or cancellable) if it is not a zero divisor.*[5]

5: That is, for any $b \in R$, either $ab = 0$ or $ba = 0$ imply $b = 0$.

Definition 4.1.8 (Integral Domain) *An integral domain (or, simply domain) is a commutative ring with 1 such that $1 \neq 0$ and $ab = 0$ implies either $a = 0$ or $b = 0$, for all $a, b \in R$.*[6]

6: It has no zero divisors.

Proposition 4.1.2 *If R is commutative and unital, then R is a domain if and only if $(R \setminus \{0\}, \cdot)$ is a monoid.*

That is, for all $r \in R \setminus \{0\}$ and $1 \neq 0$, $x \mapsto rx$ is an *injection*.

Definition 4.1.9 (Field) *A field is a commutative, unital ring such that $1 \neq 0$ and for all $0 \neq a \in R$, the element a is a unit.*

In this case, for all $r \in R \setminus \{0\}$ and $1 \neq 0$, $x \mapsto rx$ is a *bijection*.

Proposition 4.1.3 *We have that a commutative, unital ring R is a field if and only if $(R \setminus \{0\}, \cdot)$ is a group.*

Example 4.1.3 (Fields) We have the usual examples $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_p$.

Proposition 4.1.4 *Every finite domain is a field.*[7]

7: Injective for a finite set implies bijective.

Definition 4.1.10 (Division Ring) *A division ring (or skew field) is a unital ring R such that every $r \in R \setminus \{0\}$ is a unit, and $1 \neq 0$.*[8]

8: Division rings are precisely "noncommutative" fields.

Definition 4.1.11 (Subring) *A subring of a ring R is a subset $S \subseteq R$ which inherits a ring structure from R.*[9]

9: In other words, S is closed under $+$, $\cdot$, and with those operations $(S, +, \cdot)$ is a ring.

Remark 4.1.1 (Subring Equivalent Definition) A subset $S \subseteq R$ is a subring if

(i) $(S, +) \leq (R, +)$.
(ii) S is closed under multiplication.

Example 4.1.4 Let $R := \mathbb{M}_2(\mathbb{R}) \ni 1$, but

$$S := \left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \in R \right\},$$

is a subring, yet $1_S \neq 1$.

Now, when we talk about unital rings, we usually want its subrings to have the same 1. In practice, when people are discussing rings with unity, they are considering the case where the subrings inherit the identity.[10]

10: The issue is that Dummit and Foote do not define subring this way.

Example 4.1.5 Let $R := \mathbb{Z}$. We have that $S = 2\mathbb{Z}$ is a subring, but $1 \notin S$

Example 4.1.6 There are some classic examples of rings.

(a) $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$
(b) The *quaternions*

$$\mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\},$$

where i, j, k are symbols which satisfy[11]

$$i^2 = j^2 = k^2 = -1$$

11: Here, $ij = k = -ji$, $jk = i = -ki$, and $ki = j = -ik$. We know $\mathbb{H}$ is a divison ring. What is the formula for inverses? Well, the conjugate

$$\overline{x} := a - bi - cj - dk,$$

and

$$x\overline{x} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R},$$

so we can divide by it. Thus,

$$x^{-1} = \frac{\overline{x}}{x\overline{x}}.$$

(c) *Function rings*

$$\mathfrak{F}(X, R) = \{f : X \to R \text{ functions}\},$$

where

$$(f + g)(x) = f(x) + g(x)$$

and

$$(fg)(x) = f(x)g(x),$$

taking X to be a set and R to be a ring
(d) Given a ring R, S, the *product ring* $R \times S$ has component-wise operations.

4.2 Quadratic Integer Rings

Take D to be a square-free integer.[12] Define a subring $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$ which can be written as the set

12: That is, it is nonzero and has no repeated prime factor.

$$\{a + b\sqrt{D} : a, b \in \mathbb{Q}\}.$$

We actually have that $\mathbb{Q}(\sqrt{D})$ is a *field*. Well,

$$(a + b\sqrt{D})^{-1} = \frac{a}{a^2 - b^2 D} + \frac{-b}{a^2 - b^2 D}\sqrt{D}.$$

If $a^2 - b^2 D = 0$, then $D = (a/b)^2$, which is impossible if $a, b \in \mathbb{Q}$, because D is square-free.[13] Now, let $\mathbb{Z}[\sqrt{D}]$ be the integral coefficient subset of $\mathbb{Q}(\sqrt{D})$. It is a subring. In fact, it is a domain, inheriting the lack of zero divisors from $\mathbb{C}$. The famous example is the *Gaussian integers* $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{i}]$. If $D \equiv 1 \pmod 4$, then let $\omega = (1 + \sqrt{D})/2 \in \mathbb{C}$. Well, we can always write

13: In fact, if D is square-free, then the expression $a + b\sqrt{D}$ is unique.

$$\omega^2 = \frac{(1 + \sqrt{D})^2}{4} = \frac{1 + 2\sqrt{D} + 1 + 4k}{4},$$

which is just
$$\left(\frac{1}{2}+k\right)+\frac{1}{2}\sqrt{D}=\omega+k.$$

Now, define
$$\mathcal{O}=\mathcal{O}_{\mathbb{Q}(\sqrt{D})}:=\begin{cases}\mathbb{Z}[\sqrt{D}], & D\equiv 2,3 \pmod 4\\ \{a+b\omega : a,b\in\mathbb{Z}\}, & D\equiv 1 \pmod 4).\end{cases}$$

We claim $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a subring of $\mathbb{Q}(\sqrt{D})$.[14] We call this the *ring of integers* inside $\mathbb{Q}(\sqrt{D})$. For instance, when $D=-3$,
$$\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}=\{a+b\omega : a,b\in\mathbb{Z}\},$$
where
$$\omega=\frac{1}{2}+\frac{1}{2}\sqrt{-3}=\frac{1}{2}+\frac{\sqrt{3}}{2}i.$$

This ring is known as the *Eisenstein integers*.[15]

14: Closure under multiplication comes from $\omega^2=\omega+k$.

15: An exercise is to show
$$\mathcal{O}=\left\{\frac{a+b\sqrt{3}i}{2}\right\},$$
where $a,b\in\mathbb{Z}$ and $a\equiv b \pmod 2$.

Proposition 4.2.1 *Let D be square free with $D\equiv 1 \pmod 4$. Then, if $x=a+b\sqrt{D}\in\mathbb{Q}(\sqrt{D})$, then $x\in\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ if and only if $a-b\in\mathbb{Z}$ and $2a\in\mathbb{Z}$.*

Definition 4.2.1 (Norm Map) *We have a norm*
$$\mathbb{Q}(\sqrt{D})\to\mathbb{Q}$$
defined by
$$N(a+b\sqrt{D})=(a+b\sqrt{D})(a-b\sqrt{D})=a^2-b^2D\in\mathbb{Q}.$$

The norm above has the properties $N(\alpha)=0$ if and only if $\alpha=0$, $N(\alpha\beta)=N(\alpha)N(\beta)$, and $\alpha\in\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ implies $N(\alpha)\in\mathbb{Z}$.

Proposition 4.2.2 *An element $\alpha\in\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a unit if and only if $N(\alpha)\in\mathbb{Z}^\times=\{\pm1\}$.*

Proof. Since N is multiplicative and $N(1)=1$, it is easy to see that if $\alpha\in\mathcal{O}^\times$, then $N(\alpha)\in\mathbb{Z}^\times$. Conversely, if $\alpha=a+b\sqrt{D}$ and $N(\alpha)\in\mathbb{Z}^\times$, then $a^2-b^2D=\pm1$. Well, by our formula for reciprocals, $\alpha^{-1}\in\mathcal{O}$. □

Remark 4.2.1 (Pell's Equation) This means $\alpha=x+y\sqrt{D}\in\mathcal{O}^\times$ for $x,y\in\mathbb{Q}$ if and only if $x^2-Dy^2=\pm1$.

Example 4.2.1 Consider the Gaussian integers. Then, $\mathcal{O}=\mathbb{Z}[i]$, so
$$\mathcal{O}^\times=\{a+bi : a,b\in\mathbb{Z},a^2+b^2=1,\}=\{\pm1,\pm i\}\simeq C_4.$$

Example 4.2.2 Consider the Eisenstein integers. It turns out,[16]

$$\mathcal{O}^\times = \{\pm 1, \pm\omega, \pm\omega^2\} \simeq \langle\omega\rangle \simeq C_6.$$

16: Here, ω is a primitive sixth root of unity.

Remark 4.2.2 If D is square-free and $D < 0$, then $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{D})}$ is finite. If $D > 0$, then $\mathcal{O}^\times_{\mathbb{Q}(\sqrt{D})}$ is infinite.

4.3 Monoid and Group Rings

Usually you will hear about "group rings," but it is worth considering a slightly more general object. Let G be a monoid and R be a commutative unital ring.

Definition 4.3.1 (Monoid Ring) *We define the set of formal sums*

$$R[G] := \left\{\sum_{g\in G}^{\text{finite}} a_g[g] : a_g \in R\right\}.$$

This is the monoid ring $R[G]$.[17]

17: Really, an element of $R[G]$ is a tuple of $(a_g)_{g\in G}$, where $a_g \in R$, such that

$$\left|\{g \in G : a_g \neq 0\}\right| < \infty.$$

Then, $[h] = (a_g)$ such that $a_h = 1$ and $a_g = 0$.

Proposition 4.3.1 $R[G]$ *is a ring via the "obvious" formulae:*

$$\sum_g a_g[g] + \sum_g b_g[g] = \sum_g (a_g + b_g)[g]$$

and

$$\left(\sum_{g_1} a_{g_1}[g_1]\right)\left(\sum_{g_2} b_{g_2}[g_2]\right) = \sum_g \left(\sum_{g_1g_2=g} a_{g_1}b_{g_2}\right)[g].$$

The idea is that

$$[g_1][g_2] = [g_1g_2].$$

Proposition 4.3.2 $R[G]$ *is unital, where* $1 = [e]$*, where* $e \in G$ *is the identity.*[18]

18: If G is not commutative, there is no reason to expect $R[G]$ to be, either. If G is a group, then $R[G]$ is called a *group ring*.

Example 4.3.1 If $|G| = n < \infty$, where $G = \{g_1, \ldots, g_n\}$, then

$$R[G] = \left\{\sum_{k=1}^{n} a_k[g_k] : a_k \in R\right\}.$$

Example 4.3.2 Let $G = \{e, g\} \simeq \langle g | g^2\rangle$. Let $R = \mathbb{Q}$. Then,

$$\mathbb{Q}[G] = \{a_0[e] + a_1[g] : a_0, a_1 \in \mathbb{Q}\},$$

where the operations are

$$(a_0[e] + a_1[g]) + (b_0[e] + b_1[g]) = (a_0 + b_0)[e] + (a_1 + b_1)[g]$$

and

$$(a_0[e] + a_1[g])(b_0[e] + b_1[g]) = (a_0b_0 + a_1b_1)[e] + (a_0b_1 + a_1b_0)[g].$$

Since G is abelian, $\mathbb{Q}[G]$ is commutative. Is this a field/domain? No:

$$([e] + [g])([e] - [g]) = 0.$$

Exercise 4.3.1 $\mathbb{Q}[G] \simeq \mathbb{Q} \times \mathbb{Q}$.[19]

19: This is an isomorphism of rings.

Example 4.3.3 (Polynomial Ring) Let $G = \{e, a, a^2, a_3, \dots\} = \{a^n\}_{n \in \mathbb{Z}_{\geq 0}}$. This is a monoid, but not a group.[20] Then, we could form $R[G]$. We will write $x := [a]$, and a short exercise shows us $x^k = [a^k]$. A typical element in $R[G]$ can be seen as

$$\{a_0 + a_1x + \cdots + a_rx^r : g \geq 0, a_i \in R\}.$$

As such, $R[G]$ is the ring of polynomials in one generator x with coefficients in R. Usually, we will write $R[x]$ for this.

20: In particular, it is the *free monoid* on one generator.

4.4 Homomorphisms and Isomorphisms

Let S, R be rings.

Definition 4.4.1 (Ring Homomorphism) *A homomorphism $\varphi : R \to S$ is a function which "preserves all the structure." That is,*

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

and

$$\varphi(ab) = \varphi(a)\varphi(b),$$

for all $a, b \in R$.

Remark 4.4.1 Even if $1_R \in R$ and $1_S \in S$, a homomorphism of rings $\varphi : R \to S$ *might* or *might not* have $\varphi(1_R) = 1_S$.[21]

21: These are the consequences of following Dummit and Foote here.

Example 4.4.1 Let R_1, R_2 be unital rings. Define $S := R_1 \times R_2$, where $1_S = (1_{R_1}, 1_{R_2})$. Now, $\varphi : R_1 \to S$ defined by $\varphi(r) := (r, 0)$ is a ring homomorphism, but $\varphi(1_{R_1}) \neq 1_S$.[22]

22: Check that this is a ring homomorphism. It will be quick.

Definition 4.4.2 (Unit-Preserving Homomorphism) *We will often specify a homomorphism to be unit-preserving, sending* 1 *to* 1.

Definition 4.4.3 (Image) *Given $\varphi : R \to S$, a homomorphism, $\varphi(R) \subseteq S$ is a subring of S.*

Definition 4.4.4 (Kernel) *We have that* $\ker\varphi := \{r \in R : \varphi(r) = 0\}$ *is a subring of* R.[23]

23: Usually this does not contain 1. According to Rezk, this means it *really* is not a ring.

Definition 4.4.5 (Ring Isomorphism) *An isomorphism is a homomorphism* $\varphi : R \to S$ *such that* φ^{-1} *exists.*[24]

24: Isomorphisms of rings certainly have to preserve unity, if it exists.

4.5 Ideals and Quotients

In some sense, ideals are the parallel of normal subgroups in rings. However, there are instances where this inherited intuition fails.

Definition 4.5.1 (Ideal) *Let* R *is a ring and* $I \subseteq R$ *be a subset. Then, if* $r \in R$, *write*

$$rI := \{rx : x \in I\}$$

and

$$Ir := \{xr : x \in I\}.$$

Then, $I \subseteq R$ *is a left ideal if* $I \leq (R, +)$ *and* $rI \subseteq I$ *for all* $r \in R$. *Similarly, a right ideal* $I \leq (R, +)$ *and* $Ir \subseteq I$ *for all* $r \in R$. *Then, a two-sided ideal (or, just ideal) is* $I \subseteq R$ *which is both a left and a right ideal.*

Proposition 4.5.1 *If* R *is commutative, then left ideals are the same as right ideals, so we just call them ideals.*[25]

25: For the moment, only worry about two-sided ideals.

Example 4.5.1 (Unit Ideal) Let $I := R$.

Example 4.5.2 (Trivial Ideal) Let $I := \{0\} \subseteq R$.

Remark 4.5.1 Any ideal is a subring using Dummit and Foote's definition of subring. In particular, if $1 \in R$, then the only ideal $I \subseteq R$ with $1 \in I$ is the unit ideal.

Given $I \subseteq R$ which is a left, right, or two-sided ideal, we can form

$$R/I := \{a + I : a \in R\},$$

where $a + I = \{a + x : x \in I\}$ is a coset of I in the group $(R, +)$. If I is two-sided, then R/I is a ring such that the *quotient map* $\pi : R \to R/I$ is a ring homomorphism.

Definition 4.5.2 (Quotient Ring) *Our ring structure for the quotient ring* R/I *is defined by*

$$(a + I)(b + I) := (ab) + I.$$

Exercise 4.5.1 Show that the operation above makes R/I into a ring if I is two-sided.[26]

26: In particular, we need to show that the operation is "well-defined." This fact *absolutely* uses that I is two-sided.

Remark 4.5.2 Note that π is certainly surjective, by construction, and $\ker\pi = I$. Note further that if $\varphi : R \to S$ is any homomorphism of rings, then $I := \ker\varphi \subseteq R$ is *always* a two-sided ideal.

Lemma 4.5.2 (Homomorphism Theorem) *Let $\varphi : R \to S$ be a homomorphism of rings. Let $I \subseteq R$ be a two-sided ideal. If $I \subseteq \ker\varphi$, then there exists a unique ring homomorphism $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi}(a + I) = \varphi(a)$.*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & S \\ R/I \arrow[ur, dashed, "\exists!"', "\overline{\varphi}"] & \end{tikzcd}$$

Figure 4.1: Diagram of the homomorphism theorem, which holds if $I \leq \ker\varphi$. We omit the proof, since it mirrors the theorem for groups.

Theorem 4.5.3 (First Isomorphism Theorem) *If $\varphi : R \to S$ is a ring homomorphism, then $\ker\varphi$ is an ideal in R, $\varphi(R)$ is a subring of S, and we have an isomorphism of rings*

$$\overline{\varphi} : R/\ker\varphi \xrightarrow{\sim} \varphi(R).$$

$$\begin{tikzcd} R \arrow[rrr, "\varphi"] \arrow[dr, two heads, "\pi"'] & & & S \\ & R/\ker\varphi \arrow[r, "\sim", "\overline{\varphi}"'] & \varphi(R) \arrow[ur, hook, "\iota"'] & \end{tikzcd}$$

Now, let R be a general ring with a subring $A \subseteq R$ and ideal $I \subseteq R$.

Theorem 4.5.4 (Second Isomorphism Theorem) *We have the following:*

(i) *$A + I$ is a subring of R.*
(ii) *I is an ideal in $A + I$.*
(iii) *$A \cap I$ is an ideal in A.*
(iv) *$A/(A \cap I) \simeq (A + I)/I$ is an isomorphism of rings.*[27]

27: In fact, we have the map $x + (A \cap I) \mapsto x + I$.

Proof. Both the first and second isomorphism theorems for rings have proofs akin to the group theorems. Prove them as an exercise. □

$$\begin{tikzcd} & R \arrow[d, dash] & \\ & A + I & \\ A \arrow[ur, dash] & & I \arrow[ul, "\text{ideal}"'] \\ & A \cap I \arrow[ul, "\text{ideal}"] \arrow[ur, dash] & \end{tikzcd}$$

Figure 4.2: Diagram of the second isomorphism theorem

Theorem 4.5.5 (Lattice Isomorphism Theorem) *Let $I \subseteq R$ be an ideal in a ring. Then, there is a bijective correspondence*

$$\begin{Bmatrix} \text{ideals } J \subseteq R \\ \text{st } I \subseteq J \end{Bmatrix} \overset{\sim}{\longleftrightarrow} \begin{Bmatrix} \text{ideals in} \\ R/I \end{Bmatrix}$$
$$J := \pi^{-1}(\overline{J}) \longmapsto \pi(J) \subseteq R/I$$

The opposite map is $\overline{J} \mapsto \pi^{-1}(\overline{J})$.

4.6 Polynomial Rings

Let R be a unital ring. We define the polynomial ring

$$R[x] := \text{ set of formal expressions}$$

$$f = \sum_{k \in \mathbb{Z}_{\geq 0}} a_k x^k,$$

where $a_k \in R$ and *almost all* of the a_k are 0.

Definition 4.6.1 (Degree of Polynomial) *The degree* $\deg f$ *of an* $f \in R[x]$ *is the largest* n *such that* $a_n \neq 0$, *or it is* $-\infty$ *if no such* n *exists. That is,*[28]

$$\deg : R[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}.$$

28: We take $-\infty$ since that is certainly less than $\mathbf{0}$, giving us a nice ordering.

Definition 4.6.2 (Constant Polynomial) *A polynomial* $f \in R[x]$ *is constant if* $\deg f \in \{0, -\infty\}$.

Note that

$$\left\{\begin{matrix}\text{constant}\\ \text{polynomials}\end{matrix}\right\} \xhookrightarrow{\text{subring}} R[x],$$

where we have an isomorphism of the LHS with R, taking $a \mapsto a \cdot x^0$.[29]

29: This is so canonical, that we usually just write $R \subseteq R[x]$.

Proposition 4.6.1 *Let* R *be a domain. Then,*

(i) $f, g \in R[x]$ *implies* $\deg(fg) = \deg(f) + \deg(g)$.[30]
(ii) $(R[x])^\times = R^\times$.
(iii) $R[x]$ *is a domain.*

30: Assume $-\infty + k = -\infty$ for any k.

(i) *Proof.* Let $f = a_m x^m +$ lower deg polynomials, $a_m \neq 0$ and $g = b_n x^n + \cdots$, where $b_n \neq 0$. Then,

$$fg = (a_m b_n) x^{m+n} + \cdots,$$

where $a_m b_n \neq 0$.[31] □

31: We use that R is a domain.

(ii) *Proof.* We know that $\deg 1 = 0$. If $fg = 1$, then $\deg f + \deg g = 0$, so $\deg f = \deg g = 0$, meaning $f, g \in R \subseteq R[x]$. Thus, $R[x]^\times = R^\times$. □

(iii) *Proof.* If $f, g \in R[x]$ and $f, g \neq 0$, then $\deg f, \deg g \in \mathbb{Z}_{\geq 0}$. Then, $\deg fg \in \mathbb{Z}_{\geq 0}$, so $fg \neq 0$. □

Note that given R, we can form

$$R \rightsquigarrow R[x] \rightsquigarrow (R[x])[y] \rightsquigarrow ((R[x])[y])[z] \rightsquigarrow \cdots,$$

so we usually write $(R[x])[y] = R[x, y] \simeq (R[y])[x]$.[32]

32: If R is a domain, so is $R[x_1, x_2, \ldots, x_n]$.

Proposition 4.6.2 (Universal Property of Polynomial Rings) *Let* R, S *be commutative rings with 1. For every* (φ, a), *where* $\varphi : R \to S$ *is a ring homomorphism,* $\varphi(1_R) = 1_S$, *and* $a \in S$, *then there exists a unique ring homomorphism* $\widetilde{\varphi} : R[x] \to S$ *which preserves 1, so that* $\widetilde{\varphi}(r) = \varphi(r)$ *if* $r \in R \subseteq R[x]$, *and* $\widetilde{\varphi}(x) = a$.[33]

33: The universal property is our recipe for forming new ring homomorphisms.

Proof. Given φ, a, define

$$\begin{aligned} R[x] &\xrightarrow{\widetilde{\varphi}} S \\ f = \sum^{\text{finite}} c_k x^k &\longmapsto \sum \varphi(c_k) a^k. \end{aligned}$$

Verify that $\widetilde{\varphi}$ is a ring homomorphism preserving unity. Uniqueness is the observation that the rules $\widetilde{\varphi}$ must satisfy force this formula:

$$\widetilde{\varphi}\left(\sum^{\text{finite}} c_k x^k\right) = \sum \widetilde{\varphi}(c_k x^k) = \sum \widetilde{\varphi}(c_k)\widetilde{\varphi}(x)^k,$$

forcing our formula. □

Consider the special case $S = R$ and $\varphi = \mathrm{id}_R : R \to R$.

Corollary 4.6.3 *Let R be commutative and unital. Let $a \in R$. Then there exists a unique ring homomorphism $\widetilde{\varphi} : R[x] \to R$ such that $\widetilde{\varphi}|_R = \mathrm{id}_R$, where $R \subseteq R[x]$, and $\widetilde{\varphi}(x) = a$. We have the formula*[34]

$$\widetilde{\varphi}\left(\sum c_k x^k\right) = \sum c_k a^k =: f(a).$$

34: This homomorphism of rings is called *evaluation at a*, which is a neat fact: evaluation of a polynomial is a homomorphism. This is nice because $(f+g)(a) = f(a) + f(b)$ and $(fg)(a) = f(a)g(a)$.

Remark 4.6.1 Given R as commutative and unital, we get a function $R[x] \to \mathfrak{F}(R, R)$, where the latter is the set of all functions $R \to R$, which is a ring under pointwise operations. The map is

$$\begin{aligned} R[x] &\xrightarrow{\text{ev}} \mathfrak{F}(R, R) \\ f &\longmapsto (a \mapsto f(a)), \end{aligned}$$

so ev is a ring homomorphism preserving 1.

Observe that $\mathrm{ev} : R[x] \to \mathfrak{F}(R, R)$ can fail to be injective.

Example 4.6.1 Consider $R = \mathbb{Z}/p = \mathbb{F}_p$, where p is a prime. Then, we have $\mathrm{ev} : \mathbb{F}_p[x] \to \mathfrak{F}(\mathbb{F}_p, \mathbb{F}_p)$. Define $f := x^p - x \in \mathbb{F}_p[x]$. Then, $\mathrm{ev}(f) = 0$, because $a^p = a$ for all $a \in \mathbb{F}_p$.[35]

35: We use Fermat's Little Theorem. This is precisely why algebraists do not think of polynomials as functions.

4.7 Particular Ideals and Zorn's Lemma

Given a ring R and a subset $A \subseteq R$, then we can form

$$(A) := \bigcap_{\substack{\text{ideals } I \subseteq R \\ \text{st } A \subseteq I}} I.$$

Note that the intersection of ideals is an ideal, so $(A) \subseteq R$ is the smallest ideal of R which contains the set A. We call (A) the *ideal generated by A*. Notationally, if $A = \{a_1, \ldots, a_n\}$, then $(A) = (a_1, \ldots, a_n)$.[36] Now, define

36: We use parentheses, which is mostly standard. Sometimes you will see $\langle A \rangle$.

$$\begin{aligned} RA &:= \{r_1a_1 + \cdots + r_ka_k : r_i \in R, a_i \in A, k \geq 0\} \\ AR &:= \{a_1r_1 + \cdots + a_kr_k : r_i \in R, a_i \in A, k \geq 0\} \\ RAR &:= \{r_1a_1r_1' + \cdots + r_ka_kr_k' : r_i, r_i' \in R, a_i \in A, k \geq 0\}. \end{aligned}$$

Proposition 4.7.1 *If R is unital, then $(A) = RAR$. If R is commutative and unital, then $(A) = AR = RA$. If $1 \notin R$, then*[37]

$$(A) = \langle A \rangle + RA + AR + RAR.$$

37: We only care about unital rings, so do not worry about this.

Proof. Prove the above as an exercise.[38] □

38: We need to (1) verfiy that RAR is an ideal. Then, (2) show that $A \subseteq J$, which uses that $1 \in R$. Finally, (3) show that if $I \subseteq R$ is an ideal such that $A \subseteq R$, then $J \subseteq I$.

Definition 4.7.1 (Principal Ideal) *We define a principal ideal I to be $I = (a)$, where $a \in R$.*

In a unital ring, we have a formula $I = (a) = RaR$, and if R is commutative, then $I = (a) = Ra$.

Example 4.7.1 Let $R := \mathbb{Z}[x]$, the integral polynomial ring. Define an ideal $I := (2, x) \subseteq \mathbb{Z}[x]$. We claim that I is *not* a principal ideal.

Proof. Recall that

$$I = \{g \cdot 2 + h \cdot x : g, h \in \mathbb{Z}[x]\}.$$

Suppose $I = (p)$ for some $p \in \mathbb{Z}[x]$. Since $2, x \in I$, there exist $f, g \in \mathbb{Z}[x]$ such that $2 = pf$ and $x = pg$. Then, $\deg(2) = \deg(p) + \deg(f)$ and $\deg(x) + \deg(p) + \deg(g)$, meaning $\deg(p) + \deg(f) = 0$ and $\deg(p) + \deg(g) = 1$. Hence, $\deg(p) = \deg(f) = 0$ and $\deg(g) = 1$. That is, $p, f \in \mathbb{Z} \subseteq \mathbb{Z}[x]$; i.e., $2 = pf$ implies $p, f \in \{\pm 1, \pm 2\}$. For instance, if $p = \pm 2$, then $x = \pm 2g = \pm 2(a+bx) - \pm 2a + \pm 2bx$, implying $\pm 2b = 1$.[39] We are left with the case $p = \pm 1$, which give us $I = \mathbb{Z}[x]$. We claim this is not true, either. If $1 \in I$, then $1 = 2m + xn$, where $m, n \in \mathbb{Z}[x] \xrightarrow{\mathrm{ev}_0} \mathbb{Z}$, which sends us to $1 = 2m(0) + 0n(0)$, which is impossible, since $m \in \mathbb{Z}$. □

39: This is a contradiction to $b \in \mathbb{Z}$.

Example 4.7.2 If $R := \mathbb{F}$ is a field, then consider $\mathbb{F}[x, y]$. Then, $I := (x, y) \subseteq \mathbb{F}[x, y]$ is not principal.

Proposition 4.7.2 *Let R be commutative and unital. Then, R is a field if and only if R has exactly two ideals (which necessarily are $R \neq (0)$.)*[40]

40: The wording here cleverly exlcudes the zero ring, which is *not* a field.

Proof. An element $a \in R^\times$ if and only if $(a) = R$. If R is a field, then $1 \neq 0$. If $I \subseteq R$ and $I \neq (0)$, then pick any $a \in I \setminus \{0\}$. Since R is a field, $a \in R^\times$ so $Ra = R \subseteq I$, meaning $I = R$. Conversely, if $R \neq \{0\}$ with only ideals $R, (0)$, then if $a \in R \setminus \{0\}$, then $I = Ra \subseteq R$ is an ideal. We see that $(0) \neq I$, so $I = R$, meaning $a \in R^\times$.[41] □

41: You will hear algebraists call fields the *simplest* kind of ring, since they are sparse in ideals.

Corollary 4.7.3 *Any nonzero $\varphi : \mathbb{F} \to R$ ring homomorphism from a field is injective.*

Proof. If $\ker\varphi \subseteq F$ as an ideal, then $\ker\varphi = (0)$ so φ is injective $\square$

Definition 4.7.2 (Maximal Ideal) *Let R be unital. An ideal $M \subseteq R$ is called maximal if $M \neq R$ and if $M \subseteq N \subseteq R$, where N is an ideal in R, either $N = M$ or $N = R$.*[42]

42: That is, M is maximal among proper ideals.

Proposition 4.7.4 *Let R be commutative and unital. An ideal $M \subseteq R$ is maximal if and only if R/M is a field.*

Proof. Via the lattice isomorphism theorem, we have a correspondence between ideals in R/M and ideals in R which contain M. $\square$

Definition 4.7.3 (Prime Ideal) *Let R be commutative with 1. Then, an ideal $P \subseteq R$ is prime if $P \neq R$ and if $ab \in P$, then either $a \in P$ or $b \in P$.*

Remark 4.7.1 We can restate the definition above as R/P is a monoid under multiplication.

Proposition 4.7.5 *P is a prime ideal if and only if R/P is a domain.*[43]

43: Note that, as a corollary, R is a domain if and only if (0) is prime.

Corollary 4.7.6 *Every maximal ideal is prime.*

Proof. All fields are domains. $\square$

Example 4.7.3 Let $R := \mathbb{Z}$. The only ideals in $\mathbb{Z}$ are of the form (n). We have that (n) is maximal if and only if $n = \pm$ prime. It is prime if and only if $n = \pm$ prime or $n = 0$.

Theorem 4.7.7 (Maximal Ideal Theorem) *Let R be unital. Every proper ideal is contained in some maximal ideal.*[44]

44: In particular, every nonzero unital ring has at least one maximal ideal.

Corollary 4.7.8 *If R is unital and commutative, then $R \neq (0)$ implies there exists a quotient ring which is a field.*

Definition 4.7.4 (Partial Order) *A partial order $\leq$ on X is a relation such that $x \leq x$, $x \leq y$, $y \leq x$ implies $x = y$, and $x \leq y$, $y \leq z$ implies $x \leq z$.*

Definition 4.7.5 (Chain) *In a poset $(X, \leq)$, a chain $C \subseteq X$ is a totally ordered subset.*[45]

45: That is, for all $x, y \in C$, either $x \leq y$ or $y \leq x$.

Definition 4.7.6 (Upper Bound) *For $S \subseteq X$, an upper bound of S is $u \in X$ such that $s \leq u$ for all $s \in S$.*

Definition 4.7.7 (Maximal Element) *A maximal element of X is an element $m \in X$ such that if $m \leq x$, then $m = x$ for all $x \in X$.*[46]

46: In other words, it is maximal among all things it can be compared to.

Lemma 4.7.9 (Zorn's) *Let $(X, \leq)$ be a nonempty poset. If every nonempty chain in X has an upper bound in X, then X has a maximal element.*

Proof. It is equivalent to the axiom choice. We are not studying set theory, so look elsewhere for the proof. □

Lemma 4.7.10 (Zorn's Equivalent) *Let $(X, \leq)$ be a poset. If every chain in X has an upper bound in X then X has a maximal element.*[47]

47: We took out nonempty.

Proof of Maximal Ideal Theorem. Let $1 \in R \supsetneq I$ be an ideal. let

$$X = \{J \subseteq R \text{ ideals } : J \neq R \text{ and } I \subseteq J\}.$$

By Zorn's lemma, X has a maximal element which is the desired thing. Well, $I \in X$, so X is nonempty. Suppose we have a nonempty chain $C \subseteq X$. Let $A = \bigcup_{J \in C} J \subseteq R$. We claim that A is a proper ideal with $I \subseteq A$. Then, $A \in X$ and A is an upper bound of C. Well, $I \subseteq A$ is easy, since $C \neq \varnothing$. Clearly A is an ideal. Now, why is $A \neq R$? If $A = R$,then $1 \in A$, but then $1 \in \bigcup J$, so there exists a $J \in C$ such that $1 \in J$, meaning $J = R$, a contradiction. □

4.8 Rings of Fractions

Dummit and Foote do not give as rigorous of a construction of rings of fractions, at least until far later in the text. Still, it is an important construction. Let R be commutative with 1. Let $D \subseteq R$ be a *multiplicatively closed*[48] subset. We can form a ring

48: By this we mean if $a, b \in D$, then $ab \in D$, and $1 \in D$. That is, D is a submonoid $(D, \cdot) \subseteq (R, \cdot)$.

$$D^{-1}R = \left\{\frac{r}{d} \text{ sort of } : r \in R, d \in D\right\},$$

called the *ring of fractions* of R with respect to D.[49]

49: We will construct this object formally, after discussing some examples.

Definition 4.8.1 (Field of Fractions) *Given a domain R and $D := R \setminus \{0\}$, then $D^{-1}R = \mathrm{Frac}(R)$, the field of fractions of R.*

For instance, the familiar example is $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. You may also see the notation $\mathbb{F}_{\mathbb{Z}}$ or $F_{\mathbb{Z}}$, depending on the context.

Definition 4.8.2 (Field of Rational Functions) *Given a polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$, where $\mathbb{F}$ is a field, we could take $\mathrm{Frac}(\mathbb{F}[x_1, \ldots, x_n])$, which is denoted $\mathbb{F}(x_1, \ldots, x_n)$.*

Example 4.8.1 If $0 \in D$, then $J = R = D^{-1}R = \{0\}$, the trivial ring.

Example 4.8.2 Given an $a \in R$, we could form $D = \{a^k : k \geq 0\}$. We could form $a^{-1}R := D^{-1}R$.

Definition 4.8.3 (Laurent Polynomials) *The Laurent polynomials are denoted*

$$\mathbb{F}[x^{\pm 1}] := x^{-1}(\mathbb{F}[x]).$$

Elements can be uniquely written as

$$\sum_{k=n_0}^{n_1} a_k x^k, \quad n_0 \leq n_1 \in \mathbb{Z}, a_k \in \mathbb{F}.$$

Definition 4.8.4 (Localization) *Given a prime ideal $P \subseteq R$ and $D := R \setminus P$, then $D^{-1}R = R_P$ is called the localization of R with respect to P.*[50]

50: The localization finds extreme importance in *commutative algebra* and *algebraic geometry*.

Example 4.8.3 (p-local Integers) Form the localization

$$\mathbb{Z}_{(p)} \simeq \left\{\frac{a}{b} : p \nmid b\right\} \subseteq \mathbb{Q}.$$

Example 4.8.4 What about in a polynomial ring over a field? Well, we could form the localization $\mathbb{F}[x]_{(x)}$ which is precisely

$$\left\{\frac{f}{g} : \frac{f(0)}{g(0)} \text{ is defined}\right\}.$$

Our goal is to produce a ring homomorphism ψ (preserving unity)

$$R \xrightarrow{\psi} D^{-1}R,$$

where $D^{-1}R$ is the ring of fractions. In particular, D is our set of "denominators." Given $a \in R$ and $d \in D$, we want

$$\frac{a}{1} \sim \frac{ad}{d},$$

but if $da = 0$, then we need the above to equal $0/1 = 0$. This construction, in general, may kill some elements of R. We end up "giving up" injectivity of ψ, despite it being the natural "inclusion" into R. Define

$$J := \{r \in R : \text{ there exists } d \in D \text{ st } dr = 0\}.$$

Note that $J = \{0\}$ if and only if all elements of D are non zero divisors.

Proposition 4.8.1 *We have that*

(i) J is an ideal in R.
(ii) if $d \in D$ and $r \in R$, then $dr \in J$ implies $r \in J$.

Put a relation $\sim$ on $R \times D = \{(r, d)\}$ where $(r_1, d_1) \sim (r_2, d_2)$ if and only if there exists a $d \in D$ such that $d(r_1d_2 - d_1r_2) = 0$. That is, if and only if $r_1d_2 - d_1r_2 \in J$. We claim that $\sim$ is an equivalence relation.[51] We write out transitivity: Suppose $(r_1, d_1) \sim (r_2, d_2)$ and $(r_2, d_2) \sim (r_3, d_3)$. Then, $r_1d_2 - r_2d_1 \in J$ and $r_2d_3 - r_3d_2 \in J$. We want to show $(r_1, d_1) \sim (r_3, d_3)$, or equivalently, $r_1d_3 - d_1r_3 \in J$. Well, we can write

$$(r_1d_2 - d_1r_2)d_3 + d_1(r_2d_3 - d_2r_3) \in J,$$

which after some cancellation gives us $r_1d_3 - d_1r_3 \in J$.

51: Reflexivity and symmetry are immediate.

Remark 4.8.1 (Notation) Let $[r/d]$ be the equivalence class of (r, d), $D^{-1}R$ is the set of equivalence classes, $\psi : R \to D^{-1}R$ where $\psi(r) = [r/1]$ is a ring homomorphism preserving unity. Also, 1 is $[1/1]$. We claim that $D^{-1}R$ is a commutative unital ring with[52]

$$[r_1/d_1] + [r_2/d_2] := [(r_1d_2 + d_1r_2)/(d_1d_2)]$$

and

$$[r_1/d_1] \cdot [r_2/d_2] := [(r_1r_2)/(d_1d_2)].$$

These are standard fraction operations.

52: We omit the proof, but the long part is to check that the operations are well-defined, since they are defined on equivalence classes.

Proposition 4.8.2 *Given R, D, there exists a commutative ring $D^{-1}R$ and a ring homomorphism $\psi : R \to D^{-1}R$ such that*

(i) if $d \in D$, then $\psi(d) \in (D^{-1}R)^{\times}$.
(ii) every element $x \in D^{-1}R$ has the form $x = \psi(r)\psi(d)^{-1}$ for some $r \in R, d \in D$.[53]
(iii) $\ker \psi = J$.

53: That is, they are of the form "r/d."

(i) *Proof.* We have

$$[d/1] \cdot [1/d] = [d/d] = [1/1] = 1.$$

□

(ii) *Proof.* Any element is of the form

$$x = [r/d] = [r/1] \cdot [1/d] = \psi(r)\psi(d)^{-1}.$$

□

(iii) *Proof.* Note that $\psi(r) = 0$ if and only if $[r/1] = [0/1]$, which is true if and only if $r \cdot 1 - 0 \cdot 1 \in J$. □

Thus, our construction is complete and does what we want. Now, rings of fractions come with a *universal property*, so let us do some investigation.

Proposition 4.8.3 (Universal Property of Rings of Fractions) *Let $\varphi : R \to S$ be a ring homomorphism preserving 1 between commutative unital rings. Let $D \subseteq R$ be a multiplicatively closed subset, taking $\psi : R \to D^{-1}R$ to the ring of fractions. If $\psi(D) \subseteq S^{\times}$, then there exists a unique ring homomorphism $\overline{\varphi} : D^{-1}R \to S$ such that $\overline{\varphi} \circ \psi = \varphi$.*

Proof. We start with existence. Let $\overline{\varphi}([r/d]) := \varphi(r)\varphi(d)^{-1}$. We need to check that this is well-defined. If $[r_1/d_1] = [r_2/d_2]$, then $r_1d_2 - d_1r_2 \in J$,

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\psi"'] & S \\
D^{-1}R \arrow[ur, dashed, "\exists!\ \overline{\varphi}"']
\end{tikzcd}$$

Figure 4.3: Commutative diagram for the universal property of rings of fractions

so there exists $d \in D$ such that $d(r_1 d_2 - d_1 r_2) = 0$. hence, we can take

$$\varphi(d)(\varphi(r_1)\varphi(d_2) - \varphi(d_1)\varphi(r_2)) = 0,$$

but $\varphi(d) \in S^\times$, so our multiplication by $\psi(d)^{-1}$ gets us $\varphi(r_1)\varphi(d_2) = \varphi(d_1)\varphi(r_2)$, so

$$\varphi(r_1)\varphi(d_1)^{-1} = \varphi(r_2)\varphi(d_2)^{-1} = \varphi(r_2)\varphi(d_2)^{-1}.$$

Let us show it is a (unique) ring homomorphism. We have uniqueness, since every $x \in R$ has the form $\psi(r)\psi(d)^{-1}$, so

$$\overline{\varphi}(\psi(r)\psi(d)^{-1}) = \overline{\varphi}(\psi(r))\overline{\varphi}(\psi(d)^{-1}),$$

which is just $\varphi(r)\varphi(d)^{-1}$. $\square$

Proposition 4.8.4 *Let $\mathbb{F}$ be a field, $R \subseteq \mathbb{F}$ a subring with $1_{\mathbb{F}} \in R$. Then, R is a domain. Let $Q := \mathrm{Frac}(R) = (R \setminus \{0\})^{-1}R$. Then, Q is isomorphic to the smallest subfield of $\mathbb{F}$ which contains R.*[54]

54: This is one of the more “usual” constructions of the field of fractions. We show that the two definitions coincide, isomorphically.

Proof. Consider the injection $\varphi : R \hookrightarrow \mathbb{F}$. Then, $\varphi(R \setminus \{0\}) \subseteq \mathbb{F} \setminus \{0\}$. so there exists a unique $\overline{\varphi} : Q \to \mathbb{F}$. Well, $\ker(\overline{\varphi}) \subseteq Q$ is an ideal, so $\ker(\overline{\varphi}) = \{0\}$. Thus, $\overline{\varphi}$ is injective, meaning $Q \simeq \overline{\varphi}(Q) \subseteq \mathbb{F}$, and $R = \overline{\varphi}(R)$. If $\mathbb{F}' \subseteq \mathbb{F}$ is any subfield with $R \subseteq \mathbb{F}$, then $Q \subseteq \mathbb{F}'$, since $Q = \{rd^{-1} : r \in R, d \in R \setminus \{0\}\} \subseteq \mathbb{F}'$.[55] $\square$

55: We abuse inclusion notation a lot in this proof.

Remark 4.8.2 A common example of this is $\mathbb{Z} \subseteq \mathbb{R}$, but we can squeeze in $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Introduction to Modules 5

Hereafter, all rings will be unital. The idea is that there is an analogy. Given a group G, recall that we have a category Set_G of G-sets. Now, given a ring R, we get a category of R-modules.

5.1 Category Mod_R of R-Modules

Definition 5.1.1 (Left R-Module) *A left R-module is an ordered triple $(M, +, \cdot)$ where $(M, +)$ is an abelian group and $\cdot : R \times M \to M$ is a function sending $(r, m) \mapsto rm$, where*[1]

(i) $(r_1 + r_2)m = r_1 m + r_2 m$.
(ii) $r(m_1 + m_2) = rm_1 + rm_2$.
(iii) $r_1(r_2 m) = (r_1 r_2)m$.
(iv) $1m = m$.

1: Let $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$. Note that these properties force $0_R m = 0_M$. Also, $(-1)m = -m$.

Definition 5.1.2 (Right R-Module) *A right R-module is $(N, +, \cdot)$, where $(N, +)$ is an abelian group and $\cdot : N \times R \to N$ is a function satisfying similar axioms.*

Definition 5.1.3 (Opposite Ring) *Let $(R, +, \cdot)$ be a ring. Then, the opposite ring R^{op} is a ring defined by $(R, +, \cdot^{op})$, where $a \cdot^{op} b = b \cdot a$.*

Example 5.1.1 Consider $R := \mathbb{M}_n(\mathbb{F})$. Here, $R^{\text{op}} \neq R$, since the matrix ring is not commutative. Nonetheless, $R \simeq R^{\text{op}}$ as rings. Our isomorphism is given by $\varphi : A \mapsto A^t$, the transpose. This works since $(AB)^t = B^t A^t$ and it preserves addition.

Example 5.1.2 Consider the ring

$$R := \mathbb{M}_\infty(\mathbb{F}) := \left\{ (a_{ij}) : \begin{array}{c} a_{ij} \in \mathbb{F} \text{ for } i, j \in \mathbb{Z}_+ \text{ st for all } j \\ \text{only finitely many } a_{ij} \\ \text{are nonzero} \end{array} \right\}.$$

The transpose definitely does not work. We claim that $R \not\simeq R^{\text{op}}$.

Proposition 5.1.1 *A left R-module is a right R^{op}-module. That is, if $M \in \mathsf{LMod}_R$, then we an form $\widetilde{M} \in \mathsf{RMod}_R$, we can define in $\widetilde{M}$ that $m \cdot r := rm$ in M.*[2]

2: Note that for groups, G and G^{op} are always isomorphic via inverses.

We define a category LMod_R of left R-modules. The *objects* ob LMod_R are left R-modules M, and *morphisms* are homomorphisms of left R-modules.

Remark 5.1.1 If R is a field $\mathbb{F}$, then $\mathsf{LMod}_{\mathbb{F}} = \mathsf{Vect}_{\mathbb{F}}$.

Definition 5.1.4 (Module Homomorphism) *Left R-module homomorphisms are functions $\varphi : M \to M'$ such that*

(i) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$.
(ii) $\varphi(rm) = r\varphi(m)$.

Definition 5.1.5 (Module Isomorphism) *An isomorphism φ is an invertible homomorphism of modules.*[3]

3: As an exercise, prove that this is true if and only if φ is bijection.

Remark 5.1.2 Notationally, sometimes we will write $\mathrm{Hom}_R(M, N)$ or $\mathrm{Hom}_R^{\mathrm{left}}(M, N)$ for the set of left R-module homomorphisms.

We also have a category RMod_R of right R-modules, defined as you might expect. The morphisms will be denoted like $\mathrm{Hom}_R^{\mathrm{right}}(M, N)$.

Proposition 5.1.2 (Facts About $\mathrm{Hom}_R^{\mathrm{left}}$) *Let $M, N, P \in \mathsf{LMod}_R$. Then,*

(i) $\mathrm{Hom}_R(M, N)$ *is an abelian group, where $\varphi, \psi \mapsto \varphi + \psi$ is defined by* $(\varphi + \psi)(m) := \varphi(m) + \psi(m)$.[4]
(ii) If R is commutative, then $\mathrm{Hom}_R(M, N) \in \mathsf{Mod}_R$. *Remember, if R is commutative, then* $\mathsf{LMod}_R = \mathsf{RMod}_R$, *so we usually just write* Mod_R.
(iii) Composition is bilinear:

$$\begin{aligned} \mathrm{Hom}_R(N, P) \times \mathrm{Hom}_R(M, N) &\longrightarrow \mathrm{Hom}_R(M, P) \\ (\varphi, \psi) &\longmapsto \varphi \circ \psi \end{aligned}$$

is bilinear. That is, $\varphi \circ (\psi_1 + \psi_2) = \varphi \circ \psi_1 + \varphi \circ \psi_2$, and the same reversing φ and ψ.

4: This is easy to check.

Remark 5.1.3 In general, $\mathrm{Hom}_R(M, N)$ need not be an R-module.That is, $\psi = r\varphi$ might not form an R-module homomorphism. We have that $\psi(rr'm)$ is $r\varphi(r'm) = rr'\varphi(m)$, but $r'\psi(m) = r'r\varphi(m)$. These are generally not the same, unless R is commutative.

Definition 5.1.6 (Endomorphism Ring) *We define* $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ *of module endomorphisms of M.*

Proposition 5.1.3 $\mathrm{End}_R(M)$ *is a ring with unity. The structure is given by: $+$ being addition of homomorphisms, $\cdot$ is composition of homomorphisms, and unity given by* $1 = \mathrm{id}_M$.

Example 5.1.3 Let $\mathbb{F}$ be a field and take $M := \mathbb{F}^n \in \mathsf{Mod}_{\mathbb{F}} = \mathsf{Vect}_{\mathbb{F}}$. Then,

$\mathrm{End}_{\mathbb{F}}(\mathbb{F}^n)$. Well, we know that

$$\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^m) \xrightarrow{\sim} \mathbb{M}_{m\times n}(\mathbb{F}),$$

where $+$ is $+$ of matrices and $\circ$ is $\cdot$ of matrices. Hence, the endomorphism ring $\mathrm{End}_{\mathbb{F}}(\mathbb{F}^n) \simeq \mathbb{M}_n(\mathbb{F})$.

Remark 5.1.4 Define

$$\mathbb{F}^{\infty} := \{(a_k)_{k\in\mathbb{Z}_+} : a_k \in \mathbb{F} \text{ st all but finitely many } a_k = 0\}$$

is an $\mathbb{F}$-vector space. Then, $R := \mathrm{End}_{\mathbb{F}}(\mathbb{F}^{\infty}) = \mathbb{M}_{\infty}(\mathbb{F})$ is from earlier.

Definition 5.1.7 (Automorphism Group) *We define* $\mathrm{Aut}_R(M)$ *to be the automorphism group of a module* M.

Remark 5.1.5 Since we just need the invertible endomorphisms, it is clear that $\mathrm{Aut}_R(M) = \mathrm{End}_R(M)^{\times}$.

Example 5.1.4 We have that

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{F}^n) = \mathrm{End}_{\mathbb{F}}(\mathbb{F}^n)^{\times} = \mathrm{GL}_n(\mathbb{F}) \subseteq \mathbb{M}_n(\mathbb{F}) \simeq \mathrm{End}_{\mathbb{F}}(\mathbb{F}^n).$$

Example 5.1.5 (Free Module of Rank One) If R is a ring with unity, then $M = R$ is a left R-module by $(R, +, \cdot)$.[5]

5: The easiest way to think about this is when we write $\mathbb{F}$ to be a vector space over itself.

Example 5.1.6 Let $R := \mathbb{M}_2(\mathbb{F})$. Let $M := \mathbb{F}^2$. Then, M has the natural structure of a left R-module. Clearly $M \not\simeq R$ as a module, as it is too small.

Exercise 5.1.1 What is $S := \mathrm{End}_R(M) = \mathrm{End}_{\mathbb{M}_2(\mathbb{F})}(\mathbb{F}^2)$?

Proof. Well, $S = \{f : \mathbb{F}^2 \to \mathbb{F}^2\}$ of R-module homomorphisms. This is just the set of abelian group homomorphisms. That is, $\varphi : \mathbb{F}^2 \to \mathbb{F}^2$ such that $\varphi(Av) = A\varphi(v)$ for all $A \in \mathbb{M}_2(\mathbb{F})$ and $v \in \mathbb{F}^2$. Note that $\lambda \in F$ implies we can form λI_2. As a consequence of $\varphi \in \mathrm{End}_R(M)$ is $\varphi(\lambda I_2 v) = \lambda I_2 \varphi(v)$, so $\varphi(\lambda v) = \lambda\varphi(v)$. Hence, φ is an $\mathbb{F}$-linear map, so $\varphi(v) = Bv$ for a fixed $B \in \mathbb{M}_2(\mathbb{F})$. In order for it to be an R-module map, we need $\varphi(Av) = A\varphi(v)$ for all $A \in \mathbb{M}_2(\mathbb{F})$. That is, $B(Av) = A(Bv)$ for all $v \in \mathbb{F}^2$ and $A \in R$. Thus, we need $BA = AB$ for all $A \in R$, so $\mathrm{End}_R(M) = \{\lambda I_2 : \lambda \in \mathbb{F}\} \simeq \mathbb{F}$.[6] $\square$

6: This is the center of the matrix ring.

Example 5.1.7 Let $\mathbb{F}$ be a field and G a group. Then, set $R := \mathbb{F}[G]$, the group ring of G over $\mathbb{F}$. What is a module over $\mathbb{F}[G]$?

5.2 Quotients

Definition 5.2.1 (Submodule) *A subset $N \subseteq M$ is a submodule if $(N, +) \leq (M, +)$ and $rN \subseteq N$ for all $r \in R$.*[7]

7: As you should expect, N is a module in its own right.

Example 5.2.1 Note that if $R := \mathbb{Z}$, then a $\mathbb{Z}$-module is precisely an abelian group. Then, a submodule is *exactly* a subgroup.

Example 5.2.2 Let $R := \mathbb{F}$, a field. Then, $\mathsf{Mod}_{\mathbb{F}} = \mathsf{Vect}_{\mathbb{F}}$ and submodules are subspaces.

Example 5.2.3 Consider $R := \mathbb{F}[x]$. An $\mathbb{F}[x]$-module is the same thing as a pair (V, T), where $V \in \mathsf{Vect}$ and $T : V \to V$ is an $\mathbb{F}$-linear map. If

$$f = \sum_{k=1}^{n} c_k x^k \quad \text{and} \quad c_k \in \mathbb{F},$$

then

$$f(T) = \sum_k c_k T^k$$

and

$$f(T)v = \sum_k c_k T^k(v).$$

Let V_T be this R-module. Then, submodules of V_T are precisely T-invariant subspaces.[8]

8: Recall that this means $W \subseteq V$ such that $T(W) \subseteq W$.

Example 5.2.4 If R is an R-module over itself, then a submodule of R is *left* ideals. This is clear that the ideal properties force the submodule ideals.

Definition 5.2.2 (Quotient Module) *Let R be a ring, M a module, and $N \subseteq M$ a submodule. Then, the quotient module M/N has*

(i) underlying abelian group M/N.
(ii) scalar multiplication given by

$$r(x + N) := rx + N.$$

Proposition 5.2.1 (Homomorphism Theorem) *Let $\varphi : M \to N$ be a homomorphism of R-modules and $A \subseteq M$ a submodule. If $A \subseteq \ker \varphi$, then there exists a unique homomorphism $\overline{\varphi} : M/A \to N$ such that $\overline{\varphi} \circ \pi = \varphi$.*[9]

9: $\pi : M \twoheadrightarrow M/A$ is the quotient homomorphism.

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & N \\ M/A \arrow[ur, dashed, "\exists!"', "\overline{\varphi}"] & \end{tikzcd}$$

Figure 5.1: Here is the standard homomorphism theorem diagram, where $\varphi(A) = 0$.

Theorem 5.2.2 (First Isomorphism Theorem) *Let $\varphi : M \to N$ be a homomorphism of R-modules. Then, we have an isomorphism of modules $M/\ker\varphi \xrightarrow{\sim} \varphi(M)$. Note that $\ker\varphi \subseteq M$ is a submodule and $\varphi(M) \subseteq N$.*

$$\begin{tikzcd}
M \arrow[rrr, "\varphi"] \arrow[dr, "\pi"'] & & & N \\
& M/\ker\varphi \arrow[r, "\sim", "\overline{\varphi}"'] & \varphi(M) \arrow[ur, hook, "\iota"'] &
\end{tikzcd}$$

Figure 5.2: We have $\overline{\varphi}(x+\ker\varphi) = \varphi(x)$.

Theorem 5.2.3 (Second Isomorphism Theorem) *Let $A, B \subseteq M$ be submodules. Then,*

(i) $A + B$ *is a submodule.*
(ii) $A \cap B$ *is a submodule of* A.
(iii) B *is a submodule of* $A + B$.
(iv) $A/A \cap B \xrightarrow{\sim} (A+B)/B$.

Remark 5.2.1 The diamond isomorphism theorem is cleaner for modules than the other structures we have seen. This is because we can form quotients by arbitrary submodules, so we do not need a notion of "normality."[10]

10: Remember, for rings we had ideals acting as "normal" rings.

Theorem 5.2.4 (Third Isomorphism Theorem) *Let A, B be sub modules of M and $A \subseteq B$. Then,*

(i) $B/A \subseteq M/A$ *is a submodule.*
(ii) $M/B \xrightarrow{\sim} (M/A)/(B/A)$.

Theorem 5.2.5 (Fourth Isomorphism Theorem) *Let $N \subseteq M$. Then, we have a bijection*

$$\left\{\begin{matrix}\text{submodules } A \subseteq M \\ \text{st } N \subseteq A\end{matrix}\right\} \underset{\sim}{\overset{\text{bijection}}{\longleftrightarrow}} \left\{\begin{matrix}\text{submodules} \\ \overline{A} \subseteq M/N\end{matrix}\right\},$$

where $A \mapsto \pi(A)$ and $\pi(A) \mapsto \pi^{-1}(A)$.

Let M be an R-module and $S \subseteq M$ a subset. Define[11]

11: Note that RS is a submodule of M.

Proposition 5.2.6

$$RS = \bigcap_{\text{submodules } N \subseteq M \, S \subseteq N} N$$

That is, RS is the *smallest* submodule containing S. We say that M is "generated by" S if $RS = M$.

Definition 5.2.3 (Finitely Generated) *We say M is finitely generated if there exists $S \subseteq M$ with $|S| < \infty$ such that $S = M$.*[12]

12: In particular, if $Rx = M$ for some $x \in M$, then M is a *cyclic module*.

Example 5.2.5 It is clear that R is a cyclic R module, as $1 \in R$. More generally, if $I \subseteq R$ is a left ideal (submodule), then R/I is a cyclic module.[13]

13: It is generated by the coset $1 + I$.

Proposition 5.2.7 *Every cyclic module is isomorphic to some R/I*

Proof. If M is cyclic, pick a generator $x \in M$ such that $Rx = M$. Define a homomorphism of modules $\varphi : R \to M$ such that $\varphi : r \mapsto rx$.[14] Since M is cyclic, φ is surjective. We get isomorphism from $M \simeq R/\ker\varphi$ where I is $\ker\varphi$. □

14:

$$\begin{aligned} \varphi(r_1 + r_2) &= (r_1 + r_2)x \\ &= r_1 x + r_2 x \\ &= \varphi(r_1) + \varphi(r_2) \\ \varphi(r'r) &= (r'r)x \\ &= r'\varphi(r) \end{aligned}$$

5.3 Coproducts and Products

Let $\{M_i\}_{i \in I}$ be an indexed set of R-modules.

Definition 5.3.1 (Module Product) *Define*[15] *the (direct) product*

$$\prod_{i \in I} M_i := \{(x_i)_{i \in I} : x_i \in M_i\}.$$

If $I = \{1, \dots, n\}$, then

$$\prod_{i \in I} M_i = M_1 \times \cdots \times M_n = \{(x_1, \dots, x_n) : x_i \in M_i\}.$$

15: The module structure on $M := \prod M_i$ is component-wise.

Definition 5.3.2 (Module Coproduct) *Define the coproduct (or direct sum)*

$$\bigoplus_{i \in I} M_i := \{(x_i)_{i \in I} : |\{i \in I : x_i \neq 0\}| < \infty\} \subseteq \prod_{i \in I} M_i.$$

This is a module.[16] *If I is finite, then*

$$\bigoplus_{i \in I} M_i = M_1 \oplus \cdots \oplus M_n.$$

16: The definition tells us that finitely many x_i are nonzero.

Remark 5.3.1 By definition, it is clear that

$$M_1 \oplus \cdots \oplus M_n \simeq M_1 \times \cdots \times M_n.$$

Let us loosely discuss some universal properties. Consider the set

$$\left\{ N \xrightarrow{f} \prod_{i \in I} M_i \right\}$$

of module homomorphisms. Then we can directly build $f_i : N \to M_i$ of R-module homomorphisms. Then, $f(y) := (f_i(y))_{i \in I}$. On the other hand, consider the set

$$\left\{ \bigoplus_{i \in I} M_i \xrightarrow{f} N \right\}$$

of module homomorphisms. Then, we can build $f_i : M_i \to N$, where $f((x_i)_{i \in I}) = \sum f_i(x_i)$.[17] Remember, the product of G, H in Grp is just $G \times H$. Yet, the coproduct $G * H$ is the "free product," which *does not* look like a product.

17: The duality comes from the fact that we are mapping *into* our object for products and *out of* our object for coproducts.

Example 5.3.1 The coproduct $C_2 * C_2 \simeq D_\infty$ in Grp. This one can be done simply in terms of presentations. Let $C_2 \simeq \langle a | a^2 \rangle$ and $C_2 \simeq \langle b | b^2 \rangle$. Then, $C_2 * C_2 \simeq \langle a, b | a^2, b^2 \rangle$.

5.4 Internal Direct Sums and Free Modules

Fix a module M and consider a collection $\{N_i \subseteq M\}_{i \in I}$ of submodules. We can then form the coproduct map

$$\bigoplus_{i \in I} N_i \xrightarrow{\varphi} M,$$

where φ is the "tautological map." That is, $\varphi((x_i)) = \sum x_i$, where $(x_i) \in N_i$. This just means φ is the sum of the inclusions.

Definition 5.4.1 (Internal Direct Sum) *We say M, as above, is an internal direct sum of submodules $\{N_i\}$ if φ is an isomorphism.*

Proposition 5.4.1 *Let M and $\{N_i\}$ be as above. Then, define*[18]

$$N := \sum_{i \in I} N_i \subseteq M$$

Then, the following are equivalent:

(i) N is an internal direct sum of $\{N_i\}$.
(ii) For every $\{i_1, \dots, i_n\} \subseteq I$ and $j \notin \{i_1, \dots, i_n\}$ we have

$$N_j \cap (N_{i_1} + \cdots + N_{i_n}) = \{0\}.$$

(iii) Every $x \in N$ can be written uniquely as $x = x_1 + \cdots x_n$, where $x_k \in N_{i_k}$ for pairwise distinct i_k.

18: The sum is the submodule given by $\bigcup N_i$, which is *not* usually a submodule.

Example 5.4.1 Let $N_1, N_2 \subseteq M$. Then,

$$N_1 \oplus N_2 \xrightarrow{\sim} M$$

via φ if and only if $N_1 + N_2 = M$ and $N_1 \cap N_2 = \{0\}$.[19]

19: Recall that this is *precisely* how we use internal direct sums for vector spaces.

Example 5.4.2 Let $N_1, N_2, N_3 \subseteq M$. You can have $N_i \cap N_j = \{0\}$ for all $i \neq j$, but $N_1 \oplus N_2 \oplus N_3 \to M$ is not an isomorphism. For instance, with $M = R \oplus R$, then we could define

$$\begin{aligned} N_1 &= \{(r, 0) : r \in R\} \\ N_2 &= \{(0, r) : r \in R\} \\ N_3 &= \{(r, r) : r \in R\}. \end{aligned}$$

Now, let R be unital.

Definition 5.4.2 (Free R-Module) *A free R-module on a set S is (M, e) where M is and R-module and $e : S \to M$ is a function sending $s \mapsto e_s$ of "basis elements."*[20]

20: By this, we mean that for all $x \in M$ there exists a unique collection $\{a_s \in R\}_{s \in S}$ such that

$$x = \sum_{s \in S} a_s e_s,$$

where we necessarily have $a_s = 0$ for all but finitely many $s \in S$.

For instance, $S := [n]$, then $e : S \to M$ gives us $e_1, \ldots, e_n$. Then, every $x \in M$ can be *uniquely* written as

$$x = \sum_{k=1}^{n} a_k e_k$$

for $a_k \in R$.

Example 5.4.3 Let $R := \mathbb{F}$ a field, Then, every $\mathbb{F}$-module admits the structure of a free $\mathbb{F}$-module.

Proposition 5.4.2 *A free module exists for every set S. In fact,*

$$M := \bigoplus_{s \in S} R$$

is free on $e : S \to M$ by $(e_s)_t := \delta_{st}$.[21]

21: This is the Kronecker delta.

Theorem 5.4.3 (Universal Property of Free Modules) *Let $(M, e : S \to M)$ be a free module. Then, for a module N and function $\varphi : S \to N$, there exists a unique R-module homomorphism $\widetilde{\varphi} : M \to N$ such that $\widetilde{\varphi} \circ e = \varphi$.*

$$\begin{tikzcd} S \arrow[r, "\varphi"] \arrow[d, "e"'] & N \\ M \arrow[ur, dashed, "\exists!"', "\widetilde{\varphi}"] & \end{tikzcd}$$

Figure 5.3: Universal property of free modules

Warning: Unlike vector spaces, most modules are not free!

Example 5.4.4 For instance, let $R := \mathbb{Z}$. Consider the module $M = \mathbb{Z}/(3) \ni e = 1 + (3)$.

5.5 Simple and Semi-Simple Modules

Fix R.

Definition 5.5.1 (Simple Module) *An R-module M is simple if it has exactly two submodules.*[22]

22: Necessarily, $\{0\} \neq M$. That is, M is nontrivial.

Proposition 5.5.1 *Every simple module is cyclic and isomorphic to one of the form R/I, where I is a "maximal left ideal."*[23]

23: That is, I is maximal among *proper* left ideals in R.

Proof. Let M be simple. Then, $M \neq \{0\}$, so there exists $x \in M$ such that $x \neq 0$. Pick any such x and define $\varphi : R \to M$ by $\varphi(r) = rx$. This is an R-module homomorphism. We claim that φ is surjective. Well, $\varphi(R) \subseteq M$ is a submodule, and since $\varphi(R)$ is nontrivial, $\varphi(R) = M$. Then, we have $\pi : R \to R/\ker\varphi$, and via our isomorphism theorem we have $\overline{\varphi} : R/\ker\varphi \xrightarrow{\sim} M$ where $\overline{\varphi}(r + I) = \varphi(r)$. $I := \ker\varphi$ is a left ideal. Since $R/I \simeq M$, R/I is simple.[24] Well, submodules of R/I correspond exactly to submodules $J \subseteq R$ such that $I \subseteq J$. If we have a submodule $\overline{J}$, then we just take $\pi^{-1}(\overline{J})$. Simplicity gives us maximality. □

24: Isomorphisms preserve submodules.

Remark 5.5.1 An altered proof via Zorn's lemma gives us that any ring has at least one nontrivial maximal left ideal.

Example 5.5.1 Note that if $R := \mathbb{F}$ or $R := D$, a division ring, then there is only one simple module up to isomorphism.

Example 5.5.2 Let $R := \mathbb{Z}$. All simple modules are isomorphic to $\mathbb{Z}/(p)$, where p is prime. That is, the simple $\mathbb{Z}$-modules are the cyclic groups of prime order. Note that $\mathbb{Z}$, although it is cyclic, is *not* a simple $\mathbb{Z}$-module.

Example 5.5.3 Let R be $\mathbb{M}_n(\mathbb{F})$ for $n \geq 1$. Then, we can define $M := \mathbb{F}^n$ of "column vectors" as a module over the matrix ring. It is simple as an R-module, but it is certainly not a simple $\mathbb{F}$-module![25]

25: If $v \in \mathbb{F}^n$ with $v \neq 0$, then $\{Av : A \in \mathbb{M}_n(\mathbb{F})\}$ has to be all of $\mathbb{F}^n$. This is just a bit of linear algebra exercise.

Proposition 5.5.2 (Schur's Lemma) *If S, S' are simple R-modules and $f : S \to S'$ is a module homomorphism, then either $f = 0$ or f is an isomorphism. In particular, $D := \mathrm{End}_R(S)$ is a division ring.*[26]

26: Recall that $\mathrm{End}_R(S)$ is always a unital ring for modules.

Proof. Let $f : S \to S'$. We have submodules $\ker f \subseteq S$ and $f(S) \subseteq S'$. Suppose $f \neq 0$. That is, there exists $0 \neq s \in S$ such that $f(x) \neq 0$. Then, $\ker f \neq S$, so $\ker f = \{0\}$, and $f(S) \neq 0$, so $f(S) = S'$. Thus, f is a bijection.[27] □

27: The structure theory of simple modules is quite easy!

Example 5.5.4 Take $\mathbb{F}^n$ as a $\mathbb{M}_n(\mathbb{F})$-module. Then, $\mathrm{End}_R(\mathbb{F}^n) = \mathbb{F}$, a division ring.

Definition 5.5.2 (Summand) *A submodule $N \subseteq M$ is a summand of M if there exists $N' \subseteq M$ so that the tautological map $N \oplus N' \xrightarrow{\sim} M$ with $(x, x') \mapsto x + x'$ is an isomorphism.*[28]

Note that $N' \simeq M/N$. This is *not* equality. Do not confuse them.

28: Note that N' is not unique. Let R be a ring and $M = R \oplus R$. Let $N = R \oplus 0$. Then, $N' = \{(0, r)\}$ and $N'' = \{(r, r) : r \in R\}$ can be used to form

$$M = N \oplus N' = N \oplus N''.$$

Proposition 5.5.3 *Let $N \subseteq M$ be a submodule. The following are equivalent:*

(i) *N is a summand of M.*
(ii) *There exists a module homomorphism $r : M \to N$ such that $r \circ \iota = \mathrm{id}_N$, where $\iota : N \hookrightarrow M$ is the inclusion.*[29]
(iii) *There exists a module endomorphism $e : M \to M$ such that $e \circ e = e$ and $e(M) = N$.*[30]

29: We will often call r a "retraction."

30: Here, e is *idempotent*. In linear algebra, we call such e *projection* maps or *projectors*.

Proof. Start with (i) $\Rightarrow$ (iii). We have that every $x \in M$ can be written uniquely as $x = y + y'$ where $y \in N$ and $y' \in N'$. We define $e(x) := y$, and we claim that $e : M \to M$ is a module homomorphism and $e \circ e = e$ and $e(M) = N$. If we have $x_1, x_2 \in M$, then we can write them uniquely as $x_1 = y_1 + y_1'$ and $x_2 = y_2 + y_2'$, where $y_1, y_2 \in N$ and $y_1', y_2' \in N'$. Then,

$$x_1 + x_2 = (y_1 + y_2) + (y_1' + y_2'),$$

so

$$e(x_1 + x_2) = y_1 + y_2 = e(x_1) + e(x_2).$$

Also, $rx_1 = ry_1 + ry_1'$, so $e(rx_1) = re(x_1)$.[31] It is clear that $e(M) = N$ and e is idempotent. The idea is that

31: Thus, e is a module homomorphism.

$$e \sim \begin{pmatrix} \mathrm{id}_N & 0 \\ 0 & 0 \end{pmatrix} \quad \text{wrt} \quad N \oplus N'.$$

Now, we prove (iii) $\Rightarrow$ (ii). Given e, define $r : M \to N$ by $r(x) := e(x)$. Then, $r \circ i = \mathrm{id}_N$. Finally, consider (ii) $\Rightarrow$ (i). We have $r : M \to N$ such that $r|_N = \mathrm{id}_N$. Define $N' := \ker r$. We claim that $N \oplus N' \xrightarrow{\sim} M$ via the tautological action. Define an inverse function $M \to N \oplus N'$ by $x \mapsto (r(x), x - r(x))$, then we are done. $\square$

Definition 5.5.3 (Semi-Simple Module) *We say that M is semi-simple if every submodule is a summand.*

Remark 5.5.2 Every simple module S is semi-simple, as we have a trivial decomposition $S = S \oplus 0$.[32]

32: Occasionally we write $\mathbf{0} \equiv \{0\}$.

Our goal is to prove that every semi-simple module is isomorphic to the coproduct $\bigoplus_i S_i$ of simple modules.[33]

33: Note that for "semi-simple" rings, which includes fields, every corresponding module is semi-simple.

Example 5.5.5 Let $R := \mathbb{F}[x]$. Then, R is not semi-simple as an R-module. For instance, $I := (x) = x\mathbb{F}[x]$ is a submodule of R, but not a summand.

Proposition 5.5.4 *Let M be a semi-simple module. Suppose $N \subseteq M$ is a submodule. Then, both N and M/N are semi-simple.*

Proof. Let $P \subseteq N$ be a submodule. Then, P is a submodule of M. Since M is semi-simple, there exists a retraction $r : M \to P$ so that $r|_P = \mathrm{id}_P$. Let $r' := r|_N : N \to P$. Then, $r'|_P = \mathrm{id}_P$, so P is a summand of N. Consider the quotient module N/N. Let $\pi : M \to M/N$ be the quotient map. Consider a submodule $\overline{P} \subseteq M/N$. Let $P := \pi^{-1}(\overline{P}) \subseteq M$. We have that $N \subseteq P \subseteq M$ is a chain of submodules. Since M is semi-simple, there exists a retraction $r : M \to P$ such that $r|_P = \mathrm{id}_P$. Define $r' : M/N \to \overline{P}$ by $r'(x+N) := r(x) + N$.[34] $\square$

34: This map is well-defined, since $r|_N = \mathrm{id}_N$, since $N \subseteq P$. Also, $r'|_{\overline{P}} = \mathrm{id}_{\overline{P}}$, by construction.

Lemma 5.5.5 *Let $f : M \to L$ be a surjective homomorphism from a semi-simple M. Then, there exist submodules $N, N' \subseteq M$ such that*

(i) $N \oplus N' \xrightarrow{\sim} M$.
(ii) $N' \simeq L$.

Proof. Let $N := \ker f$. Since M is semi-simple, we can find a submodule N' so that $N \oplus N' = M$.[35] For (ii), the isomorphism is given by

$$N' \xrightarrow{f|_{N'}} L,$$

which is injective since $\ker f = N \cap N' = 0$.[36] $\square$

35: This is (i).

36: It is surjective. If $\overline{x} \in L$, pick $x \in M$ such that $f(x) = \overline{x}$. Write $x = y + y'$ where $y \in N$ and $y' \in N'$. Then, $f(x) = f(y')$.

Corollary 5.5.6 *If M is a semi-simple module, then if M has a simple quotient module, then M contains a simple submodule.*

Proof. See the lemma. Simplicity is preserved under the isomorphism $N' \xrightarrow{\sim} L$. $\square$

Proposition 5.5.7 *Every nontrivial semi-simple module contains a simple submodule.*

Proof. The trivial module 0 is always semi-simple.[37] Let $M \neq 0$. Pick an element $x \in M$ with $x \neq 0$. Then, we get a cyclic submodule $Rx \subseteq M$. Then, $Rx \neq 0$ and semi-simple. Without loss of generality, we can assume the module is nontrivial and cyclic. We know how to classify cyclic modules.[38] We can take $M := R/I$, where $I \subsetneq R$ is a left ideal. We will construct a simple quotient module of M. The

$$\left\{ \begin{matrix} \text{submodules} \\ \overline{J} \subsetneq R/I \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{submodules } J \subseteq R \\ \text{st } I \subseteq J \subsetneq R \end{matrix} \right\}.$$

We want to take $(R/I)/\overline{J} \xrightarrow{\sim} R/J$. The observation is that we need to find a left ideal J containing I which is maximal among proper left ideals containing I.[39] Apply Zorn's lemma to the poset on the RHS above. $\square$

37: It is excluded since simple modules are nontrivial.

38: They are quotients of the ring by left ideals.

39: This will imply that R/J is simple (as there are no intermediate ideals).

Definition 5.5.4 (M^{SS}) *Let M be a module. Define*

$$\mathrm{Simp}(M) := \{S \subseteq M : S \text{ simple submodule}\}.$$

Then, we take[40]

$$M^{\mathrm{SS}} := \sum_{S \in \mathrm{Simp}(M)} S := \begin{matrix} \text{submodule of } M \\ \text{generated by } \bigcup_{\mathrm{Simp}(M)} S \end{matrix} \subseteq M.$$

40: Really, M^{SS} is the set of all sums of $x_i \in S_i$ for some $S_i \in \mathrm{Simp}(M)$.

Note that $\mathbb{Z}^{\mathsf{SS}} = 0$.

Example 5.5.6 Let $R := \mathbb{Z}$. Remember, $\mathsf{Mod}_{\mathbb{Z}}$ is just abelian groups. Let M be an abelian group. Then, M^{SS} is the subgroups generated by all $x \in M$ such that $|x| = p$ for some prime p. For instance, if we take $(\mathbb{Z}/p^2)^{\mathsf{SS}} = (p\mathbb{Z}/p^2) \simeq \mathbb{Z}/p$.

Proposition 5.5.8 *Consider $N \subseteq M^{\mathsf{SS}}$. Then, there exists a subset $X \subseteq$ $\mathrm{Simp}(M)$ such that the tautological map*

$$N \oplus \bigoplus_{S \in X} S \xrightarrow{\sim} M^{\mathsf{SS}} \overset{\iota}{\hookrightarrow} M$$

is an isomorphism.

Proof. We want to use Zorn's lemma. Let $\mathscr{P}$ be the set of subsets $A \subseteq$ $\mathrm{Simp}(M)$ such that the tautological map

$$N \oplus \bigoplus_{S \in A} S \xrightarrow{f_A} M$$

is injective.[41] It is clear that $\mathscr{P}$ is a poset with $\subseteq$. Note that $\mathscr{P} \neq \varnothing$, since $\varnothing \in \mathscr{P}$. We claim that every nonempty chain $\mathscr{C} \subseteq \mathscr{P}$ has an upper bound in $\mathscr{P}$. The idea is to consider

41: As before, $\mathrm{Image}(f_A) \subseteq M^{\mathsf{SS}}$.

$$B := \bigcup_{A \in \mathscr{C}} A \subseteq \mathrm{Simp}(M).$$

In fact, $B \in \mathscr{P}$; i.e.,

$$f_B : N \oplus \bigoplus_{S \in B} S \to M$$

is injective. An element in the domain of f_B can be written

$$z := (x, y_1, \ldots, y_k) \quad x \in N, y_i \in S_i, S_k \in B.$$

Suppose $f_B(z) = 0$. Each $S_i \in A_i$ for some $A_i \in \mathscr{C}$. Since $\mathscr{C}$ is totally ordered, there exists a j so that $A_i \subseteq A_j$, so $S_1, \ldots, S_k \in A_j \in \mathscr{P}$. Thus, f_{A_i} is injective and $f_{A_i}(z) = f_B(z) = 0$, so $z = 0$. By Zorn's lemma, there exists $X \in \mathscr{P}$ which is maximal. We get

$$f_X : N \oplus \bigoplus_{S \in X} S \to M^{\mathsf{SS}} \subseteq M$$

which is injective. We claim that $\mathrm{Image}(f_X) = M^{\mathsf{SS}}$. If f_X is not surjective onto M^{SS}, then there exists $S' \in \mathrm{Simp}(M)$ not in the image of f_X. Yet, we can form

$$S' \cap \mathrm{Image}(f_X) = 0,$$

since S' is simple. Hence,

$$f_{X \cup \{S'\}} : N \oplus \bigoplus_{S \in X} S \oplus S' \to M$$

is also injective, which contradicts maximality. $\square$

Corollary 5.5.9 *M^{SS} is isomorphic to a direct sum of simple submodules.*

Proof. Use the proposition with $N = 0$. □

Corollary 5.5.10 *M^{SS} is semi-simple.*

Proof. If $N \subseteq M^{\mathsf{SS}}$, use the proposition and take $N' := \bigoplus_X S$. Then, $N \oplus N' \xrightarrow{\sim} M^{\mathsf{SS}}$.[42] □

42: That is, N is a summand of M^{SS}.

Theorem 5.5.11 (Semi-Simple Structure Theorem) *Let M be an R-module. The following are equivalent:*

(i) M is semi-simple.
(ii) $M = M^{\mathsf{SS}}$.
(iii) M is isomorphic to a direct sum of simple submodules.

Proof. Start with (i) $\Rightarrow$ (ii). Let M be semi-simple. Well, $M^{\mathsf{SS}} \subseteq M$, so $M^{\mathsf{SS}} \oplus N = M$ for some submodule $N \subseteq M$.[43] We showed that submodules of semi-simple modules are semi-simple, so N is semi-simple. If $N = 0$, we are done. If $N \neq 0$, then there exists a simple submodule $S \subseteq N$.[44] Then, $S \subseteq M^{\mathsf{SS}} \cap N$, a contradiction to the definition of the "direct sum." Thus, $N = 0$. For (ii) $\Rightarrow$ (i), the corollary tells us M^{SS} is semi-simple. Similarly, (ii) $\Rightarrow$ (iii) comes from M^{SS} being a direct sum of simple submodules. Finally, (iii) $\Rightarrow$ (ii) is immediate.[45] □

43: This is what it means for M to be semi-simple.

44: This was proved earlier.

45: The hypothesis literally implies

$$M = \sum_{S \in \mathrm{Simp}(M)} S,$$

which is just M^{SS}.

Remark 5.5.3 The dimension $\dim \mathscr{V}$ of a vector space $\mathscr{V}$ over $\mathbb{F}$ is precisely the number of summands in a simple direct sum decomposition. In particular, it is the number of copies of $\mathbb{F}$ in the decomposition (since the only simple submodules of $\mathscr{V}$ are isomorphic to $\mathbb{F}$).

5.6 Semi-Simple Rings

Let R be unital.

Definition 5.6.1 (Semi-Simple Ring) *We say that R is semi-simple as a ring if R is a semi-simple as a (left) R-module.*

Example 5.6.1 Let $R := \mathbb{M}_n(\mathbb{F})$, where $\mathbb{F}$ is a field (or division ring). Let $I_k \subseteq R$ be the set of matrices which are nonzero only in the kth column. $I_k \simeq \mathbb{F}^n$ is a simple module.[46] Well,

$$R \simeq I_1 \oplus \cdots \oplus I_n$$

as R-modules.

46: $\mathbb{F}^n$ is the set of column vectors; i.e., the space $\mathbb{F}^{1\times n}$.

Example 5.6.2 Let $R := \mathbb{Z}$ or $R := \mathbb{F}[x]$. This is not a semi-simple ring, since neither of these have simple submodules whatsoever.

Proposition 5.6.1 *Let R be a ring. The following are equivalent:*

(i) R is semi-simple as a ring.[47]
(ii) Every R-module is semi-simple.

Furthermore, if these hold, then

(a) R is a finite direct sum of simple submodules.
(b) there are only finitely many simple R-modules up to isomorphism.

47: That is, R is semi-simple as an R-module.

To attack this, we will need a few lemmas.

Lemma 5.6.2 *Let R be a ring. If M is an R-module and $M = \bigoplus_i M_i$ for some $\{M_i \subseteq M\}$. Then,*

$$M^{\mathrm{SS}} = \bigoplus_i M_i^{\mathrm{SS}}.$$

Proof. Clearly each $M_i^{\mathrm{SS}} \subseteq M^{\mathrm{SS}}$, so $\sum_i M_i^{\mathrm{SS}} \subseteq M^{\mathrm{SS}}$. Then, the tautological map

$$\bigoplus_i M_i^{\mathrm{SS}} \to M^{\mathrm{SS}}$$

is injective. We just want to show that it is surjective. Suppose $S \subseteq M$ is a simple submodule.[48] Now, simple modules are always cyclic, so $S = Rx \simeq R/I$ for some $x \in M$ with $x \neq 0$.[49] We can write $x = (x_i)$ where $x_i \in M_i$ and all but finitely many $x_i = 0$. We claim that each nonzero x_i is contained in some simple submodule of M_i. In fact, $S_i := Rx_i \subseteq M_i$ is a simple submodule. Then,

$$J := \ker \xrightarrow{\text{inj}} R \xrightarrow{r \mapsto x_i} Rx_i$$

leaves $Rx_i \simeq R/J$, and since I is maximal among left ideals, $J = I$, so $S_i \simeq S$, meaning $x_i \in M_i^{\mathrm{SS}}$. □

48: Of course, this also means $S \subseteq M^{\mathrm{SS}}$.
49: Note, $Ix = 0$. Thus, $Ix_I = 0$.

Lemma 5.6.3 *Let M be a cyclic module. If*

$$\bigoplus_i M_i = M$$

for some $\{M_i \subseteq M\}_{i \in I}$, then $M_i = 0$ for all but finitely many i.

Proof. Pick a generator $x \in M$. Then, $M = Rx$. The same idea arises, taking $x = (x_i)$ where $x_i \in M_i$ and all but finitely many are 0. The claim is that the direct sum decomposition implies $Rx_i = M_i$ for all $i \in I$. Write $x = x_1 + \cdots + x_n$, where $x_k \neq 0$ and $x_k \in M_{k_i}$ for distinct k_i. Suppose $y \in M_j$ where $j \notin \{k_1, \ldots, k_n\}$. Since M is cyclic, we can write $y = rx$ for some $r \in R$. On the other hand,[50]

50: We abuse notation in the standard way, switching back and forth between tuple and sum notation for the internal direct sum.

$$\underbrace{y}_{M_y} = rx = \underbrace{rx_1 + \cdots + rx_n}_{M_{k_1}+\cdots+M_{k_n}},$$

but there is no overlap, so this forces both sides to be 0.[51] Thus, $M_j = 0$. □

51: We use that $\bigoplus M_i = M$.

Now, we can prove the proposition from earlier.

Proof of Proposition. Start with (ii) ⇒ (i). If every R-module is semi-simple, then R is semi-simple as a module, so R is semi-simple as a ring. Conversely, consider (i) ⇒ (ii). Suppose R is semi-simple. Then, $R = R^{\mathrm{SS}}$. Consider $M = \bigoplus_J R$, a free module, It is clear that

$$M^{\mathrm{SS}} = \bigoplus R^{\mathrm{SS}} = \bigoplus R$$

implies M is semi-simple. Now, we have a fact that every R module is isomorphic to a quotient of a free module. We can take the simplest map

$$\bigoplus_{x\in M} R \xrightarrow{\text{surj}} M.$$

Plus, quotients of semi-simple modules are semi-simple. Finally for (a), R is a cyclic R-module, so $R = \bigoplus_{i=1}^n S_i$, by the lemma. What about (b)? Well, if S is simple then it is cyclic, so $S \simeq R/I$. □

Lemma 5.6.4 *Suppose $M = \bigoplus_{i\in I} S_i$, where each $S_i \subseteq M$ is a simple submodule. Then, any simple submodule of M is isomorphic to one of the S_is.*

Proof. Consider $S \subseteq M$. Then, $S = Rx$ for some $x \in M$ with $x \neq 0$. Then, $x = x_1 + \cdots + x_n$, where each $0 \neq x_k \in S_{i_k}$ and $S_{i_1}, \ldots, S_{i_n}$ are distinct summands in the direct sum decomposition. In particular, consider the projection $\pi : M \twoheadrightarrow S_{i_1}$. Then, $\pi|_S : S \to S_{i_1}$ is an isomorphism.[52] □

52: Use Schur's lemma. We know $\pi(x) = x_1 \neq 0$.

For the finiteness aspect of the proposition, we use the lemma. If S is a simple submodule and R is semi-simple, then S is isomorphic to a submodule of R. The lemma says $S \simeq S_k$ for some $k = 1, \ldots, n$.

Lemma 5.6.5 *Suppose $S = S \oplus N$ for S simple. Suppose further that $S' \subseteq M$ is simple with $S' \not\subseteq N$. Then, the tautological map yields*

$$S' \oplus N \xrightarrow{\sim} M.$$

Plus, $S \simeq S'$.

Proof. We have that $S' \cap N = 0$, as S' is simple and $S' \not\subseteq N$. First, let $\pi : M \twoheadrightarrow S$ be the projection. Then, $\ker \pi = N$. We note that $\pi|_{S'} : S' \to S$ is an isomorphism, again by Schur's lemma. Given $x \in M$, write $x = x_1 + x_2$, where $x_1 \in S$ and $x_2 \in N$. Since $\pi|_{S'} : S' \to S$ is an isomorphism, there exists $y_1 \in S'$ such that $\pi(y_1) = x_1$. Observe $y_2 := x_1 - y_1 \in \ker \pi = N$. Thus, $y_1 \in S$ and $y_2 + x_2 \in N$, so

$$y_1 + (y_2 + x_2) = y_1 + x_1 - x_1 + x_2 = x,$$

so $S' + N = M$. Therefore,

$$S' \oplus N \xrightarrow{\sim} M.$$

□

Proposition 5.6.6 *If we can write*

$$M = \bigoplus_{i=1}^{m} S_i = \bigoplus_{j=1}^{n} S'_j.$$

where the S_i, S'_j are simple submodules, then $m = n$ and there exists $\sigma \in S_m$ so that $S_i \simeq S'_{\sigma(j)}$.[53]

53: That is, these simple direct sum decompositions are isomomrphic up to reordering. We only show this for the finite case, but it is true for *infinite* coproducts too.

Proof. We perform induction on $\min(m, n)$. The base case is 0. Consider $1 \leq m \leq n$. Write $M = S'_1 \oplus N$, where $N = \bigoplus_m S'_j$. There exists an i so that $S_i \not\subseteq N$. Without loss of generality (we use reordering), suppose $i = 1$. Then, $S_1 \not\subseteq N$. By the lemma, $S_1 \oplus N \xrightarrow{\sim} M$ and $S_1 \simeq S'_1$. We also ahve that $M \simeq S_1 \oplus N'$, where $N' := \bigoplus_n S_i$. Yet, $N \simeq M/S_1 \simeq N'$, so

$$\bigoplus_{i=2}^{m} S_i \simeq \bigoplus_{j=2}^{n} S'_j.$$

By induction, $m - 1 = n - 1$, and

$$\{S_i\} \xrightarrow{\sim} \{S'_j\}$$

up to reordering. □

Example 5.6.3 (Group Ring Modules) Let $\mathbb{F}$ be a field and G be a finite group where $|G| = n < \infty$. Define $R := \mathbb{F}[G]$. What are R-modules?[54] Well, they are precisely "representations of G." That is, let $(\mathscr{V}, \rho)$, where $\mathscr{V}$ is an $\mathbb{F}$-vector space and

54: For this aside, G does not have to be finite.

$$\rho : G \to \mathrm{Aut}_{\mathbb{F}}(\mathscr{V}).$$

Let

$$r = \sum_{g \in G}^{\text{finite}} a_g[g],$$

where $a_g \in \mathbb{F}$. Then, with $v \in \mathscr{V}$, we get

$$rv = \sum_{g \in G}^{\text{finite}} a_g \rho_g(v) \in \mathscr{V}.$$

For instance, if $G = C_n \langle x | x^n \rangle$, then $\mathbb{F}[G] \ni a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. We get an automorphism $\rho : G \to \mathrm{GL}_n(\mathbb{F})$, where $\mathscr{V} = \mathbb{F}^n$. We get

$$(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})(v) = \sum a_k \rho_{x^k}(v).$$

For instance, take the *regular representation*, taking $\mathscr{V} = R = \mathbb{F}[G]$. This has a basis given by group elements in G. If we take our basis $\mathbb{F}[G] = \mathbb{F}\{[g], g \in G\}$, then $\rho : G \to \mathrm{Aut}_{\mathbb{F}}(\mathscr{V})$. If $h \in G$, then $\rho_h([g]) := [hg]$. As an example, take $G := C_4 = \{e, x, x^2, x^3\}$. Then,

$$\mathscr{V} = \mathbb{F}[G] = \mathbb{F}\{[e], [x], [x^2], [x^3]\} \simeq \mathbb{F}^4.$$

We have

$$\rho_x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Proposition 5.6.7 *If G is finite with $|G| = n$ and $n^{-1} \in \mathbb{F}$.*[55] *Then, $\mathbb{F}[G]$ is semi-simple. As a consequence, every G-representation over $\mathbb{F}$ (every $\mathbb{F}[G]$-module) is a coproduct of irreducible representations (simple $\mathbb{F}[G]$-modules).*

55: Recall, we have a ring homomorphism

$$\mathbb{Z} \to \mathbb{F}$$

with $1 \mapsto 1$ and $n \mapsto$ "n". Then, if $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, this is always true. If $\mathbb{F} = \mathbb{F}_p$, then it is true only if $p \nmid n$.

Proof. Let $R := \mathbb{F}[G]$. Suppose we are given an R-module M and an R-submodule $N \subseteq M$. We want to show there exists an R-module map $r : M \to N$ such that $r|_N = \mathrm{id}_N$.[56] Note that $N \subseteq M$ is an $\mathbb{F}$-subspace, so there exists an $\mathbb{F}$-linear retraction $\psi : M \to N$ so that $\psi|_N = \mathrm{id}_N$. Define $\varphi : M \to N$ by

$$\varphi(x) := \frac{1}{|G|} \sum_{g \in G} [g]\psi([g^{-1}]x).$$

56: Remember, finding a retraction is the same as finding a summand.

We claim that φ is precisely the retraction we are looking for. Note the inclusion of $\varphi(M) \subseteq N$.

We first want to show that φ is an R-module map. Second, we want to show that $\varphi|_N = \mathrm{id}_N$.

Pick $h \in G$. We already know φ is $\mathbb{F}$-linear, so we just need to show

$$\varphi([h]x) = \frac{1}{|G|} \sum_{g \in G} [g]\psi([g^{-1}h]x).$$

Re-index with $g = hg'$. Then,

$$\frac{1}{|G|} \sum_{g \in G} [hg']\psi([(hg')^{-1}h]x) = [h]\varphi(x).$$

Recall that $x \in N$ implies $[g]x \in N$.

We compute,

$$\varphi(x) = \frac{1}{|G|} \sum_{g \in G} [g]\psi([g^{-1}]x) = \frac{1}{|G|} x = x,$$

so $\varphi|_N = \mathrm{id}_N$. □

Let R be a ring and take N, M to be R-modules. Write

$$N = \bigoplus_{j=1}^{n} N_j \quad \text{and} \quad M = \bigoplus_{i=1}^{m} M_i.$$

The idea to form a homomorphism $f : N \to M$, considering the vectors

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Proposition 5.6.8 *Under the identification above, any R-module homomorphism $f : N \to M$ can be written as (f_{ij}) as an $m \times n$ matrix with $f_{ij} \in \operatorname{Hom}_R(N_j, M_i)$. That is,*

$$f(x) = \begin{pmatrix} f_{11}(x_1) + \cdots + f_{1n}(x) \\ \vdots \\ f_{m1}(x_1) + \cdots + f_{mn}(x_n). \end{pmatrix}$$

We can interpret

$$P \xrightarrow{g} N \xrightarrow{f} M$$

as matrix multiplication $(g_{kj})(f_{ij})$.[57]

57: That is, our method of writing matrices in linear algebra *actually* works because of the direct sum decomposition: *not* because we are dealing with vector spaces.

Theorem 5.6.9 (Artin-Wederburn) *Every semi-simple ring is isomorphic to one of the form*

$$R = \prod_{k=1}^{r} \mathbb{M}_{n_k}(D_k),$$

where $D_1, \ldots, D_r$ are division rings, taking $n_k \geq 1$ and $r \geq 0$.

Proof. We know that R is semi-simple, so we can write

$$R = \bigoplus_{k=1}^{n} S_k,$$

where the $S_k \subseteq R$ are simple submodules. Note that

$$R^{\text{op}} \simeq \operatorname{End}_R(R) = \operatorname{Hom}_R(R, R).$$

Let $a \in R$, and define $\varphi_a : R \to R$ by $\varphi_a(x) := xa$. We claim that φ_a is a map of left modules. Let $b, x \in R$. Then,[58]

58: If we had multiplied a on the left, then it would *not* be a map of left modules (though, it would be one of right modules).

$$\varphi_a(bx) = (bx)a = b(xa) = b\varphi_a(x).$$

Yet,

$$\varphi_a(\varphi_b(x)) = \varphi_a(xb) = (xb)a = x(ba) = \varphi_{ba}(x),$$

as $\varphi_a \circ \varphi_b = \varphi_{ba}$. We have an isomorphism of rings $R^{\text{op}} \simeq \operatorname{End}_R(R)$. Now, we can precisely write

$$\operatorname{End}_R(R) \xrightarrow{\sim} \{f_{ij} \in \operatorname{Hom}_R(S_j, S_i)\}.$$

Schur's lemma tells us that if S, S' are simple, then

$$\operatorname{Hom}(S, S') \simeq \begin{cases} 0, & S \not\simeq S' \\ D, & S \simeq S', \end{cases}$$

where D is a division ring. We will now write

$$R \simeq \bigoplus_{k=1}^{n} S_k^{\oplus n_k}.$$

Each of the S_k are simple, where $S_i \not\simeq S_j$ if $i \neq j$, but we can take $n_k \geq 1$. Using our new form of R, we have that[59]

$$R^{\mathrm{op}} \simeq \mathrm{End}_R(R) \simeq \prod_{k=1}^{n} \mathrm{End}_R(S_k^{\oplus n_k}) = \prod_{k=1}^{n} \mathbb{M}_{n_k \times n_k}(D_k).$$

□

59: Per Schur's, we take $D_k := \mathrm{End}_R(S_k)$. Note that

$$\mathbb{M}_k(D) \simeq \mathbb{M}_k(D^{\mathrm{op}}).$$

Example 5.6.4 (Complex Group Rings) Consider $\mathbb{C}[G]$. We can always write

$$\mathbb{C}[G] \simeq \prod_{k=1}^{n} \mathbb{M}_{n_k}(\mathbb{C}),$$

where $|G| = n < \infty$. Note that if we have a division ring $D \neq \mathbb{C}$ and $\mathbb{C} \subseteq \mathrm{Center}(D)$, we can pick $x \in D \setminus \mathbb{C}$. We can consider the ring $R := (\mathbb{C}, x)$. Thus, R is commutative. It turns out, it is really hard to have larger division rings containing $\mathbb{C}$, since it is algebraically closed. Putting a finite dimension restriction on D forces equality with $\mathbb{C}$.

Particular Domains and Modules 6

We now return to our standard progression, approaching principal ideal domains, which have a very satisfying theory. Hereafter, all rings will be commutative and unital.

6.1 Preliminaries

We have a unique ring homomorphism sending $1 \mapsto 1$. Take $\varphi : \mathbb{Z} \to R$, where $\ker \varphi = (p)$. For instance, if $R = \mathbb{Z}/4$, then $p = 4$. If $R = \mathbb{F}$ is a field (or domain), then $\ker \varphi \subseteq \mathbb{Z}$ is a prime ideal. Either p is a prime number or $p = 0$.

Definition 6.1.1 (Characteristic) *We define the characteristic of a field to be*

$$\operatorname{char} \mathbb{F} = p,$$

as above. For instance, $\operatorname{char}(\mathbb{Q}, \mathbb{R}, \mathbb{C}) = 0$ *and* $\operatorname{char}(\mathbb{Z}/p) = p$.

Now, let $R_1, \ldots, R_n$ be rings. We can build the product ring

$$R := R_1 \times \cdots \times R_n.$$

Let $A, B \subseteq R$ be ideals. We get

$$\begin{aligned} R &\xrightarrow{\varphi} R/A \times R/B \\ r &\longmapsto (r + A, r + B). \end{aligned}$$

We have that φ is a ring homomorphism, but it is *also* an R-module homomorphism.[1] Clearly, $\ker \varphi = A \cap B$. In fact, we get a homomorphism $\overline{\varphi} : R/A \cap B \to R/A \times R/B$ is an injection. If A, B are ideals, recall that we write $A + B$ to be the set of pairwise sums. We also define

$$AB := \{a_1 b_1 + \cdots + a_k b_k : a_i \in A, b_j \in B, k \geq 0\} \subseteq R,$$

which is an ideal.[2] If we have two sets of generators $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_n)$, then

$$A + B = (a_1, \ldots, a_m, b_1, \ldots, b_n)$$

and

$$AB = (\ldots, a_i b_j, \ldots).$$

Definition 6.1.2 (Comaximal) *We say $A, B \subseteq R$ are comaximal (or coprime) if $A + B = R$. Equivalently, A, B are comaximal if there exists an $a \in A$ and $b \in B$ so that $a + b = 1$.*

1: When is φ an isomorphism? There is no reason to generally believe that φ is a surjection.

2: Note that this is not the product set, which usually is not an ideal.

Example 6.1.1 Let $(a), (b) \subseteq \mathbb{Z}$. We have that $(a), (b)$ are comaximal if and only if $\gcd(a, b) = 1$.[3]

3: This is why you will hear comaximal referred to as coprime.

Proof. By the standard lemma, $(a) + (b) = (d)$, where $d = \gcd(a, b)$, but $(1) = R$. □

Theorem 6.1.1 (Chinese Remainder Theorem) *If $A, B \subseteq R$ are comaximal ideals, then $A \cap B = AB$. We have that φ induces an isomorphism*[4]

$$R/AB \xrightarrow{\sim} R/A \times R/B.$$

4: This is both an isomorphism of rings and of R-modules.

Proof. First, $AB \subseteq A \cap B$ via the obvious inclusion. Conversely, if $x \in A \cap B$, then use $1 = a + b$ via comaximality. We get

$$x = x(a + b) = xa + xb \in BA, AB,$$

so $A \cap B \subseteq AB$. We know we have an injection

$$R/AB = R/A \cap B \to R/A \times R/B$$

given by $r \mapsto (r + A, r + B)$. Is it surjective. Well, consider $(\overline{r}_1, \overline{r}_2) \in R/A \times R/B$. Lift to elements $r_1, r_2 \in R$. Using $1 = a + b$ for some $a \in A$ and $b \in B$, set

$$r := r_2 a + r_1 b,$$

and modulo A we get $r + A = r_2 a + r_1 b + A = r_1 b + A$. We also know that $b = 1 - a \equiv 1 \pmod{A}$. We can write $r = r_2 a + r_1 b = r_2 a - r_1 a + r_1$, so $r \equiv r_1 \pmod{A}$. Likewise, $r \equiv r_2 \pmod{B}$. Thus, $\overline{\varphi}$ is an isomorphism. □

Example 6.1.2 If $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, then we get a ring isomorphism

$$\mathbb{Z}/(ab) \xrightarrow{\sim} \mathbb{Z}/a \times \mathbb{Z}/b.$$

Proposition 6.1.2 *Let $A_1, \ldots, A_n \subseteq R$ be pairwise comaximal.*[5] *Then,*

$$A_1 \cdots A_n = A_1 \cap \cdots \cap A_n$$

and

$$R/(A_1 \cdots A_n) \xrightarrow{\sim} (R/A_1) \times (R/A_2) \times \cdots \times (R/A_n).$$

5: That is, $A_i + A_j = R$ if $i \neq j$.

Proof. Proceed by induction on n. The base case of $n = 2$ is the Chinese Remainder Theorem. For $n \geq 3$, set $A = A_1$, $B = A_2 \cdots A_n$. We claim that A, B are comaximal, and we can continue the argument from there. For each $k = 2, \ldots, n$, there exists $x_k \in A_1, a_k \in A_k$ so that $1 = x_k + a_k$. Then,

$$a = (x_2 + a_2)(x_3 + a_3) \cdots (x_n + a_n),$$

which we can expand to

$$\underbrace{(a_2 \cdots a_n)}_{B} + x_2(\text{stuff}) + x_3(\text{stuff}) + \cdots + x_n(\text{stuff}),$$

and the latter terms are all in $A = A_1$. Thus, A, B are comaximal. $\square$

Example 6.1.3 If we again take $R := \mathbb{Z}$,

$$\mathbb{Z}/(p_1^{k_1} \cdots p_d^{k_d}) \xrightarrow{\sim} \mathbb{Z}/(p_1^{k_1}) \times \cdots \times \mathbb{Z}/(p_d^{k_d}),$$

where the p_i are distinct primes.

6.2 Euclidean Domains and PIDs

Note that, at least within textbook literature, the definition of Euclidean domains is rather inconsistent. Morally, they reflect the same idea.

Definition 6.2.1 (Euclidean Domain) *A Euclidean domain is a commutative domain R with unity so that there exists a function*[6]

$$N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

such that for all $a, b \in R$ and $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $N(r) < N(b)$.[7]

6: We call this function a norm.

7: The idea is that in $\mathbb{F} = \mathrm{Frac}(R)$, $a/b = q + r/b$.

Example 6.2.1

(a) Let $R := \mathbb{Z}$ and $N(a) = |a|$.
(b) Let $R := \mathbb{F}[x]$ and $N(f) := \deg f$.[8]
(c) Let $R := \mathbb{Z}[i]$ and $N(a + bi) = |a + bi|^2 = (a + bi)(a - bi) = a^2 + b^2$. In this case, note that $N(\alpha\beta) = N(\alpha)N(\beta)$.[9]
(d) Let $R := \mathbb{Z}[\sqrt{-5}]$. The obvious guess for N is $N(a + b\sqrt{-5}) = a^2 + 5b^2$. This does *not* satisfy the definition.

8: We use polynomial long division.

9: See 418 notes for the proof. It is a simple geometric proof using the interger lattice in $\mathbb{C}$.

Definition 6.2.2 (Principal Ideal Domain) *A principal ideal domain (PID) is a domain so that every ideal is principal.*

Proposition 6.2.1 *Euclidean domains are PIDs.*

Proof. Let R be a Euclidean domain with $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Let $(0) \neq I \subseteq R$ be an ideal. There exists a $d \in I$ such that $a \neq 0$. We can pick any $d \in I \setminus \{0\}$ for which $N(d)$ is minimized. We claim that $I = (d)$. Clearly, $(d) \subseteq I$. Let $a \in I$. There exist $q, r \in R$ such that $a = qd + r$, where either $r = 0$ or $N(R) < N(d)$. Note that $r = a - qd \in I$, but either $r = 0$ so $a = qd \in (d)$, or $N(r) < N(d)$, which contradicts minimality of $N(d)$. $\square$

Using this implication, some examples of PIDs are $\mathbb{Z}, \mathbb{F}[x], \mathbb{F}, \mathbb{Z}[i]$. We also have that $\mathcal{O}_{\mathbb{Q}[\sqrt{-3}]}$ is a Euclidean domain.

Definition 6.2.3 (Associates) *Let R be a domain. We say $a, b \in R$ are associates if there exists a unit $u \in R^\times$ such that $b = ua$.*[10]

10: This is an equivalence relation.

Definition 6.2.4 (Divides) *We say $a \mid b$ (a divides b) if there exists a $c \in R$ such that $b = ac$.*

Remark 6.2.1 We have that a, b are associates if and only if $(a) = (b)$.

Remark 6.2.2 We have that $a \mid b$ if and only if $(a) \supseteq (b)$.[11]

11: Equivalently, $b \in (a)$.

Definition 6.2.5 (GCD) *Let $a, b \in R$. A GCD (greatest common divisor) of a, b is $d = \gcd(a, b) \in R$ such that*

(i) $d \mid a$ and $d \mid b$.
(ii) if $e \in R$, $e \mid a$ and $e \mid b$, then $e \mid d$.[12]

12: That is, (d) is minimal among principal ideals which contain a, b.

Corollary 6.2.2 *The GCD is unique up to associates.*

Proposition 6.2.3 *If R is a PID, then GCDs always exist. In fact, $d = \gcd(a, b)$ if and only if $(a, b) = (d)$.*

Proposition 6.2.4 *In a PID, every nonzero prime ideal is maximal.*

Proof. Let $p \in R \setminus \{0\}$. We have that (p) is prime if and only if $R/(p)$ is a domain. Additionally, (p) is maximal if and only if $R/(p)$ is a field. Consider a prime ideal $(0) \neq (p) \subsetneq R$. We want to show $(p) \subseteq (a) \subseteq R$, then either $(a) = (p)$ or $(a) = R$. We will show $(p) \subsetneq (a) \subseteq R$ implies $(a) = R$. We do have that $a \notin (p) \subseteq (a)$, but $p \in (a)$, so $p = ab$ for some $b \in R$. Either $a \in (p)$ or $b \in (p)$, but $a \notin (p)$, so $b \in (p)$. Thus, $b = cp$ for some $c \in R$, meaning $p = ab = acp$, therefore $1 = ac$. Thus, $a \in R^\times$, meaning $(a) = R$. □

Proposition 6.2.5 *$\mathcal{O} := \mathbb{Z}[\sqrt{-5}]$ is not a PID.*

Proof. Define
$$I := (3, 2 + \sqrt{-5}).$$
Using the norm function,[13] $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha) = 0$ if and only if $\alpha = 0$. If $1 \in I$, then $1 = 3\alpha + (2 + \sqrt{-5})\beta$. We can multiply through to get
$$2 - \sqrt{-5} = 3(2 - \sqrt{-5})\alpha + 9\beta \in (3).$$
We have that $2 - \sqrt{-5} \notin (3)$, a contradiction, so $1 \notin I$. In $\mathcal{O}$, as above, $N(\alpha) = 1$ if and only if $\alpha = \pm 1$. We have that $N(\alpha) = a^2 + 5b^2 = 1$, so $\mathcal{O}^\times = \{\pm 1\}$. Suppose I is principal. Then, we can write
$$3 = (a + b\sqrt{-5})\alpha$$
and
$$2 + \sqrt{-5} = (a + b\sqrt{-5})\beta$$

13: This is not in the Euclidean sense.

for some $\alpha, \beta \in \mathbb{O}$. Take the norm:

$$9 = (a^2 + 5b^2)N(\alpha)$$

and

$$9 = (a^2 + 5b^2)N(\beta),$$

so $a^2 + 5b^2 \mid 9$. Note that since the norm uses squares, we only have a few choices: $\{1, 9\}$. Therefore, either $a^2 + 5b^2 = 1$, so $a^2 + 5b^2 \in \mathbb{O}^\times$, meaning $I = \mathbb{O}$, a contradiction. If $a^2 + 5b^2 = 9$, then $N(\alpha), N(\beta) = 1$, so $\alpha, \beta \in \{\pm 1\}$. Thus, $3 = (\pm 1)(a + b\sqrt{-5})$ and $2 + \sqrt{-5} = \pm(a + b\sqrt{-5})$, which is a contradiction. Thus, I is not principal. □

Proposition 6.2.6 *Let R be a domain. Elements a of R can be divided into 4 non-overlapping groups:*

(i) $a = 0$.
(ii) *a is a unit.*
(iii) *a is reducible.*[14]
(iv) *a is irreducible.*[15]

14: That is, $a \neq 0$, not a unit, and if $a = bc$ for some b, c which are not units.

15: This means $a \neq 0$, a is not a unit, and is not reducible.

We can restate these groups in terms of ideals, and prove the irreducibility equivalence.

Proposition 6.2.7

(i) $(a) = \{0\}$.
(ii) $(a) = R$.
(iii) *anything else*
(iv) $(a) \neq 0$ *and* (a) *is maximal among proper principal ideals.*

Proof. Suppose a is irreducible. Then, $a \neq 0$ and $a \notin R^\times$. Suppose $(a) \subsetneq (b) \subseteq R$. Then, $a = bc$ for some $c \in R \setminus R^\times$. Yet, since a is irreducible, b is a unit, so $(b) = R$. Thus, (a) is maximal among proper principal ideals. Conversely, suppose (a) is maximal among proper principal ideals. If $a = bc$, with $b, c \notin R^\times$, then $(a) \subsetneq (b) \subsetneq R$. This is a contradiction to maximality, so a is not reducible. □

Example 6.2.2 Let $R := \mathbb{F}$ be a field. We have

(i) 0.
(ii) $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.
(iii) $\varnothing$.
(iv) $\varnothing$.

Example 6.2.3 Let $R := \mathbb{Z}$. Then,

(i) 0.
(ii) $\mathbb{Z}^\times = \{\pm 1\}$.
(iii) composites.
(iv) $\pm p$ where p is prime.

Example 6.2.4 Let $R := \mathbb{F}[x]$, where $\mathbb{F}$ is a field. We get

(i) 0.
(ii) $\mathbb{F}^{\times} \subseteq \mathbb{F}[x]$.
(iii) f reducible.
(iv) f irreducible polynomials.[16]

16: We need nonzero, non-unit, $f \neq gh$ for non-constant g, h of smaller degree strictly.

Example 6.2.5 If we take a look at $\mathbb{C}[x]$, then irreducibles are precisely of the form $(x-a)$, up to units, where $a \in \mathbb{C}$. On the other hand, if we look at $\mathbb{R}[x]$, then irreducibles are either $(x-a)$ for $a \in \mathbb{R}$ or (x^2+bx+c) for $b, c \in \mathbb{R}$, where $b^2 - 4c < 0$.

Remark 6.2.3 If we have one irreducible dividing another, they must be associates.

Definition 6.2.6 (Prime Element) *We say $p \in R$ is prime if $p \neq 0$ and (p) is a prime ideal. In other words, $p \neq 0$ and if $p \mid ab$, then $p \mid a$ or $p \mid b$.*[17]

17: We force $p \notin R^{\times}$.

Proposition 6.2.8 *Let R be a domain. Every prime element is irreducible.*

Proof. Let p be prime. Then, $(p) \subsetneq (a) \subseteq R$. Thus, $p = ab$ for some $b \in R$ with $b \notin R^{\times}$. In turn, $p \mid a$ or $p \mid b$, but p cannot divide a since $(p) \subsetneq (a)$, so $p \mid b$. Thus, $b = cp$ for some $c \in R$. Then, $p = ab = acp$, so $1 = ac$, meaning $a, c \in R^{\times}$, and $a \in R^{\times}$ implies $(a) = R$. Thus, (p) is maximal among principal ideals, so it is irreducible. □

Example 6.2.6 Consider $R := \mathbb{Z}[\sqrt{-5}]$. We have $3 \in R$. If we have $3 = \alpha\beta$, then $N(3) = N(\alpha)N(\beta) = 9$, but $N(\alpha) \neq 3$. Thus, at least one of the RHS is 1, so one is a unit. As such, 3 is irreducible. On the other hand, it is *not* prime. We can factor $3^2 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$. Then, $3 \mid \alpha\beta$, but $3 \nmid \alpha$ and $3 \nmid \beta$.[18]

18: We have

$$(3) = \{3a + 3b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Proposition 6.2.9 *If R is a PID, then prime is the same as irreducible.*

Proof. We have already shown the forward direction. Conversely, if (a) is irreducible, then (a) is maximal among proper principal ideals. Yet, all ideals are principal, so (a) is maximal. Thus, $R/(a)$ is a field, and in particular, $R/(a)$ is prime, so a is prime. □

6.3 Unique Factorization Domains and Fermat

Definition 6.3.1 (Unique Factorization Domain) *A unique factorization domain (UFD) is a domain R such that for all $R \in R \setminus (\{0\} \cup R^\times)$,*

(i) there exists $r = p_1 p_2 \cdots p_n$, where the p_i are irreducible and $n \geq 1$.
(ii) this factorization is unique up to reorderings and units.

Remark 6.3.1 The latter statement is saying if $r = p_1 \cdots p_n = q_1 \cdots q_m$ with p_i, q_i are irreducible, then $m = n$ and there exists $\sigma \in S_N$ such that $p_k \sim_{\text{units}} q_{\sigma(k)}$.

Remark 6.3.2 That is, $(r) = (p_1) \cdots (p_n)$ with p_i irreducible, which is unique up to reordering.[19]

19: These are products of ideals, as discussed earlier.

Definition 6.3.2 (ACC for Principal Ideals) *We say R has the ACC for principal ideals if for $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, then with $\{I_k\}_{k \in \mathbb{Z}_+}$, $I_k = (a_k)$ implies there exists n such that $I_k = I_n$ for all $k \geq n$.*[20]

20: That is, every chain stabilizes, as you might expect.

Lemma 6.3.1 *Every PID has the ACC for principal ideals.*

Proof. Let

$$(b) = J := \bigcup_{k \geq 1} I_k \subseteq R,$$

so there exists n such that $b \in I_n$, so $J = I_n$. □

Theorem 6.3.2 *PIDs are UFDs.*

Proof. Let R be a PID. We want to show every nonzero, non-unit in R has $r = p_1 \cdots p_n$ for p_i irreducible. Suppose $a \in R \setminus (\{0\} \cup R^\times)$ for which this is not true.[21] Then, a is not irreducible, so a is reducible. Then, there exists a factorization $a = a'b$ and $a, b \notin \{0\} \cup R^\times$. Thus, a' also is not a product of irreducibles. We have $a_1 = a_2 b_2$ bad, so a_2 is bad and $b_2 \notin R^\times$. Continue iterating in this way. Then, we get a a chain of principal ideals

21: Call this property "bad."

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq \cdots \subseteq R,$$

a contradiction to the ACC.[22] We now need to prove uniqueness,m which uses that irreducibles are prime (which is true in a PID). Suppose $a = p_1 \cdots p_n = q_1 \cdots q_m$, where p_i, q_i are irreducible. Of course, $p_1 \mid q_1 q_2 \cdots q_m$, so $p_1 \mid q_j$ for some j. Reorder so that $j = 1$. Thus, $p_1 \sim_{\text{units}} q_1$. What we get here is that $q_1 = p_1 u$ for some $u \in R^\times$, so canceling p_1 gives us

22: In practice, this means the process *must* stop if we keep pulling off elements.

$$(up_2) \cdots p_n = q_2 \cdots q_m,$$

and induction by the number of factors tells us $n = m$ and the factors are the same up to reordering and units. □

Example 6.3.1 Let $\mathcal{O} := \mathbb{Z}[i]$. This is a PID, so it is UFD. What are the irreducible elements? Well, recall that we have the norm $N : \mathcal{O} \to \mathbb{Z}_{\geq 0}$ so that $N(a + bi) = a^2 + b^2$, which is multiplicative. We also have $\mathcal{O}^\times = \{\pm 1, \pm i\}$. Let us start with a lemma.

Lemma 6.3.3 *Let $\alpha \in \mathcal{O}$ with $N(\alpha) = p$, a prime in $\mathbb{Z}$. Then, α is irreducible in $\mathcal{O}$.*

Proof. If $\alpha = \beta\gamma$, then since norm is multiplicative, either β or γ is a unit in $\mathcal{O}$. $\square$

For instance, $N(2 \pm i) = 2^2 + 1^2 = 5$, so $2 \pm i$ are both irreducible, yet they are not associates.[23] Algebraic number theorists will say "irreducibles in $\mathbb{Z}[i]$ sit over irreducibles in $\mathbb{Z}$."

23: Just check products of the four units.

Proposition 6.3.4 *If R is commutative, unital, $S \subseteq R$ is unital, and $P \subseteq R$ is a prime ideal, then $S \cap P \subseteq S$ is a prime ideal.*[24]

24: We call this a "restricted ideal."

Proof. Suppose $a, b \in S$ so that $ab \in S \cap P$. Yet, $P \subseteq R$ is prime, so either $a \in P$ or $b \in P$, but both are in S so we win. $\square$

Alternatively, we have a subring inclusion $S/(S \cap P) \subseteq R/P$, where the latter is a domain, and subrings of domains are domains.

Proposition 6.3.5 *Let $p \in \mathbb{Z}$ be a prime number. Let $\alpha \in \mathcal{O} = \mathbb{Z}[i]$ be an irreducible element. The following are equivalent:*[25]

(i) *α is a divisor of p in $\mathcal{O}$.*
(ii) *$p\mathbb{Z} = \alpha\mathcal{O} \cap \mathbb{Z}$.*

25: Algebraic number theorists say that "α lies over p."

Proof. Since α is irreducible in $\mathcal{O}$, we have that $(\alpha) = \alpha\mathcal{O}$ is maximal in $\mathcal{O}$. Thus, it is a prime ideal in $\mathcal{O}$. Then, by the previous proposition, $\alpha\mathcal{O} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. We know that $\alpha\mathcal{O} \cap \mathbb{Z} = q\mathbb{Z}$ for some unique prime number q. Now, start with (i) $\Rightarrow$ (ii). If $\alpha \mid p$ in $\mathcal{O}$, then $p \in \mathcal{O} \cap \mathbb{Z} = q\mathbb{Z}$, so $p = q$. Conversely, if $q = p$, $p \in \alpha\mathcal{O}$, so $p = \alpha\beta$ for some $\beta \in \mathcal{O}$. $\square$

Remark 6.3.3 If $\alpha \in \mathcal{O}$ is irreducible and $\alpha\mathcal{O} \cap \mathbb{Z} = p\mathbb{Z}$, we can $p = \alpha\beta$ for $\beta \in \mathcal{O}$. Applying the field norm yields $p^2 = N(p) = N(\alpha)N(\beta)$. There are two cases, when $N(\alpha) = p$ and when $N(\alpha) = p^2$. If $N(\alpha) = p^2$, then $N(\beta) = 1$, so $\beta \in \mathcal{O}^\times$, so $\alpha \sim_{\text{units in } \mathcal{O}} p$. Thus, $\alpha \in \{\pm p, \pm pi\}$. Now, if $N(\alpha) = p$, then $N(\beta) = p$, so $p = \alpha\beta$ is an irreducible factorization of p in $\mathcal{O}$, meaning α, β are unique up to units. Note that if $\alpha = a + bi$, then

$$p = N(\alpha) = (a + bi)(a - bi),$$

so in this case, $\alpha, \beta \in \{a \pm bi\}$ up to units by unique factorization. Consequently, every irreducible α in $\mathcal{O}$ lies over a unique prime number $p \in \mathbb{Z}$. Exactly one of the following happens:

(i) $N(\alpha) = p^2$ and $\alpha \in \{\pm p, \pm pi\}$.

(ii) $N(\alpha) = p$ and $a^2 + b^2 = p = (a+bi)(a-bi)$.[26]

Corollary 6.3.6 *Let $p \in \mathbb{Z}$ be prime. We have that p factors nontrivially in $\mathbb{O}$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*[27]

Example 6.3.2 Let $p = 2 = 1^2 + 1^2$. Then, $p = (1+i)(1-i)$, which is an irreducible factorization. Note that $i(1-i) = 1+i$, so $1+i$ and $1-i$ are associates.

Example 6.3.3 Let $p = 3$, which is not a sum of squares. Then, 3 is irreducible in the Gaussian integers.

Example 6.3.4 Let $p = 5 = 2^2 + 1^2 = (2+i)(2-i)$. These are two irreducibles in $\mathbb{O}$ over 5 up to units.[28]

Remark 6.3.4 If $p = a^2 + b^2$. Then, $a + bi \sim_{\text{units}} a - bi$ if and only if $p = 2$.

Lemma 6.3.7 (Lagrange) *Let p be a prime of the form $p = 4m + 1$ for some $m \in \mathbb{Z}$. Then, there exists $n \in \mathbb{Z}$ such that $p \mid n^2 + 1$. That is, $n^2 \equiv -1 \pmod{p}$.*[29]

Proof. We proved this in the homework. □

Theorem 6.3.8 (Fermat) *If $p \in \mathbb{Z}$ is prime, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 2 \pmod{4}$ or $p \equiv 1 \pmod{4}$.*[30]

Proof. We know $2 = 1^2 = 1^2$, so assume p is an odd prime. If $p = a^2 + b^2$, then $p \equiv 0, 1, 2 \pmod{4}$, so $p \not\equiv -1 \pmod{4}$, as $a^2, b^2 \equiv 0, 1 \pmod{4}$. Thus, $p \equiv 1 \pmod{4}$ for odd p. Suppose $p \equiv 1 \pmod{4}$. By Lagrange's lemma, there exists an $n \in \mathbb{Z}$ such that $p \mid n^2 + 1$. We can factor $n^2 + 1 = (n+i)(n-i)$ in $\mathbb{O}$. Thus,

$$p \mid n^2 + 1 = (n+i)(n-i) \quad \text{in } \mathbb{O}.$$

Suppose p is irreducible in $\mathbb{O}$, which is true if and only if p is prime in $\mathbb{O}$ (PID). Then, p dividing a product implies $p \mid n + i$ or $p \mid n - i$. Then, one of $n + i, n - i \in p\mathbb{O}$, which is impossible. Thus, p *cannot* be irreducible in $\mathbb{O}$. Thus, p is reducible in $\mathbb{O}$, so $p = (a+bi)(a-bi)$ for some irreducible $a \pm bi$ in $\mathbb{O}$. □

6.4 Torsion Modules, Independence, and Rank

Let M be an R-module, where R is a domain.

26: That is, p is not irreducible in $\mathbb{O}$.

27: Using the field norm, this also gives us the factorization for free.

28: Note that these are not associates.

29: To clarify, $-1 \in \mathbb{F}_p$ has a square root.

30: That is, not if $p \equiv -1 \pmod{4}$.

Definition 6.4.1 (Torsion) *We say that $x \in M$ is torsion if there exists an $r \in R \setminus \{0\}$ such that $rx = 0$.*[31]

31: That is, $R \to Rx \subseteq M$ where $r \mapsto rx$ has nontrivial kernel.

Definition 6.4.2 (Set of Torsion Elements) *We define*

$$M_{tors} := \{x \in M : x \text{ is torsion }\}.$$

Definition 6.4.3 (Torsion Module) *We say that M is torsion if $M = M_{tors}$.*

Definition 6.4.4 (Torsion Free) *We say that M is torsion free if $M_{tors} = \{0\}$.*

Lemma 6.4.1 *$M_{tors} \subseteq M$ is a submodule and M/M_{tors} is torsion free.*

Proof. The proof is the same as in the case of $R = \mathbb{Z}$, and $\mathbb{Z}$-modules are abelian groups. □

Lemma 6.4.2 *If $N \subseteq M$ is a submodule, then M/N is torsion if and only if for all $x \in M$ there exists $r \in R \setminus \{0\}$ such that $rx \in N$.*

Proof. The proof is obvious. □

Proposition 6.4.3 *A cyclic module $M = R/I$, is a torsion module if and only if $I \neq 0$.*

Proof. Suppose there exists $a \in I \setminus \{0\}$. Then, $a \cdot b \in I$, so $\overline{b} \in (R/I)_{\text{tors}}$. Conversely, if $I = 0$, then $M = R$, so $R_{\text{tors}} = 0$, because R is a domain. □

Example 6.4.1 If $R = \mathbb{F}$, a field, then if $\mathscr{V}$ is a $\mathbb{F}$-linear space, then $\mathscr{V}_{\text{tors}} = 0$. All vector spaces are torsion free.

Definition 6.4.5 (R-Linearly Dependent) *We say that $\{x_i\}_{i \in I}$ is R-linearly dependent if there exists*

$$\sum_{i \in I}^{\text{finite}} r_i x_i = 0,$$

where not all $r_i = 0$ (all but finitely many $r_i = 0$).[32]

32: The $r_i \in R$.

That is, if $\{x_1, \ldots, x_n\}_{i=1,\ldots,n}$, then R-dependence happens if and only if there exists $r_1, \ldots, r_n \in R$ with some $r_k \neq 0$ such that

$$r_1 x_1 + \cdots + r_n x_n = 0.$$

Definition 6.4.6 (R-Linearly Independent) *A set $\{x_i\}_{i \in I}$ is R-independent if it is not R-dependent.*

Remark 6.4.1 If $\{x_i\}$ is R-independent, then $x_i \neq x_j$ for $i \neq j$.

Note that R-independence is precisely equivalent to giving a map

$$\begin{aligned} \bigoplus_{i \in I} R &\xrightarrow{f} M \\ e_i &\longmapsto x_i \end{aligned}$$

which is *injective*.[33] If this is the case, we can consider the submodule $R\{x_i\} \subseteq M$, which is free.

33: The e_i are the standard basis elements.

Definition 6.4.7 (Maximally R-Independent) *We say that $S \subseteq M$ is maximally R-independent if both*

(i) it is R-independent.
(ii) if $S \subseteq T \subseteq M$ and T is R-independent, then $S = T$.

Example 6.4.2 The basis of a free module is always maximally R-independent.

Example 6.4.3 Take $0 \neq (a) \subseteq R$, then $\{a\}$ is R-independent.

Example 6.4.4 Let $R := \mathbb{Z}$ and take $M := \mathbb{Q}$ as a $\mathbb{Z}$-module. The subset $\{1\} \subseteq \mathbb{Q}$ is maximally $\mathbb{Z}$-independent.

Lemma 6.4.4 *Let $S \subseteq M$ be an R-independent subset. Then, S is maximally R-independent if and only if M/RS is a torsion module.*

Proof. Let $y \in M$. Look at the quotient image $\overline{y} = y + N \in M/N$, where $N = RS \subseteq M$. The element $\overline{y} \in M/N$ is torsion if and only if there exists $b \in R \setminus \{0\}$ such that $b\overline{y} = 0$. We can recast this as saying there exists $b \in R \setminus \{0\}$ with $a_1, \ldots, a_n \in R$ and $x_1, \ldots, x_n \in S$ such that $by = a_1x_1 + \cdots + a_nx_n$. Thus, $\overline{y}$ is torsion if and only if $y \in S$ or $S \cup \{y\}$ is R-dependent. Therefore, all $\overline{y} \in M/N$ are torsion if and only if S is maximally R-independent. $\square$

Example 6.4.5 Let $R := \mathbb{F}$, a field. The only torsion module is 0. We have that if $\mathcal{V} \in \mathsf{Mod}_{\mathbb{F}}$, then $S \subseteq \mathcal{V}$ is maximally $\mathbb{F}$-independent, which holds if and only if it is $\mathbb{F}$-linear independent and $\mathcal{V} = \mathbb{F}S$. This is true if and only if S is a basis of $\mathcal{V}$.

Proposition 6.4.5 *Every R-independent subset $S \subseteq M$ is contained in some maximally R-independent subset. In particular, every module has at least one R-independent subset.*[34]

34: Applying this to $R = \mathbb{F}$, this is precisely the statement that every vector space has a basis.

Proof. Use Zorn's lemma, applied to the poset of R-independent subsets which contain S. $\square$

Theorem 6.4.6 (Invariance of Rank) *Let M be an R-module over a domain. Let $S \subseteq M$ be a finite subset with $|S| = n$ such that $M/(RS)$ is torsion. Then, there exists a $T \subseteq S$ such that T is maximally R-independent, and every maximally R-independent subset of M has size equal to $|T| = m \leq n$.*[35]

35: The standard proof uses the replacement/ interchange theorem, which is usually used in linear algebra to discuss dimension. This is ugly, so we will use dimension, looking at the case of finitely generated free modules, and then look at the general case.

Definition 6.4.8 (Module Rank) *In the case of the theorem above, we define*

$$\operatorname{rank}(M) := \textit{ size of any } R\textit{-independent subset of } M.$$

Corollary 6.4.7 *Let $M := R^{\oplus n}$. Then,* $\operatorname{rank}(M) = n$*. If $R^{\oplus n} \simeq R^{\oplus m}$ is an isomorphism of R-modules, then $m = n$.*

Example 6.4.6 Let $R := \mathbb{F}$ be a field. If $\mathcal{V}$, an $\mathbb{F}$-linear space, has a spanning set S of size $n < \infty$, then S contains a basis T of size $m \leq n$, and every basis of $\mathcal{V}$ has size m.

Consider the special case $M := R^{\oplus m}$.

Lemma 6.4.8 *If $M = R^{\oplus m}$, then every R-independent subset S of M has size less than or equal to m, and such an S is maximally R-independent if and only if $|S| = m$.*

Proof. Define $\mathbb{F} := \operatorname{Frac}(R) \supseteq R$. We have $M = R^{\oplus m} \subseteq \mathcal{V} := \mathbb{F}^{\oplus m}$. This is an $\mathbb{F}$-vector space and an R-module. If $S \subseteq M$, and also $S \subseteq \mathcal{V}$, then S is R-independent in M if and only if S is $\mathbb{F}$-independent in $\mathcal{V}$. Similarly, S is maximally R-independent in M if and only if S is maximally $\mathbb{F}$-linearly independent in $\mathcal{V}$.[36] Now, we prove the claim. If $S = \{x_i\}_{i \in I} \subseteq M$ is R-independent, then

36: The lemma follows from linear algebra applied to $\mathcal{V}$.

$$\sum_{i \in I}^{\text{finite}} a_i x_i = 0$$

implies all $R \ni a_i \in 0$. Suppose

$$\sum_{i \in I}^{\text{finite}} c_i x_i = 0,$$

where $c_i \in \mathbb{F}$. Then, each $c_i = a_i/b_i$, where $a_i, b_i \in R$ and $b_i \neq 0$. Let $b = b_1 \cdots b_n$ for all nonzero c_i (the other $c_k = 0$ if $k \neq 1, \dots, n$). We can then rewrite the sum as

$$\sum_{i=1}^{n} (bc_i) x_i = 0,$$

with $bc_i \in R$, and R-independence tells us that all $bc_i = 0$, so all $c_i = 0$. Conversely, if S is $\mathbb{F}$-independent then S is R-independent is the same but easier. Now, it is trivial that if $S \subseteq M$ is maximally $\mathbb{F}$-independent, then S is maximally R independent. Suppose $S \subseteq M$ is maximally R-independent, but suppose further that there exists a $v \in \mathcal{V}$ with $v \notin S$ so that $S \cup \{v\}$ is $\mathbb{F}$-independent in $\mathcal{V}$. Then, there exists a $b \in R \setminus \{0\}$ such that $bv \in M$.[37] If $S \cup \{v\}$ is $\mathbb{F}$-independent, so is $bS \cup \{bv\} \subseteq M$, meaning

37: We have $v = (v_1, \dots, v_m) \in \mathbb{F}^{\oplus m}$.

$bS \cup \{bv\}$ is R-independent in M> Yet, bS is maximally R-independent by the following lemma, a contradiction. $\square$

Lemma 6.4.9 *If $S \subseteq M = R^{\oplus m}$ is maximally R-independent and if $b \in R \setminus \{0\}$, then bS is also maximally R-independent.*

Proof. S being R-independent implies bS is R-independent. Consider $RbS \subseteq RS \subseteq M$. If S is maximally R-independent, then M/RS is torsion. Also, RS/RbS is torsion, as for all $\overline{x} \in RS/RbS$ has $b\overline{x} = 0$. We claim that this means M/RbS is torsion. If $\overline{y} \in M/RbS$, then since m/RS is torsion, there exists $a \in R \setminus \{0\}$ such that $a\overline{y} \in RS$, but then $b(a\overline{y}) \in RbS$. Thus, $ba\overline{y} = 0$ for $ba \in R \setminus \{0\}$. $\square$

Corollary 6.4.10 *If $N \subseteq M$, then N, M/N are torsion, so M is torsion.*

Example 6.4.7 Remember, $\mathbb{Q}$ is a $\mathbb{Z}$-module. We have that $\operatorname{rank}(\mathbb{Q}) = 1$.

Proposition 6.4.11 (Finding Maximally R-Independent T) *Let T be any subset of S which is R-independent and has maximal size.*

Proof. Existence comes from the fact that $\varnothing$ is R-independent. If $T \subseteq S$ is maximal among subsets of S which are R-independent, then we claim that RS/RT is torsion. Well, RS/RT is generated as an R-module by the image of $S \setminus T$.[38] Let $x \in S \setminus T$. Then, $T \cup \{x\} \subseteq M$ is not R-independent, by the maximality of T.[39] Then, $a\overline{x} = 0$ in $RS/RT \subseteq M/RT$, so RS/RT is torsion. Consider $RS/RT \subseteq M/RT$. Well, $(M/RT)/(RS/RT) \simeq M/RS$. Since the submodule RS/RT is torsion and the quotient M/RS is torsion, we have that M/RT is torsion. Suppose $S, T \subseteq M$ such that T is maximally R-independent of size n and S is R-independent with $|S| = n + 1$. We will show a contradiction. Since T is maximally R-independent, M/RT is torsion. Take $S = \{x_1, \ldots, x_{n+1}\}$, then there exists $d \in R \setminus \{0\}$ such that $dS = \{dx_1, \ldots, dx_{n+1}\} \subseteq RT \simeq R^{\oplus n}$ and dS is also R-independent. Last time, we showed this is impossible. $\square$

38: We take the quotient image.

39: That is, there exists $ax = b_1 t_1 + \cdots + b_n t_n$, where $t_i \in T$, $a \neq 0$, and $a, b_i \in R$.

Corollary 6.4.12 *If R is a domain and $R^m \simeq R^n$ with $m, n \geq 0$, then $m = n$.*

Proof. We have that $\operatorname{rank}(R^n) = n$, and rank is an invariant. $\square$

Proposition 6.4.13 *Let M be a domain R-module. Take $N \subseteq M$ to be a submodule. If* $\operatorname{rank}(N) = n$ *is finite and* $\operatorname{rank}(M/N) = m$, *then* $\operatorname{rank}(M) = \operatorname{rank}(N) + \operatorname{rank}(M/N)$.

6.5 Annihilators

Let R be a unital ring and M be a left R-module.

Definition 6.5.1 (Annihilator) *We define the annihilator*

$$\operatorname{Ann}(M) := \{x \in R : xM = 0\} \subseteq R.$$

Proposition 6.5.1 *We have that* $\operatorname{Ann}(M) \subseteq M$ *is a two-sided ideal.*

Proof. We have that $0M = 0$. If $xM = 0 = yM$, then $(x + y)M = 0$. If $xM = 0$, then $xrM \subseteq xM$, so $xrM = 0$. Also, $r(xM) = r0 = 0$. □

Exercise 6.5.1 Prove that

$$\operatorname{Ann}(M) = \ker\left[R \to \operatorname{End}_{\mathbb{Z}}(M)\right].$$

Proposition 6.5.2 *If* $M \simeq N$*, then* $\operatorname{Ann}(M) = \operatorname{Ann}(N)$.[40]

40: The proof is short, but this is particularly intuitive.

Proof. If $\varphi : M \xrightarrow{\sim} N$ is an R-module isomorphism, then $x\varphi(m) = 0$ if and only if $xm = 0$. □

Proposition 6.5.3 *Let* $I \subseteq R$ *be a two-sided ideal. Then,* $\operatorname{Ann}(R/I) = I$.

Proof. If $x \in \operatorname{Ann}(R/I)$, then $x\overline{1} = \overline{0}$, $x1 \in I$ so $x \in I$. If $x \in I$, then for all $y \in R$, we have $xy \in I$, so $x\overline{y} = 0$. □

Remark 6.5.1 If $I \subseteq R$ is only a left ideal, we can have $\operatorname{Ann}(R/I) \subsetneq I$.

Example 6.5.1 Let $R := \mathbb{M}_2(\mathbb{F})$. Let $I := \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$ be a left ideal. Then, $\operatorname{Ann}(R/I) = 0 \neq I$.

Proposition 6.5.4 *Let* $I, J \subseteq R$ *be two-sided ideals. Then,* $R/I \simeq R/J$ *as left* R*-modules if and only if* $I = J$.[41]

41: A useful example is when R is commutative.

Proof. We have that the respective annihilators are isomorphic for R-modules, plus $\operatorname{Ann}(R/I) = I$. □

Corollary 6.5.5 *Let* R *be commutative with* M, N *cyclic as* $R0$*modules. Then,* $M \simeq N$ *as* R*-modules if and only if* $\operatorname{Ann}(M) = \operatorname{Ann}(N)$.

6.6 Modules Over PIDs

Now, let R be a PID. Then, for cyclic modules, we have $R/(a) \simeq R/(b)$ as R-modules if and only if $(a) = (b)$. That is, if $a \sim_{\text{units}} b$.

Proposition 6.6.1 (Cylic Modules) *There are three types of cyclic modules over a PID:*

(i) trivial: $R/(a) \simeq 0$ *for* $a \in R^{\times}$.
(ii) nontrivial torsion: $R/(a)$ *for* $a \neq 0, a \notin R^{\times}$.
(iii) free: $R/(0) \simeq R$.

Proposition 6.6.2 *Let R be a PID. Then, every finitely generated R-module is isomorphic to one of the form*[42]

$$M \simeq R/(a_1) \oplus \cdots \oplus R/(a_k).$$

42: That is, a finite direct sum of cyclic modules.

Remark 6.6.1 (Chinese Remainder Theorem) Factor

$$R \ni a = p_1^{k_1} p_2^{k_2} \cdots p_d^{k_d},$$

where $p_1, \ldots, p_d$ are distinct-up-to-units primes in R, the $k_1, \ldots, k_d \geq 1$, and $d \geq 0$. Then, $(a) = (p_1^{k_1})(p_2^{k_2}) \cdots (p_d^{k_d})$. Thus,

$$R/(a) \simeq R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_d^{k_d}).$$

Theorem 6.6.3 (Elementary Divisor) *Every finitely generated module over a PID R is isomorphic to one of the form*

$$M \simeq R^r \oplus R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_u^{k_u}),$$

where $r \geq 0, u \geq 0$, and $p_1, \ldots, p_u$ are primes in R and $k_i \geq 1$.[43] *Furthermore, this is unique in the sense that if we also have*

$$M \simeq R^{r'} \oplus R/(q_1^{\ell_1}) \oplus \cdots \oplus R/(q_v^{\ell_v})$$

with $r', v \geq 0$ and $q_1, \ldots, q_v$ are prime with $\ell_i \geq 1$, then $r = r'$, $v = v'$, and there exists a $\sigma \in S_v$ such that $p_i \sim_{units} q_{\sigma(i)}$ with $k_i = \ell_{\sigma(i)}$.

43: The p_i are not necessarily distinct.

We need to show uniqueness and existence.

Lemma 6.6.4 *If $M \simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$ with $a_k \neq 0$, then* $\operatorname{rank}(M) = r$.

Proof. We showed that $N \subseteq M$ implies $\operatorname{rank}(M) = \operatorname{rank}(N) + \operatorname{rank}(M/N)$. In particular, $\operatorname{rank}(N_1 \oplus N_2) = \operatorname{rank}(N_1) + \operatorname{rank}(N_2)$. Thus, the claim follows from the fact that rank is an isomorphism invariant: $\operatorname{rank}(R) = 1$ and $\operatorname{rank}(R/(a)) = 0$ if $a \neq 0$.[44] □

44: The rank is zero because it is a torsion module.

Now, let R be a commutative ring, M be an R-module, and $I \subseteq R$ be an ideal such that $I \subseteq \operatorname{Ann}_R(M)$. That is,

$$IM = \{x_1 m_1 + \cdots x_n m_n : x_i \in I, m_i \in M\} = 0.$$

We have that M/IM admits the structure of an R/I-module. Set $(r + I)m := rm$. Furthermore, if $M \simeq N$ as R-modules and $IM = 0$, then

$IN = 0$ and $M \simeq N$ as R/I-modules.

Example 6.6.1 Let $R := \mathbb{Z}$ and let M be an R-module such that $(p)M = 0$, where p is a prime. Then, M is also a module over $\mathbb{Z}/p = \mathbb{F}_p$. Then, it has an invariant $\dim_{\mathbb{F}_p} M$. The idea is that $\dim_{\mathbb{F}_p}(M/pM) =: \beta(M)$ is an isomorphism invariant of abelian groups: $\beta(\mathbb{Z}/(p^k)) = 1$, $k \geq 1$, $\beta(\mathbb{Z}/(q^\ell)) = 0$ for $p \nmid q$.

Proposition 6.6.5

(i) *Let $\varphi : M \xrightarrow{\sim} N$ be an isomorphism of R-modules. Then, φ restricts an isomorphism $IM \xrightarrow{\sim} IN$ of R-modules. Furthermore, it induces an isomorphism $M/IM \xrightarrow{\sim} N/IN$ of R-modules (and R/I-modules).*
(ii) *Let $M = M_1 \oplus \cdots \oplus M_n$ of R-modules, then $IM = IM_1 \oplus \cdots \oplus IM_n$. Then, we get a nice isomorphism*

$$M/IM \simeq M_1/IM_1 \oplus \cdots \oplus M_n/IM_n$$

of R-modules (and R/I-modules).
(iii) *If M is a finitely generated R-module, then M/IM is a finitely generated R-module (and R/I-module).*
(iv) *Let M be a finitely generated R-module. Let $I \subseteq R$ be a finitely generated ideal. Then, IM is a finitely generated R-module.*

Proof. For (iv), note that $M = Rx_1 + \cdots + Rx_n$. Similarly, $I = (a_1, \ldots, a_k)$. Then, the claim is

$$IM = \sum_{\substack{i=1,\ldots,k \\ j=1,\ldots,n}} Ra_i x_j.$$

□

Let R be a PID and $p \in R$ a prime (irreducible) element. Let M be a finitely generated R-module. Then, we can form submodules $p^k M \subseteq M$:[45]

45: By (iv), these are all finitely generated.

$$M = p^0 M \supseteq p^1 M \supseteq p^2 M \supseteq \cdots.$$

Using (iii), we can form finitely generated R-quotients $p^{k-1}M/p^k M$:

$$M/pM, \, pM/p^2M, \, p^2M/p^3M.$$

Well, $p^{k-1}M/p^kM = N/pN$, where $N = p^{k-1}M$. Then, these are all $R/(p)$-modules. Why do we care? Well, these are *fields*!

Definition 6.6.1 ($\alpha_{p^k}(M)$) *We define an "invariant" for $k \geq 1$:*

$$\alpha_{p^k}(M) := \dim_{R/(p)} p^{k-1}/p^k M \in \mathbb{Z}_{\geq 0}.$$

Proposition 6.6.6

(i) *If $M \simeq N$ are finitely generated R-modules, then $\alpha_{p^k}(M) = \alpha_{p^k}(N)$.*

(ii) *If* $M = M_1 \oplus \cdots \oplus M_n$*, then*[46]

$$\alpha_{p^k}(M) = \alpha_{p^k}(M_1) + \cdots + \alpha_{p^k}(M_n).$$

(iii) *If* $M = R/(a)$ *for some* $a \in R$*, then*[47]

$$\alpha_{p^k}(R/(a)) = \begin{cases} 1, & p^k \mid a \\ 0, & \textit{otherwise}. \end{cases}$$

46: The M_k are finitely generated.

47: Consequently, $\alpha_{p^k}(R) = 1$.

Proof. See the previous proposition for (i) and (ii). We now prove (iii). Our module is cyclic, so $N := p^{k-1}M$ is *also* cyclic. It is generated as a submodule of M by the class of p^{k-1}. Then, $p^{k-1}M/p^kM$ is a cyclic R-module (and $R/(p)$-module). Thus, we have forced

$$\dim_{R/(p)} p^{k-1}M/p^kM \in \{0, 1\}.$$

We can write $N = p^{k-1}M = p^{k-1}(R/(a))$, and we claim this is isomorphic to $(p^k, a)/(a)$. Map $(p^{k-1}, a) \to p^{k-1}(R/(a))$ by $x \mapsto \overline{x}$.[48] In the other case, $pN = p^kM = p^k(R/(a)) \simeq (p^k, a)/(a)$. we want to know if $N = pN$. Well, $N/pN \simeq (p^{k-1}, a)/(p^k, a)$. Well, these are equal if and only if $p^{k-1} \in (p^k, a) = (d)$, so $d = \gcd(p^k, a)$. That is, $N/pN = 0$ if and only if $\gcd(p^k, a) \mid p^{k-1}$. This happens if and only if $p^k \nmid a$. □

48: It is surjective easily. Why is it injective? Well, the kernel of the map is exactly (a), so we get an isomorphism via the first isomorphism theorem.

Definition 6.6.2 ($\beta_{p^k}(M)$) *We define for prime* p *and* $k \geq 1$

$$\beta_{p^k}(M) = \alpha_{p^k}(M) - \alpha_{p^{k+1}}(M).$$

Proposition 6.6.7

(i) $\beta_{p^k}(M)$ *is an invariant.*
(ii) $\beta_{p^k}(M)$ *is additive.*
(iii) *If* q *is prime and* $\ell \geq 1$*, then*

$$\beta_{p^k}(R/(q^\ell)) = \begin{cases} 1, & q^\ell \sim p^k \\ 0, & \textit{otherwise}. \end{cases}$$

In particular, $\beta_{p^k}(R) = 0$,

Corollary 6.6.8 *The number*

$$\beta_{p^k}\left(R^r \oplus R/(q_1^{\ell_1}) \oplus \cdots \oplus R/(q_u^{\ell_u})\right)$$

is precisely the number of summands which are isomorphic to $R/(p^k)$.[49] *Similarly,*

$$\operatorname{rank}\left(R^r \oplus R/(q_1^{\ell_1}) \oplus \cdots \oplus R/(q_u^{\ell_u})\right) = r.$$

49: That is, such that $q^{\ell_j} \sim p^k$.

We are now heading towards existence. Now, if M is finitely generated over R, then $M \simeq R^n/N$, where $R^{\oplus n} \xrightarrow{\varphi} M$ with $(c_1, \ldots, c_n) \mapsto \sum c_i x_i$ is a surjective R-module homomorphism and $M \simeq R^n/\ker\varphi$. Then, $N := \ker\varphi$.

Proposition 6.6.9 *Let R be a PID and M be a free module of rank n. Then any submodule $N \subseteq M$ is free of rank $m \leq n$.*

Proof. We have that $M = R^n \supseteq N$. Proceed by induction on n. The $n = 0$ is trivial. What about $n = 1$? Well, $(d) = N \subseteq R$, as R is a PID. If $(d) = 0$, then $N = 0$, which is free of rank zero. If $(d) \neq 0$, then $R \xrightarrow{\sim} (d)$ by $r \mapsto rd$ as R-modules.[50] Now, let $n \geq 2$. Consider the projection

$$\begin{aligned} R^n &\xrightarrow{\pi} R \\ (c_1, \ldots, c_n) &\longmapsto c_n. \end{aligned}$$

50: Since we are in a domain, the kernel is only $\mathbf{0}$.

Then, $\ker \pi = R^{n-1} \oplus 0 \subseteq R^n$. Let $N' := N \cap \ker \pi \subseteq R^{n-1}$. By induction, N' is free of rank less than or equal to $n-1$. Consider $\pi(N) \subseteq R$ as a submodule. Either $\pi(N) = 0$, so $N = N'$ and we win, or $\pi(N) = R\bar{t}$, for some $\bar{t} \in R$ for $\bar{t} \neq 0$. Lift $\bar{t}$ to some $t \in N$. We claim that $N = N' \oplus Rt$, so it is of rank $\operatorname{rank}(N') + 1 \leq (n-1) + 1 = n$. Note that $N', Rt \subseteq N$ Then, take $N = N' + Rt$, so if $x \in N$, then $\pi(x) = c\bar{t}$ for $c \in R$. Let $x' := x - ct \in N$. Then, $\pi(x') = \pi(x) - c\bar{t} = 0$, so $x' \in N'$. Thus, $x = x' + ct$. If $N' \cap Rt = 0$, then if $x \in N' \cap Rt$, then $x = ct$, so $\pi(x) = c\bar{t} = 0$. Since we are in a domain, we get $x = 0$. ☐

Definition 6.6.3 (Smith Normal Form) *Let $A \in \mathbb{M}_{m \times n}(R)$, taking $n \leq m$. We say that A is in Smith normal form if A is diagonal with d_i, and zeros beneath. and $d_1 \mid d_2 \mid \cdots \mid d_n$.*

Definition 6.6.4 (Similar) *We say $A, B \in \mathbb{M}_{m \times n}(R)$ are similar if there exists $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ so that $B = P^{-1}AQ$.*

Theorem 6.6.10 *Let R be a PID with $A \in \mathbb{M}_{m \times n}(R)$ and $n \leq m$, then A is similar to a matrix in Smith normal form.*

Proof. We want to show there exist $P_1, \ldots, P_k, \in \mathrm{GL}_m(R)$ and $Q_1, \ldots, Q_\ell \in \mathrm{GL}_n(R)$ such that

$$P_1 \cdots P_k A Q_1 \cdots Q_\ell$$

is in Smith normal form.[51] We also have a "Bézout operation" based on the standard number theory linear combination result. Leaving out *essentially* all of the matrix checking, we can get a matrix A into our desired form. Over a field, the elementary matrices are enough for this, but we do not have a Euclidean algorithm in a general PID. Now, let $A \in \mathbb{M}_{m \times n}(R)$. Define $\gcd(A) \in R$ be the greatest common divisor of all the elements in A, taken up to units. Now, we claim that if P, Q are invertible R-matrices, then $\gcd(PAQ) = \gcd(A)$. Well, for any M with entries in R,

51: Quickly, note that we have three elementary matrices. The first swithces rows and columns, the second by a row or column by a unit, and the third adds multiples of a row (or column) to another.

$$(\gcd(MA)) \subseteq (\gcd(A))$$

and

$$(\gcd(AN)) \subseteq (\gcd(A)).$$

Well, $MA = [x_{ij}]$ generates an ideal contained in $(\gcd(A))$. We will be done by the following lemma, by induction.[52] $\square$

52: The proof proceeds by induction on the number of columns, but I was not enjoying typesetting the block matrices.

Lemma 6.6.11 *For $A \in \mathbb{M}_{m\times n}(R)$ with $m \geq n$, A is similar to one of the form*

$$\begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & b_{1,1} & \cdots & b_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & b_{m-1,1} & \cdots & b_{m-1,n-1} \end{pmatrix}$$

such that d divides every entry of $B \in \mathbb{M}_{(m-1)\times(n-1)}(R)$.

Proof. For $A = 0$, we are done. Assume $A \neq 0$. Write a for the $(1,1)$-entry of A. Write $d := \gcd(A)$. We claim that if $(a) \neq (d)$, then A is similar to an A' whose $(1,1)$-entry a' is so that $(a) \subsetneq (a')$.[53] Thus, we must obtain A' similar to A with $(1,1)$-entry of which is a greatest common divisor of A' and of A. Using our operations, we get $A' \sim A$. Finally, let us prove the claim. In the first case, a does not divide some element in the first row or first column, other than itself, of course. Using the Bézout operation, we can slightly enlargen the top left generated ideal. In the second case, suppose a divides every element in the first row and column. Well, $(a) \neq (\gcd(A))$, there exists an (i,j)-entry m such that $a \nmid m$.[54] $\square$

53: If so, we can find a sequence of similar A_j whose $(1,1)$-entries satisfy strict successive inclusions $(a_i) \subsetneq (a_{i+1})$, but the ACC tells us this process must stop.

54: From here, use an elementary row operation to create a matrix with m' in the first row not divisible by a.

Proposition 6.6.12 *Let R be a PID. Let M be a finitely generated R-module. Then, there exists a chain of ideals $R \supseteq (d_1) \supseteq \cdots \supseteq (d_m)$ such that*

$$M \simeq R/(d_1) \oplus \cdots \oplus R/(d_m).$$

Proof. Pick generators $x_1, \ldots, x_n \in M$. We have the diagram

$$\begin{tikzcd} \ker(\varphi) \arrow[d, equal] & & \\ N \arrow[r, tail, "\varphi"] \arrow[d, "\simeq"] & R^m \arrow[r, two heads, "\pi"] & M \\ R^n & & \end{tikzcd}$$

with

$$M \simeq R^m/N = R^m/\varphi(R^n).$$

We can then express $\varphi : R^n \to R^m$ as a matrix A such that $\varphi(f_j) = \sum a_{ij} e_i$. Then, there exist P, Q such that $S := PAQ^{-1}$ in Smith normal form. This gives us new bases

$$f'_j := \sum_{i=1}^{n} q_{ij} f_i \in N$$

and[55]

$$e'_j := \sum_{i=1}^{m} p_{ij} e_i \in R^m.$$

55: Take $\varphi(f'_j) := \sum d_j e'_j$.

That is, $M \simeq R^m/\varphi'(R^n)$ via

$$\varphi'(x_1, \dots, x_n) = (d_1 x_1, \dots, d_n x_n, 0, \dots, 0).$$

Really, we have a map $\varphi' : R^n \to R^m = R^n \oplus R^{m-n}$, so

$$M \simeq R/(d_1) \oplus \cdots \oplus R/(d_n) \oplus R \oplus \cdots R.$$

Take $d_{n+1} = \cdots = d_m = 0$. □

Let R be a PID and M a finitely generated R-module.

Theorem 6.6.13 (Invariant Factor) *There exist $t, r \geq 0$ with*

$$R \supsetneq (a_1) \supsetneq \cdots \supsetneq (a_t) \supsetneq (0)$$

such that[56]

$$M \simeq R/(a_1) \oplus \cdots \oplus R/(a_t) \oplus R^r.$$

This is unique in the sense that if we have another decomposition with r' and t', then $r = r'$, $t = t'$, and $(a_j) = (a'_j)$.

56: The $a_1, \dots, a_t$ are called the "invariant factors."

Example 6.6.2 With $R := \mathbb{Z}$, recall that every nonabelian group of order $120 = 2^3 \cdot 3 \cdot 5$ is isomorphic to exactly one of $\mathbb{Z}/120$, $\mathbb{Z}/2 \oplus \mathbb{Z}/60$, or $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/30$.

Remark 6.6.2 The $p_1^{k_1}, \dots, p_u^{k_u}$ of an elementary divisor form are called elementary divisors.

Proposition 6.6.14 (Uniqeuness of IFD) *The invariant factor form is unique.*

Proof. If $M = R/(a_1) \oplus \cdots \oplus R/(a_t) \oplus R^r$, where $a_1 \mid a_2 \cdots \mid a_t$ and the a_j are nonzero and non-units. We have that $\operatorname{rank}(M) = r$. Well,

$$\alpha_{p^k}(M) = \Big|\{j : p^k \mid a_j\}\Big| + r.$$

Now, note that p is any prime which divides a_1. Thus, $\alpha_p(M) = t + r$, so

$$t = \max\{\alpha_p(M) - \operatorname{rank}(M)\}$$

with primes p. □

6.7 Linear Algebra via Modules

If we have $\mathscr{V}$, an $\mathbb{F}$-vector space, and a $T : \mathscr{V} \to \mathscr{V}$, an $\mathbb{F}$-linear operator, then we get a module $\mathscr{V}_T$ over $R = \mathbb{F}[x]$. The underlying set is $\mathscr{V}$, and with $f \in R$ and $v \in V$, then $f_v = f(T)v$. Furthermore, this is a bijective correspondence:
In particular, $\mathscr{V}_T \simeq \mathscr{W}_U$ as R-modules if and only if there exists a $\varphi : \mathscr{V} \xrightarrow{\sim} \mathscr{W}$ such that $\varphi T = U\varphi$.

$$\text{Operators } (\mathcal{V}, T : \mathcal{V} \to \mathcal{V}) \longleftrightarrow R = \mathbb{F}[x]\text{-modules } \mathcal{V}_T$$

$$T\text{-invariant } \mathcal{W} \subseteq \mathcal{V} \longleftrightarrow R\text{-submodules of } \mathcal{V}_T$$

$$\mathbb{F}\text{-linear } \varphi : \mathcal{V} \to \mathcal{W} \text{ st } \varphi T = U\varphi \longleftrightarrow R\text{-module hom } \mathcal{V}_T \xrightarrow{\varphi} \mathcal{W}_U.$$

Lemma 6.7.1 *Given $(\mathcal{V}, T)$, we get $\dim_{\mathbb{F}} \mathcal{V} < \infty$ if and only if $\mathcal{V}_T$ is finitely generated and torsion as an $\mathbb{F}[x]$-module.*

Proof. Suppose $v \in \mathcal{V}_T$ is not torsion. Then, $Rv \subseteq \mathcal{V}_T$. Yet, we get an R-module isomorphism $Rv \simeq R$, and $\dim_{\mathbb{F}} R = \infty$, which is impossible. Conversely, if $\mathcal{V}_T$ is finitely generated and torsion as an R-module, then

$$\mathcal{V}_T \simeq R/(f_1) \oplus \cdots \oplus R/(f_d)$$

as R-modules, with $f_i \neq 0$. Then,

$$\dim_{\mathbb{F}} \mathbb{F}[x]/(f) = \deg(f) = \dim_{\mathbb{V}} \mathcal{V} < \infty.$$

$\square$

Now, let $\mathcal{V}_T$ be a finitely generated torsion $\mathbb{F}[x]$-module. Consider $\mathrm{Ann}(\mathcal{V}_T) = (f)$.

Theorem 6.7.2 *There exists a decomposition*

$$\mathcal{V}_T \simeq R/(f_1) \oplus \cdots \oplus R/(f_d)$$

with $f_j \neq 0$ and $0 \neq f_1 f_2 \cdots f_d \in \mathrm{Ann}(\mathcal{V}_T) = (f)$.[57]

57: Remember, this f is called the *minimal polynomial* of T, the smallest polynomial killing T.

Proposition 6.7.3 *Given $(\mathcal{V}, T)$ with $\dim_{\mathbb{F}} \mathcal{V} < \infty$, let f be the minimal polynomial of T. Then, with $c \in \mathbb{F}$, the following are equivalent:*

(i) There exists a nonzero $v \in V$ such that $Tv = cv$.
(ii) $f(x) = 0$.[58]

58: That is, c is a root of the minimial polynomial.

Proof. We use that $\mathbb{F}[x]$ is a Euclidean domain. Thus, there exists a form $f = (x-c)g + r$, where $g \in \mathbb{F}[x]$ and $r \in \mathbb{F}$. Now, we have $Tv = cv$, where $v \neq 0$. Thus, $(x-c)v = Tv - cv = 0$, so $0 = f(T)v = g(T)(T-c)v + rv$, meaning $r = 0$. Thus, $f(x) = 0$. Conversely, if $f(x) = 0$, then $f = (x-c)g$ with $g \notin (f) = \mathrm{Ann}(\mathcal{V}_T)$. There exists $w \in \mathcal{V}$ such that $v = g(T)w \neq 0$, so $Tv = cv$. $\square$

Now, let

$$\begin{aligned} \mathcal{V}_T &\simeq M_1 \oplus \cdots \oplus M_m \\ &\simeq R/(f_1) \oplus \cdots \oplus R/(f_m). \end{aligned}$$

Pick a basis β of $\mathcal{V}$ such that

$$[T]_\beta = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{pmatrix}.$$

Pick β so that the first bunch is an $\mathbb{F}$-basis of M, the second is one for M_2, and so forth. If $\mathcal{V}_T = \mathbb{F}[x]/(f)$, then $f = x^k + b_{k-1}x^{k-1} + \cdots + b_0$ with $b_j \in \mathbb{F}$. Use the basis β with $e_1 = \overline{1}$, $e_2 = \overline{x}$, $e = \overline{x}^2$, and $e_i = \overline{x}^{i-1}$ of $\mathbb{F}[x]/(f)$. Then,[59]

59: We call C_f the companion matrix, for some reason.

$$[T]_\beta = C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{k-1} \end{pmatrix}.$$

Theorem 6.7.4 (Rational Canonical Form) *Any $T : \mathcal{V} \to \mathcal{V}$ can be written uniquely as*[60]

$$[T]_\beta = \begin{pmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \ddots & \\ & & & C_{f_m} \end{pmatrix},$$

where f_j is a monic polynomial such that $f_1 \mid f_2 \mid \cdots \mid f_m$.

60: That is, we dceompose into companion matrices. The proof this is *precisely* the invariant factor decomposition.

Theorem 6.7.5 (Cayley-Hamilton) *We have that $f_T \mid p_T$, so $p_T(T) = 0$.*[61]

61: The minimal polynomial divides the *characteristic polynomial*.

Proof. Note that $\det\bigl(xI - C_f\bigr) = f(x)$, so if

$$\mathcal{V}_T \simeq \bigoplus_{k=1}^{m} \mathbb{F}[x]/(f_k),$$

where is f_k is monic for all k, then

$$p_T := \det(xI - T) = f_1 \cdots f_m \in \operatorname{Ann}(\mathcal{V}_T) = (f_T),$$

the minimal polynomial.[62] □

62: We also have Jordan form for when

$$\mathcal{V}_T \simeq \bigoplus_{k=1}^{m} \mathbb{F}[x]/\bigl((x-c_i)^{k_i}\bigr).$$

On the Theory of Fields

7 Fields

Now that we have developed a working theory of commutative rings, domains, and modules, we turn our focus to *fields*. Using our work on $\mathsf{Mod}_{\mathbb{F}} = \mathsf{Vect}_{\mathbb{F}}$, we can prove many things about embeddings of fields.

7.1 Extensions and Towers

Let $\mathbb{K}$ be a field. Let $\mathbb{F} \subseteq \mathbb{K}$ be a subfield.

Definition 7.1.1 (Field Extension) *We write $\mathbb{K}/\mathbb{F}$ to mean "$\mathbb{K}$ extends $\mathbb{F}$."*[1]

1: This is certainly not a quotient, just notation.

Figure 7.1: Diagram of a field extension $\mathbb{K}/\mathbb{F}$, voiced "$\mathbb{K}$ over $\mathbb{F}$."

Remark 7.1.1 If $\mathbb{F}, \mathbb{K}$ are fields and $\iota : \mathbb{F} \to \mathbb{K}$ is a ring homomorphism preserving 1, then ι is injective, so $\iota(\mathbb{F}) \simeq \mathbb{F}$. We will abusively write $\iota : \mathbb{F} \rightarrowtail \mathbb{K}$ makes $\mathbb{K}$ into an extension of a field $\mathbb{F}$.

Definition 7.1.2 (Prime Subfield) *Every field $\mathbb{F}$ contains a prime subfield, isomorphic to either $\mathbb{Q}$ or to $\mathbb{F}_p = \mathbb{Z}/p$, where p is prime.*

Then, recalling our definition of characteristic, we have

$$\operatorname{char}(\mathbb{F}) = \begin{cases} 0, & \mathbb{Q} \subseteq \mathbb{F} \\ p, & \mathbb{F}_p \subseteq \mathbb{F}. \end{cases}$$

Now, if we have $R \subseteq S$, where S is a commutative ring and R is a subring with $1_R = 1_S$, then $S \in \mathsf{Mod}_R$.

Definition 7.1.3 (Degree) *In particular, if $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, then we define the degree*

$$[\mathbb{K} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{K}.$$

Example 7.1.1 We have that $[\mathbb{C} : \mathbb{R}] = 2$ and $[\mathbb{R} : \mathbb{Q}] > \aleph_0$.

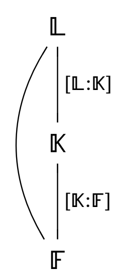

Figure 7.2: Diagram of the tower law

Theorem 7.1.1 (Tower Law) *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$. Then,*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Proof. Let $\{\alpha_i\}_{i \in I}$ be a basis of $\mathbb{K}$ over $\mathbb{F}$ and $\{\beta_j\}_{j \in J}$ be a basis of $\mathbb{L}$ over $\mathbb{K}$. We claim that $\{\alpha_i \beta_j\}_{i \in I, j \in J}$ is a basis of $\mathbb{L}$ over $\mathbb{F}$. Take $x \in \mathbb{L}$. Then,

$$x = \sum_j x_j \beta_j = \sum_j \left(\sum_i y_{ij} \alpha_i \right) = \sum_{i,j} y_{ij} (\alpha_i \beta_j),$$

so $\operatorname{span}_{\mathbb{F}}\{\alpha_i \beta_j\} = \mathbb{L}$. Uniqueness gives us linear independence. $\square$

Definition 7.1.4 (Field Embedding) *A field homomorphism is a map $\varphi : \mathbb{K} \to \mathbb{L}$ is a ring homomorphism between fields preserving 1. In particular, φ is injective, so we can call φ an "embedding" of $\mathbb{K}$ into $\mathbb{L}$.*

As usual, we take

$$\mathrm{Aut}(\mathbb{F}) = \{\varphi : \mathbb{F} \xrightarrow{\sim} \mathbb{F}\}.$$

Fix $\mathbb{F}$. Consider extensions $\mathbb{K}/\mathbb{F}$ and $\mathbb{L}/\mathbb{F}$. We need $\mathbb{K} \to \mathbb{L}$ such that $\mathbb{F}$ stays fixed.

Definition 7.1.5 (Extension Homomorphism) *A homomorphism of extensions $\mathbb{K}/\mathbb{F} \to \mathbb{L}/\mathbb{F}$ is a homomorphism of fields $\varphi : \mathbb{K} \to \mathbb{L}$ such that $\varphi|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.*

Then, we can define

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}) := \{\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} : \varphi\big|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}\} \subseteq \mathrm{Aut}(\mathbb{K}).$$

Definition 7.1.6 (Irreduicble Set) *The set of irreducible polynomials over $\mathbb{F}$ is denoted*

$$\mathrm{Irred}(\mathbb{F}) := \{f \in \mathbb{F}[x] : f \textit{ irreducible in } \mathbb{F}[x] \textit{ and } f \textit{ monic}\}.$$

Let $f \in \mathrm{Irred}(\mathbb{F})$. Then, $\mathbb{K} := \mathbb{F}[x]/(f)$ is a field, because f is irreducible and $\mathbb{F}[x]$ is a PID. Then, we get

$$\begin{tikzcd} \mathbb{F} \arrow[r, hook, "\text{scalars}"] \arrow[rr, bend right, "\text{extension } \mathbb{K}/\mathbb{F}"'] & \mathbb{F}[x] \arrow[r, two heads, "\pi"] & \mathbb{F}[x]/(f) = \mathbb{K} \end{tikzcd}$$

Remark 7.1.2 Let $[\mathbb{K} : \mathbb{F}] = \deg f = n$, and take $\mathbb{K}$ as before. Write $\alpha = x + (f) \in \mathbb{K}$. Then, $\mathbb{K}$ has an $\mathbb{F}$-basis[2]

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

Given $f, g \neq 0$ in $\mathbb{F}[x]$, then there are $q, r \in \mathbb{F}[x]$ such that

$$g = qf + r, \quad \deg r < n = \deg f,$$

as $\mathbb{K} \leftrightarrow \{r \in \mathbb{F}[x] : \deg r < n\}$ is an isomorphism of $\mathbb{F}$-vector spaces.

2: This is precisely because $\mathbb{F}[x]$ is a Euclidean domain.

Now, what has this construction given us? Well, $\mathbb{F} \subseteq \mathbb{K} \ni \alpha$ has the property that $f(\alpha) = 0$. That is, we have "formally adjoined a root of the irreducible f to the field $\mathbb{F}$."

Example 7.1.2 Let $\mathbb{F} := \mathbb{Q}$. Let $f = x^2 - 2 \in \mathbb{Q}[x]$. We claim that f is irreducible. If not, $f = (x-a)(x-b)$, so $a, b \in \mathbb{Q}$ such that $f(a) = f(b)$. Yet, $\pm\sqrt{2} \notin \mathbb{Q}$. Then, we can form $\mathbb{K} := \mathbb{Q}[x]/(x^2 - 2)$. We will write

$\alpha := x + (f) \in \mathbb{K}$, so $\alpha^2 = 2$. Let $a, b, c, d \in \mathbb{Q}$, so

$$(a + b\alpha)(c + d\alpha) = (ac + 2bd) + (ad + bc)\alpha.$$

Well,

$$(a + b\alpha)(a - b\alpha) = a^2 - 2b^2$$
$$(a + b\alpha)^{-1} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\alpha,$$

which is not dividing by zero since $a^2 = 2b^2$ implies $2 = (a/b)^2$.[3]

3: This is why we needed an irreducible.

Without proof, we state a nice irreducibility theorem.

Theorem 7.1.2 (Eisenstein's Criterion) *Let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$. Let $p \in \mathbb{Z}$ be a prime number. If $p \mid a_k$ for all $k \in \{0, \ldots, n-1\}$, and $p^2 \nmid a_0$, then $f \in \mathrm{Irred}(\mathbb{Q})$.*

Example 7.1.3 Let $\mathbb{K} := \mathbb{Q}[x]/(x^3 - 2)$. We claim $x^3 - 2 \in \mathrm{Irred}(\mathbb{Q})$, as $2 \mid 0, -2$, but $4 \nmid 2$. Now, $\alpha^3 = 2$, so $[\mathbb{K} : \mathbb{Q}] = 3$.

What does[4]

$$\mathrm{Hom}_{\mathsf{Field}}(\mathbb{Q}[x]/(f), \mathbb{L})$$

look like? Here is the answer:

4: We have $f \in \mathrm{Irred}(\mathbb{Q})$.

$$\begin{tikzcd}
\mathbb{Q} \arrow[d, hook] \arrow[rdd, bend left, "\text{exists iff char } \mathbb{L}=0"] & \\
\mathbb{Q}[x] \arrow[d, two heads] \arrow[rd, dashed, "x \mapsto \beta \in \mathbb{L}"] & \\
\mathbb{Q}[x]/(f) \arrow[r, dashed, "\text{exists iff } f(\beta)=0"'] & \mathbb{L}
\end{tikzcd}$$

Figure 7.3: The reason $\mathbb{Q} \to \mathbb{L}$ exists if and only if $\mathrm{char}\,\mathbb{L} = \mathbf{0}$ is essentially by the definition of prime subfield.

Example 7.1.4 Consider $\mathbb{K} = \mathbb{Q}[x]/(x^2 - 2)$. Then, $\mathrm{Hom}_{\mathsf{Field}}(\mathbb{K}, \mathbb{Q}) = \varnothing$, since the polynomial has no roots in $\mathbb{Q}$. On the other hand,[5]

$$\mathrm{Hom}_{\mathsf{Field}}(\mathbb{K}, \mathbb{R}) = \begin{cases} \alpha \mapsto \sqrt{2} \\ \alpha \mapsto -\sqrt{2}. \end{cases}$$

5: With these maps, $\varphi_1(\mathbb{K}) = \varphi_2(\mathbb{K})$, which are isomorphic to $\mathbb{K}$ in *two different ways*.

Example 7.1.5 Consider $\mathbb{K}' = \mathbb{Q}[x]/(x^3 - 2)$. Then,

$$\mathrm{Hom}_{\mathsf{Field}}(\mathbb{K}', \mathbb{R}) = \begin{cases} \alpha \mapsto \sqrt[3]{2}. \end{cases}$$

On the other hand,[6]

6: Here, $\varphi_i(\mathbb{K}')$ are *distinct* in $\mathbb{R}$. Then, $\mathrm{Aut}(\mathbb{K}') = \{e\}$.

$$\mathrm{Hom}_{\mathsf{Field}}(\mathbb{K}', \mathbb{C}) = \begin{cases} \alpha \mapsto \sqrt[3]{2} \\ \alpha \mapsto \zeta_3 \sqrt[3]{2} \\ \alpha \mapsto \zeta_3^2 \sqrt[3]{2}. \end{cases}$$

Definition 7.1.7 (Generated Subextension) *Let $\mathbb{L}/\mathbb{F}$ be a field extension; let $S \subseteq \mathbb{L}$. Then,*

$$\mathbb{F}(S) := \bigcap_{\substack{\mathbb{K} \subseteq \mathbb{L} \text{ subfield} \\ S \cup \mathbb{F} \subseteq \mathbb{K}}} \mathbb{K} \subseteq \mathbb{L}$$

is a subfield.

Note that the above gives us an intermediate extension.

$$\begin{tikzcd} \mathbb{L} \arrow[d, dash] \\ \mathbb{F}(S) \arrow[d, dash] \\ \mathbb{F} \end{tikzcd}$$

Now, let $S := \{\alpha_1, \ldots, \alpha_n\}$. We will write $\mathbb{F}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{L}$.

Definition 7.1.8 (Finitely Generated Extension) *We say that $\mathbb{L}/\mathbb{F}$ is a* finitely generated extension *if there exists $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ such that $\mathbb{F}(\alpha_1, \ldots, \alpha_n) = \mathbb{L}$.*

Definition 7.1.9 (Simple Extension) *We say that $\mathbb{L}/\mathbb{F}$ is a simple extension if $\mathbb{L} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{L}$.*

7.2 Algebraic Extensions

Our goal is to classify $\mathbb{K} = \mathbb{F}(\alpha)$. Consider the homomorphism $\varphi_\alpha : \mathbb{F}[x] \to \mathbb{F}(\alpha)$ as the unique ring homomorphism $\varphi_\alpha|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ and $\varphi_\alpha(x) = \alpha$.[7] Well, $\ker \varphi_\alpha \subseteq \mathbb{F}[x]$. Now, there are two cases:

7: The map φ_a is "evaluation at α" with $\varphi_\alpha(f) = f(\alpha)$.

(i) $\ker \varphi_\alpha = (0)$ if and only if α is not the root of any nonzero polynomial over $\mathbb{F}$. In this case, we say α is *transcendental* over $\mathbb{F}$. Furthermore, if we have trivial kernel, then $\varphi_\alpha : \mathbb{F}[x] \hookrightarrow \mathbb{F}(\alpha)$, so $\mathbb{F}(\alpha) \simeq \mathrm{Frac}(\mathbb{F}[x])$.
(ii) $\ker \varphi_\alpha = (m)$, where m is monic and irreducible in $\mathbb{F}[x]$. Well, $m \in \mathrm{Irred}(\mathbb{F})$, and we call m the *minimal polynomial* of α over $\mathbb{F}$.[8] Furthermore, $\mathbb{F}(\alpha) \simeq \mathbb{F}[x]/(m)$. In this case, we say $\mathbb{F}(\alpha)$ is an *algebraic simple extension*.

8: This is the smallest degree (nonzero) polynomial that has α as a root. If α is any polynomial such that $f \in \mathbb{F}[x]$ such that $f(\alpha) = 0$, then $m \mid f$.

Remark 7.2.1 Take $\mathbb{L}/\mathbb{F}$. For $\alpha \in \mathbb{L}$, we have a tower $\mathbb{F} \subseteq \mathbb{F}(\alpha) = \mathbb{K} \subseteq \mathbb{L}$. Either α is transcendental over $\mathbb{F}$ or α is algebraic over $\mathbb{F}$ with minimial polynomial $m_{\alpha,\mathbb{F}} \in \mathrm{Irred}(\mathbb{F})$.

Example 7.2.1 ($\mathbb{R}/\mathbb{Q}$) For instance, $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$, whereas $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ with minimal polynomial

$$m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2 \in \mathrm{Irred}(\mathbb{Q}).$$

Example 7.2.2 ($\mathbb{C}/\mathbb{R}$) We have that $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ with minimal polynomial $m_{i,\mathbb{R}} = x^2 + 1$.

Now, we have a extension diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Figure 7.4: Diagram of extensions via adjoining $\sqrt{2}$ and $\sqrt{3}$.

To get the degrees, we use

$$\begin{aligned}
m_{\sqrt{2},\mathbb{Q}} &= x^2 - 2 \in \mathrm{Irred}(\mathbb{Q}) \\
[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] &= 2 \\
m_{\sqrt{3},\mathbb{Q}} &= x^2 - 3 \in \mathrm{Irred}(\mathbb{Q}) \\
[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] &= 3.
\end{aligned}$$

What about the upper degrees? Well, let $m = m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}$. We have that

$$(m) = \{g \in \mathbb{Q}(\sqrt{2})[x] : g(\sqrt{3}) = 0\}.$$

We claim $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$, and if not, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

Proof of Claim. Use $\sqrt{3} \notin \mathbb{Q}$. We want to show $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. If $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, then $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$, so $3 = (a + b\sqrt{2})^2 = (a^2 + 2b^2) + 2ab\sqrt{2}$. Well, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$ with a basis $1, \sqrt{2}$ over $\mathbb{Q}$. We have a system $3 = a^2 + 2b^2$ and $0 = 2ab$.[9] □

9: From here, the proof comes down to some simple algebra.

Remark 7.2.2 Note that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

We say that $\mathbb{L}/\mathbb{F}$ is algebraic if every $\alpha \in \mathbb{L}$ is algebraic over $\mathbb{F}$.

Proposition 7.2.1 *Let $\mathbb{L}/\mathbb{F}$ and $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. The following are equivalent:*

(i) $[\mathbb{L} : \mathbb{F}] < \infty$.
(ii) $\mathbb{L}/\mathbb{F}$ *is an algebraic extension.*
(iii) Each α_k *is algebraic over* $\mathbb{F}$.

Proof. For (i) $\Rightarrow$ (ii), if $\beta \in \mathbb{L}$, we can consider $\mathbb{F} \subseteq \mathbb{F}(\beta) \subseteq \mathbb{L}$. Then,

$$\infty > [\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(\beta)][\mathbb{F}(\beta) : \mathbb{F}],$$

so β is algebraic over $\mathbb{F}$. We certainly have that (ii) $\Rightarrow$ (iii). For (iii) $\Rightarrow$ (i), we need a picture:
We claim that $[\mathbb{K}_k : \mathbb{K}_{k-1}] < \infty$.

$$\begin{tikzcd}
\mathbb{L} = \mathbb{K}_n \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
\mathbb{F}(\alpha_1, \alpha_2) = \mathbb{K}_1(\alpha_2) = \mathbb{K}_2 \arrow[d, dash] \\
\mathbb{F}(\alpha_1) = \mathbb{K}_1 \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{K} = \mathbb{K}_{k-1}(\alpha_k) \ni \alpha_k \arrow[d, dash] \\
\mathbb{K}_{k-1} \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

Figure 7.5: Note that $m = m_{\mathbb{F},\alpha} \in \mathbb{F}[x] \subseteq \mathbb{K}_{k-1}$, so there exists $m_{\alpha,\mathbb{K}_{k-1}}$.

□

Lemma 7.2.2 *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L} \ni \alpha$ be a tower such that α is algebraic over $\mathbb{F}$ and $[\mathbb{K} : \mathbb{F}] < \infty$. Then, $[\mathbb{K}(\alpha) : \mathbb{K}] \leq [\mathbb{F}(\alpha) : \mathbb{F}]$ and $[\mathbb{K}(\alpha) : \mathbb{F}(\alpha)] \leq [\mathbb{K} : \mathbb{F}]$.*

Proof. It suffices to show that

$$[\mathbb{K}(\alpha) : \mathbb{K}] \leq [\mathbb{F}(\alpha) : \mathbb{F}].$$

The LHS is $\deg m_{\alpha,\mathbb{K}}$ and the RHS is $\deg m_{\alpha,\mathbb{F}}$. Since $\mathbb{F} \subseteq \mathbb{K}$, we get an inclusion $m_{\alpha,\mathbb{F}} \in (m_{\alpha,\mathbb{K}}) \subseteq \mathbb{K}[x]$, so $\deg m_{\alpha,\mathbb{F}} \geq \deg m_{\alpha,\mathbb{K}}$. □

Definition 7.2.1 (Composite) *Define the composite extension $\mathbb{K}\mathbb{K}'$ of $\mathbb{K}, \mathbb{K}'$ to be the field generated by $\mathbb{K} \cup \mathbb{K}'$. That is, the smallest field containing both.*

$$\begin{tikzcd}
 & \mathbb{L} \arrow[dd, dash] \\
\mathbb{K}' \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathbb{K} \\
\mathbb{F} \arrow[ur, dash] &
\end{tikzcd}$$

Corollary 7.2.3 *If we have a diagram as given, where $\mathbb{L} = \mathbb{K}\mathbb{K}'$, and all are finite, then $[\mathbb{K} : \mathbb{F}] \geq [\mathbb{L} : \mathbb{K}']$ and $[\mathbb{K}' : \mathbb{F}] \geq [\mathbb{L} : \mathbb{K}]$.*

Proof. Just draw the parallelogram of adjoining (α_i) to $\mathbb{K}$ and $\mathbb{F}$ to get $\mathbb{K}$ and $\mathbb{L}$, which gives us our inequality by the tower law. □

Example 7.2.3 (Algebraic Numbers) Let $\alpha \in \mathbb{C}$. We call α algebraic if it is algebraic over $\mathbb{Q}$. That is, α is the root of some $f \in \mathbb{Q}[x]$ such that $f \neq 0$. Define the set of algebraic numbers

$$\mathbb{Q}^{\text{alg}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic}\}.$$

Proposition 7.2.4 $\mathbb{Q}^{alg}$ *is a field.*

We will need a proposition.

Proposition 7.2.5 *If* $\mathbb{L}/\mathbb{F}$ *is an extension and* $\alpha, \beta \in \mathbb{L}$ *are algebraic over* $\mathbb{F}$, *then* $\alpha + \beta$, $\alpha\beta$, *and* $-\alpha$ *are algebraic over* $\mathbb{F}$.

Proof. If α, β are algebraic over $\mathbb{F}$, then (equivalently) we have

$$[\mathbb{F}(\alpha) : \mathbb{F}] < \infty \text{ and } [\mathbb{F}(\beta) : \mathbb{F}] < \infty,$$

so via the tower law we can write

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = [\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)][\mathbb{F}(\alpha) : \mathbb{F}],$$

which is less than or equal to[10]

$$[\mathbb{F}(\beta) : \mathbb{F}][\mathbb{F}(\alpha) : \mathbb{F}] < \infty.$$

□

10: That is, every $\gamma \in \mathbb{F}(\alpha, \beta)$ is algebraic over $\mathbb{F}$. Note that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha)\mathbb{F}(\beta)$.

Exercise 7.2.1 Let $p_1, \ldots, p_r$ be distinct prime numbers. Then, we can form an algebraic extension

$$\left[\mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_r}\right) : \mathbb{Q}\right] = 2^r,$$

and since this is contained in $\mathbb{Q}^{\text{alg}}$, so $[\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = \infty$.[11]

11: Thus, we can have algebraic extensions which are infinite. We will not, however, say too much about them.

7.3 Splitting Fields

Fix a field $\mathbb{F}$ and a polynomial $f \in \mathbb{F}[x]$ with $f \neq 0$.

Definition 7.3.1 (Splitting Field) *A splitting field of f, as above, is an extension $\Sigma/\mathbb{F}$ such that*

(i) *f splits over Σ; i.e., that is*

$$f = c(x - \alpha_1) \cdots (x - \alpha_n) \in \Sigma[x],$$

for some $\alpha_i, c \in \Sigma$.

(ii) *Σ is generated over $\mathbb{F}$ by the roots of f.*[12]

12: That is, using the roots from the linear factors above,

$$\Sigma = \mathbb{F}(\alpha_1, \ldots, \alpha_n).$$

Lemma 7.3.1 *Let $\mathbb{L}/\mathbb{F}$ be an extension and nonzero $f \in \mathbb{F}[x]$ which splits over $\mathbb{L}$. Then, $\Sigma := \mathbb{F}(\alpha_1, \dots, \alpha_n) \subseteq \mathbb{L}$, where α_i are the roots of f in $\mathbb{L}$, is a splitting field of f.*

Example 7.3.1 Let $f = (x^2+1)(x^2-5) \in \mathbb{Q}[x]$. Then, a splitting field is[13]

$$\Sigma := \mathbb{Q}(\sqrt{5}, i).$$

13: There are four roots, but we only need to write two, as $-1 \in \mathbb{Q}$.

Example 7.3.2 Consider $f = x^3 - 2 \in \mathbb{Q}[x]$. Then,

$$\Sigma = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

Theorem 7.3.2 (Existence of Splitting Field) *Every $f \in \mathbb{F}[x]$ with $f \neq 0$ has a splitting field.*

Proof. Proceed by induction on $n := \deg f$. If $n = 0, 1$, then $\Sigma = \mathbb{F}$. Suppose $n \geq 2$. Choose a $p \in \mathrm{Irred}(\mathbb{F})$ sch that $p \mid f$. Then, since $\mathbb{F}[x]$ is a PID, $f = pg$ where $g \in \mathbb{F}[x]$.[14] Construct $\mathbb{F}(\alpha)/\mathbb{F}$ such that

$$m_{\alpha,\mathbb{F}} = p \in \mathrm{Irred}(\mathbb{F}),$$

and define $\mathbb{F}(\alpha) := \mathbb{F}[x]/(p)$, where $\alpha = \overline{x}$. We take $f = h(x-\alpha)$, where $h \in \mathbb{F}(\alpha)[x]$. Now, $\deg h \neq n - 1 < n$, so by induction, h has a splitting field $\Sigma/\mathbb{F}(\alpha)$. We claim that $\Sigma/\mathbb{F}$ is a splitting field of f. □

14: We have $\deg p \geq 1$ and $\deg g < n$.

Corollary 7.3.3 *If $\Sigma/\mathbb{F}$ is a splitting field of $f \in \mathbb{F}[x]$ with $\deg f = n$, then*

$$[\Sigma : \mathbb{F}] \leq n!.$$

Example 7.3.3 Let $f = x^2 - 3x + 2 = (x-1)(x-2) \in \mathbb{Q}[x]$. Then, the splitting field $\Sigma = \mathbb{Q}$.

We now discuss cyclotomic extensions, taking $\mathbb{L}/\mathbb{F}$.

Definition 7.3.2 (Primitive nth Root of Unity) *We say $\zeta \in \mathbb{L}$ is a primitive nth root of unity if $|\zeta| = n$ in $\mathbb{L}^\times$.*

Note that ζ is a root of the polynomial $f = x^n - 1 \in \mathbb{F}[x]$.

Proposition 7.3.4 *Define $\Sigma := \mathbb{F}(\zeta) \subseteq \mathbb{L}$ to be a splitting field of f.*

Proof. Note that

$$1, \zeta, \zeta^2, \dots, \zeta^{n-1} \in \mathbb{L}$$

are all roots of f. Furthermore, they are all different.[15] Thus,

$$x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1}),$$

so f splits over $\Sigma = \mathbb{F}(\zeta)$. □

15: This is precisely because ζ is *primitive*.

Note that $[\mathbb{F}(\zeta) : \mathbb{F}] \leq n$, which is usually far less than $n!$.

Definition 7.3.3 (Cyclotomic Extension) *We call such an extension, adjoining roots of unity, a cyclotomic extension.*

Example 7.3.4 The standard example is to take $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$, where $|\zeta_n| = n$ in $\mathbb{C}^\times$, forming $\mathbb{Q}(\zeta_n)$.

Proposition 7.3.5 *If $n = p$, a prime, then*

$$m_{\zeta_n,\mathbb{Q}} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

where $\deg m_{\zeta_n,\mathbb{Q}} = p - 1$. *Thus,*

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

Definition 7.3.4 (Formal Deriviative) *Let*

$$f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x].$$

We define the formal derivative

$$Df := a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1} \in \mathbb{F}[x].$$

Exercise 7.3.1 The formal derivative acts how you think it does.[16]

16: I have now proved these rules on two distinct occasions, so see my Hardt notes or my Fogel work.

Definition 7.3.5 (Separable) *Let $f \in \mathbb{F}[x]$. We have that f is separable if f, Df are relatively prime in $\mathbb{F}[x]$. That is, (f, Df) is the unit ideal in $\mathbb{F}[x]$.*

Remark 7.3.1 Let $\lambda : bF \rightarrowtail \mathbb{K}$ be a homomorphism of fields. Then, we also ket a free homomorphism of rings $\lambda : \mathbb{F}[x] \to \mathbb{K}[x]$. We precisely take this new λ to be prescribed by the formula

$$\lambda : \sum a_k x^k \mapsto \sum \lambda(a_k) x^k.$$

Then, it is an easy check that $\lambda(D(f)) = D(\lambda(f))$.

Example 7.3.5 For instance, let $\lambda : \mathbb{F} \hookrightarrow \mathbb{K}$. Then, we get a subring inclusion $\lambda : \mathbb{F}[x] \hookrightarrow \mathbb{K}[x]$.

Proposition 7.3.6 *Let $\lambda : \mathbb{F} \rightarrowtail \mathbb{K}$ be a field homomorphism. Then, $f \in \mathbb{F}[x]$ is separable if and only if $\lambda(f) \in \mathbb{K}[x]$ is separable over $\mathbb{K}$.*[17]

17: An element $f \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$ if and only if $f \in \mathbb{Q}(i)[x]$ is separable over $\mathbb{Q}(i)$.

Proof. If f is separable over $\mathbb{F}$, then $1 = uf + vD(f)$ for some $u, v \in \mathbb{F}[x]$. Well, $1 = \lambda(u)\lambda(f) + \lambda(v)D(\lambda(f))$ in $\mathbb{K}[x]$. Thus $\lambda(f)$ is separable over $\mathbb{K}$. Conversely, if f is not separable over $\mathbb{F}$, then there exists a common, non-unit factor g of f, Df, so $\lambda(g)$ is a common, non-unit factor of

$\lambda(f)$, $D(\lambda(f))$, meaning $\lambda(f)$ is not separable. $\square$

Proposition 7.3.7 *A nonzero polynomial $f \in \mathbb{F}[x]$ is separable if and only if for some irreducible factorization*

$$f = g_1 \cdots g_n, \quad \text{the } g_i \text{ are irreducible,}$$

then

(i) each g_k is separable.
(ii) there are no repeated factors.[18]

18: That is, if $i \neq j$, then $g_i \nmid g_j$.

Proof. We will show that an irreducible factor g of f divides the formal derivative Df if and only if $g^2 \mid f$, or g is not separable. Suppose g is irreducible in $\mathbb{F}[x]$ and $g \mid f$. Then,[19] $f = gh$:

19: Note that $g \mid Df$ if and only if $g \mid (Dg)h$.

$$Df = D(gh) = (Dg)h + g(Dh).$$

Then, equivalently, $g \mid Dg$ or $g \mid h$, since g is irreducible (and thus, prime). Well, the latter is the same as saying $g^2 \mid f$, whereas the former is the same as saying g is *not* separable. $\square$

Corollary 7.3.8 *Let $\mathbb{L}/\mathbb{F}$ be any extension over which nonzero $f \in \mathbb{F}[x]$ splits. Then, f is separable if and only if f has no repeated roots in $\mathbb{L}[x]$.*

Proof. Note that separability over $\mathbb{F}$ is equivalent to separability over $\mathbb{L}$. Then, without loss of generality, take $\mathbb{L} = \mathbb{F}$, writing

$$f = c(x - \alpha_1) \cdots (x - \alpha_n),$$

where $c \in \mathbb{L}^\times$. An easy fact is that $x - \alpha$ is *always* separable: $D(x - \alpha) = 1$, so f is separable if and only if it has no repeated roots. $\square$

Proposition 7.3.9 *Let $f \in \mathbb{F}[x]$ be irreducible. Then, f is separable if and only if $Df \neq 0$.*

Proof. Assume $Df \neq 0$. Let $\deg f = n$. Then, $-\infty \neq \deg Df < n$. Then, $Df \notin (f) \subseteq \mathbb{F}[x]$, so $(Df, f) = \mathbb{F}[x]$. If $Df = 0$, then $(f, Df) = (f) \neq \mathbb{F}[x]$, as desired. $\square$

Example 7.3.6 Let $\mathbb{F} := \mathbb{F}_p = \mathbb{Z}/p$. Let $f = x^p - a$, where $a \in \mathbb{F}_p$. Then, $Df = px^{p-1} - 0 = 0$ is not separable.[20]

20: Note that this polynomial factors by

$$x^p - a = (x - a)^p$$

in $\mathbb{F}_p[x]$ so this is not a contradiction to our result.

Theorem 7.3.10 *There exists a field $\mathbb{K}$ such that* $\operatorname{char} \mathbb{K} = p > 0$ *and $a \in \mathbb{K}$ so that $a = b^p$ for every $b \in \mathbb{K}$, meaning $f = x^p - a$ is irreducible and not separable.*

Corollary 7.3.11 *If* $\operatorname{char} \mathbb{F} = 0$. *Then, all irreducible polynomials are separable.*

Suppose we are given a simple, finite extension of fields $\mathbb{F}(\alpha)/\mathbb{F}$. This must be algebraic. We get a minimal polynomial $m_{\alpha,\mathbb{F}} = f \in \operatorname{Irred}(\mathbb{F})$. Now, suppose we have

$$\begin{tikzcd}
\mathbb{F}(\alpha) \arrow[r, dashed, "\varphi"] & \mathbb{L} \\
\mathbb{F} \arrow[u, dash] \arrow[r, two heads, "\lambda", "\simeq"'] & \mathbb{F}' \arrow[u, dash]
\end{tikzcd}$$

Figure 7.6: We take a simple, finite extension, map the ground field over isomorphically to another field with an associated parent extension. We show how to construct a new homomorphism φ between the parents.

Then, we get a bijective correspondence

$$\left\{\text{homs } \varphi : \mathbb{F}(\alpha) \to \mathbb{L} : \varphi\big|_{\mathbb{F}} = \lambda\right\} \xleftrightarrow[\text{bijection}]{} \{\beta \in \mathbb{L} : f'(\beta) = 0\},$$

where $f' := \lambda(f) \in \mathbb{F}'[x]$.

Corollary 7.3.12 *The # of homs $\varphi : \mathbb{F}(\alpha) \to \mathbb{L}$ is $\leq \deg f$.*

Corollary 7.3.13 (Uniqueness of Splitting Field) *If $\Sigma/\mathbb{F}$ and $\Sigma'/\mathbb{F}$ are splitting field of $f \in \mathbb{F}[x]$ then $\Sigma/\mathbb{F} \simeq \Sigma'/\mathbb{F}$.*[21]

21: Recall that an isomorphism of extensions is a field isomorphism which restricts to the identity on the ground field.

We will need to prepare some tools for this.

Proposition 7.3.14 *Consider an isomorphism $\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}'$, a nonzero polynomial $f \in \mathbb{F}[x]$, a splitting field $\Sigma/\mathbb{F}$ of f, and an extension $\mathbb{L}/\mathbb{F}'$ such that $f' := \lambda(f)$ splits over $\mathbb{L}$. Then, there exists a homomorphism of field $\varphi : \Sigma \to \mathbb{L}$ such that $\varphi|_{\mathbb{F}} = \lambda$, and $\varphi(\Sigma)$ is a splitting field of f'.*

$$\begin{tikzcd}
\Sigma \arrow[r, dashed, "\varphi"] & \mathbb{L} \\
\mathbb{F} \arrow[u, dash] \arrow[r, two heads, "\lambda", "\simeq"'] & \mathbb{F}' \arrow[u, dash]
\end{tikzcd}$$

Proof of Corollary. Take $\mathbb{F} = \mathbb{F}'$. Then, $\lambda = \mathrm{id}_{\mathbb{F}}$, meaning $\mathbb{L} = \Sigma'$. Then, the proposition gives us a triangle

$$\begin{tikzcd}
\Sigma \arrow[rr, two heads, "\varphi"] & & \Sigma' \\
& \mathbb{F} \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Note that φ must send roots of f to roots of f. Thus, $\Sigma = \Sigma'$.[22] $\square$

22: We use that both are splitting fields of f.

Proof of Proposition. We proceed by induction on $n = \deg f$. For $n = 0$, then $\Sigma = \mathbb{F}$. Suppose $n \geq 1$. Let $\alpha_1 \in \Sigma$ be a root of f, then

$$m = m_{\alpha_1,\mathbb{F}} \in \mathrm{Irred}(\mathbb{F})$$

so $m \mid f$, meaning $f = mg$ for some $g \in \mathbb{F}[x]$. We get $\lambda : \mathbb{F}[x] \xrightarrow{\sim} \mathbb{F}'[x]$ with $\lambda(f) = f' = m'g'$, with $m' = \lambda(m)$. Well, f' splits over $\mathbb{L}$, so m has a root $\beta_1 \in \mathbb{L}$. We get a diagram

$$\begin{tikzcd}
\Sigma \arrow[d, dash] & \mathbb{L} \arrow[d, dash] \\
\mathbb{F}(\alpha_1) \arrow[r, dashed, "\varphi"] \arrow[d, dash] & \mathbb{F}(\beta_1) \arrow[d, dash] \\
\mathbb{F} \arrow[r, two heads, "\lambda", "\simeq"'] & \mathbb{F}'
\end{tikzcd}$$

Then, $f = (x - \alpha_1)h$ over $\mathbb{F}(\alpha_1)$. We get an isomorphism of fields $\varphi_1 : \mathbb{F}(\alpha_1) \xrightarrow{\sim} \mathbb{F}'(\beta_1)$, a nonzero polynomial $h \in \mathbb{F}(\alpha_1)[x]$, $\Sigma/\mathbb{F}(\alpha_1)$ is a splitting field of h, and $\mathbb{L}/\mathbb{F}'(\beta_1)$ is so that $\varphi_1(h)$ splits over it. Thus, we have all elements of our proposition. □

Remark 7.3.2 We have determined that the splitting field of f in $\mathbb{F}[x]$ is unique up to isomorphism. We write $\Sigma_{f/\mathbb{F}}$ for any such splitting field. Galois theory is about the group $G := \mathrm{Aut}(\Sigma_{f/\mathbb{F}}/\mathbb{F})$.[23]

23: Note that splitting fields are not unique up to *unique* isomorphism. We made lots of choices.

Galois Theory | 8

Recall that if we have a field $\mathbb{K}$, then we can form the corresponding automorphism group $\operatorname{Aut}(\mathbb{K})$. In turn, if we have an extension $\mathbb{K}/\mathbb{F}$, then we can form the automorphism group $\operatorname{Aut}(\mathbb{K}/\mathbb{F}) \leq \operatorname{Aut}(\mathbb{K})$ of automorphisms *fixing* $\mathbb{F}$.

8.1 Automorphisms

Suppose $G \leq \operatorname{Aut}(\mathbb{K})$. Then, the *fixed field*

$$\mathbb{K}^G := \{\alpha \in \mathbb{K} : g(\alpha) = \alpha \text{ for all } g \in G\}$$

is a subfield of $\mathbb{K}$.[1] Then, suppose we have an extension $\mathbb{K}/\mathbb{F}$ and $f \in \mathbb{F}[x]$. For any $\varphi \in \operatorname{Aut}(\mathbb{K}/\mathbb{F})$, if $\alpha \in \mathbb{K}$ such that $f(\alpha) = 0$, then $f(\varphi(\alpha)) = 0$.

1: Showing that this is a field is easy.

Proposition 8.1.1 *Let $\mathbb{K}/\mathbb{F}$ be an extension and $f \in \mathbb{F}[x]$. Let*

$$R_f := \{\alpha \in \mathbb{K} : f(\alpha) = 0\}.$$

Then, $\varphi \in \operatorname{Aut}(\mathbb{K}/\mathbb{F})$ restricts to a permutation of the set R_f. We get a group homomorphism $\iota : \operatorname{Aut}(\mathbb{L}/\mathbb{K}) \to \operatorname{Sym}(R_f)$. Furthermore, if $\mathbb{K} = \mathbb{F}(R_f)$, then ι is injective.[2]

2: That is, $\operatorname{Aut}(\mathbb{K}/\mathbb{F})$ is isomoprhic to a subgroup of $\operatorname{Sym}(R_f)$.

Proof. We show injectivity. Suppose $\varphi \in \operatorname{Aut}(\mathbb{K}/\mathbb{F})$ such that $\iota(\varphi) = \mathrm{id}_{R_f}$. That is, $\varphi : \alpha \mapsto \alpha$ for all $\alpha \in R_f$. Then, $R_f \subseteq \mathbb{K}^G$, where $G := \langle\varphi\rangle \leq \operatorname{Aut}(\mathbb{K}/\mathbb{F})$. We have $\mathbb{F} \subseteq \mathbb{F}(R_f) \subseteq \mathbb{K}^G$, but if $\mathbb{F}(R_f) = \mathbb{K}$, then $\mathbb{K}^G = \mathbb{K}$, so

$$\varphi(\beta) = \beta \quad \text{for all } \beta \in \mathbb{K},$$

meaning $\varphi = \mathrm{id}_{\mathbb{K}}$. □

Example 8.1.1 Let $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. What is $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$? We know how to do this. The extension is degree three with minimal polynomial $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2 \in \operatorname{Irred}(\mathbb{Q})$. This polynomial only has one root in $\mathbb{K}$, so $\operatorname{Aut}(\mathbb{K})$ is such that $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, meaning $\operatorname{Aut}(\mathbb{K}) = \{e\}$.

Example 8.1.2 Let $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. This is generated by the roots of $x^3 - 2 \in \mathbb{Q}[x]$. Then, $G = \operatorname{Aut}(\mathbb{L}) = \operatorname{Aut}(\mathbb{L}/\mathbb{Q}) \leq \operatorname{Sym}\{\omega^i\alpha\} \simeq S_3$. We claim $G \simeq S_3$.[3] Using the tower law, we can deduce that the degree $[\mathbb{L} : \mathbb{Q}] = 6$.

3: Here, ω is the primitive third root of unity and $\alpha = \sqrt[3]{2}$.

Now, we get our answer by the following diagram.

$$\begin{tikzcd}
\mathbb{L} = \mathbb{Q}(\alpha, \omega\alpha) \arrow[r, dashed, "\text{2 choices}"] \arrow[d, dash, "2"'] & \mathbb{L} \arrow[dd, dash] \\
\mathbb{Q}(\alpha) \arrow[ur, dashed, bend right, "\text{3 choices}"'] \arrow[d, dash, "3"'] & \\
\mathbb{Q} \arrow[r, equal] & \mathbb{Q}
\end{tikzcd}$$

Example 8.1.3 Let $g = (x^2 - 2)(x^2 - 3)$ with roots $\pm\sqrt{2}, \pm\sqrt{3}$. Then, $\Sigma = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then,

$$\mathrm{Aut}(\Sigma, \mathbb{Q}) \leq \mathrm{Sym}\{\pm\sqrt{2}, \pm\sqrt{3}\} \simeq S_4$$

has order at most 4. We claim that $\mathrm{Aut}(\Sigma/\mathbb{Q}) \simeq C_2 \times C_2$.

Again, we reason via the diagram.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[r, dashed, "\sqrt{3} \mapsto \pm\sqrt{3}"] \arrow[d, dash, "2"'] & \Sigma \arrow[dd, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[ur, dashed, bend right, "\sqrt{2} \mapsto \pm\sqrt{2}"'] \arrow[d, dash, "2"'] & \\
\mathbb{Q} \arrow[r, equal] & \mathbb{Q}
\end{tikzcd}$$

8.2 Normality

Definition 8.2.1 (Normal Extension) *An extension $\mathbb{L}/\mathbb{F}$ is normal if for all $f \in \mathrm{Irred}(\mathbb{F})$, if f has a root in $\mathbb{L}$, then f splits over $\mathbb{L}$.*[4]

4: As an exercise, show that if $[\mathbb{L} : \mathbb{F}] = 2$, then $\mathbb{L}/\mathbb{F}$ is normal.

Theorem 8.2.1 *A finite extension $\mathbb{L}/\mathbb{F}$ is normal if and only if it is a splitting field of some $f \in \mathbb{F}[x]$.*[5]

5: This actually works for infinite extensions, but that is not what we are interested in.

Proof of $\Rightarrow$. Suppose $\mathbb{L}/\mathbb{F}$ is finite and normal. Then, $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_m)$, algebraic over $\mathbb{F}$. We can form the product of the minimal polynomials

$$f := m_{\alpha_1,\mathbb{F}} \cdot m_{\alpha_2,\mathbb{F}} \cdots m_{\alpha_m,\mathbb{F}} \in \mathbb{F}[x].$$

Since each minimal polynomial splits over $\mathbb{L}$, via normality, f also splits over $\mathbb{L}$, meaning $\mathbb{L} = \mathbb{F}(R_f)$, the roots of f. □

To get the other direction, we need to do some work.

Lemma 8.2.2 *Let* $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{M}$. *Define* $\mathbb{L} := \Sigma_{f/\mathbb{F}}$. *If* $\alpha, \beta \in \mathbb{M}$ *are roots of the same* $g \in \mathrm{Irred}(\mathbb{F})$, *then*

$$[\mathbb{L}(\alpha) : \mathbb{L}] = [\mathbb{L}(\beta) : \mathbb{L}].$$

That is, we have the picture

$$\begin{tikzcd}
 & & \mathbb{M} \arrow[dll, dash, bend right] \arrow[drr, dash, bend left] & & \\
\mathbb{L}(\alpha) \arrow[drr, dash] \arrow[dd, dash] & & & & \mathbb{L}(\beta) \arrow[dll, dash] \arrow[dd, dash] \\
 & & \mathbb{L} \arrow[dd, dash] & & \\
\mathbb{F}(\alpha) \arrow[drr, dash] & & & & \mathbb{F}(\beta) \arrow[dll, dash] \\
 & & \mathbb{F} & &
\end{tikzcd}$$

Proof of $\Leftarrow$. Suppose $\mathbb{L} = \Sigma_{f/\mathbb{F}}$. Suppose $g \in \mathrm{Irred}(\mathbb{F})$ such that $g(\alpha) = 0$, where $\alpha \in \mathbb{L}$. Form $\mathbb{M} := \Sigma_{g/\mathbb{L}}$. Let $\beta \in \mathbb{M}$ such that $g(\beta) = 0$. Applying the lemma,

$$[\mathbb{L}(\alpha) : \mathbb{L}] = [\mathbb{L}(\beta) : \mathbb{L}].$$

□

Proof of Lemma. We claim we have the diagram

$$\begin{tikzcd}
\mathbb{L}(\alpha) \arrow[rr, dashed, "\psi", "\simeq"'] & & \mathbb{L}(\beta) \\
\mathbb{F}(\alpha) \arrow[u, tail] \arrow[rr, dashed, "\varphi", "\simeq"'] & & \mathbb{F}(\beta) \arrow[u, tail] \\
 & \mathbb{F} \arrow[ul, tail] \arrow[ur, tail] &
\end{tikzcd}$$

We know φ exists, because α, β are roots of $g \in \mathrm{Irred}(\mathbb{F})$.[6] □

6: This is a harder proof, but we make a few uses of our theorems about splitting fields and the tower law.

Proposition 8.2.3 *Let* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *be a finite extension. If* $\mathbb{L}/\mathbb{F}$ *is normal, then* $\mathbb{L}/\mathbb{K}$ *is normal.*

Proof. Let $\mathbb{L} := \Sigma_{f/\mathbb{F}}$ for some $f \in \mathbb{F}[x] \subseteq \mathbb{K}[x]$. Then, $\mathbb{L} = \Sigma_{f/\mathbb{K}}$, so $\mathbb{L}/\mathbb{K}$ is normal. □

8.3 Galois Extensions

Definition 8.3.1 (Separable Extension) *An extension $\mathbb{K}/\mathbb{F}$ is separable if every $\alpha \in \mathbb{K}$ is such that $m_{\alpha,\mathbb{F}} \in \mathbb{F}[x]$ is separable.*

Remark 8.3.1 The observation is that in char 0, every algebraic extension is separable.[7]

7: In positive characteristic, that is certainly not true.

Definition 8.3.2 (Galois Extension) *An extension is called Galois if it is both normal and separable.*

Proposition 8.3.1 *A finite extension $\mathbb{L}/\mathbb{F}$ is Galois if and only if it is a splitting field of separable polynomial over $\mathbb{F}$.*

Proof. In char 0, this is clear. ☐

Now, we need a theorem relating the notion of a Galois extension to the theory of embeddings.

Remark 8.3.2 Recall that if we have extensions $\mathbb{K}/\mathbb{F}$, $\mathbb{L}/\mathbb{F}$, then we have the set

$$\mathrm{Emb}_{\mathbb{F}}(\mathbb{K},\mathbb{L}) := \left\{ \begin{array}{c} \mathbb{K} \xrightarrow{\varphi} \mathbb{L} \\ \text{such that } \varphi|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}} \end{array} \right\}.$$

Theorem 8.3.2 (On Embeddings) *Let $\mathbb{K}, \mathbb{L}$ be extensions over $\mathbb{F}$. Let $[\mathbb{K} : \mathbb{F}] < \infty$. Then,*

$$|\mathrm{Emb}_{\mathbb{F}}(\mathbb{K},\mathbb{L})| \leq [\mathbb{K} : \mathbb{F}]$$

with equality saturated if and only if

(i) $\mathbb{K}/\mathbb{F}$ is a separable extension, and
(ii) for all $f \in \mathrm{Irred}(\mathbb{F})$ such that f has a root in $\mathbb{K}$, f splits over $\mathbb{L}$.

We can generalize slightly and use an induction argument. Given an isomorphism $\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}'$ and extensions $\mathbb{K}/\mathbb{F}$ and $\mathbb{L}/\mathbb{F}'$. Then, we can define the set

$$\mathrm{Emb}_{\lambda}(\mathbb{K},\mathbb{L}) := \left\{ \begin{array}{c} \mathbb{K} \xrightarrow{\varphi} \mathbb{L} \\ \text{such that } \varphi|_{\mathbb{F}} = \lambda \end{array} \right\}$$

Then, our statement is in terms of λ, and we want $\lambda(f)$ to split over $\mathbb{L}$ in (ii).[8] We now give a useful lemma for proving our theorem.

8: That is, the theorem is the case $\lambda = \mathrm{id}_{\mathbb{F}}$.

Lemma 8.3.3 *Let $\mathbb{K}/\mathbb{F}$ and $\mathbb{L}/\mathbb{F}'$ be extensions, and $\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}'$ an isomorphism. Then, for any $\alpha \in \mathbb{K}$, we have*

$$|\mathrm{Emb}_{\lambda}(\mathbb{F}(\alpha),\mathbb{L})| \leq [\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_{\alpha,\mathbb{F}} =: m,$$

with equality saturated if and only if

(i) α *is separable over* $\mathbb{F}$, *and*
(ii) $m' := \lambda(m)$ *splits over* $\mathbb{L}$.

Proof. Via our diagram, we see that there is a correspondence

$$\{\varphi \in \mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{L})\} \longleftrightarrow \{\beta \in \mathbb{L} : m'(\beta) = 0\}.$$

□

Proof of Theorem. We will induct on $n := [\mathbb{K} : \mathbb{F}]$. If $n = 1$, then $\mathbb{K} = \mathbb{F}$, so $\mathrm{Emb}_\lambda(\mathbb{F}, \mathbb{L}) = \{\lambda\}$. Suppose $n \geq 2$. Pick $\alpha \in \mathbb{K} \setminus \mathbb{F}$ so $\mathbb{F} \subsetneq \mathbb{F}(\alpha)$. Define $d := [\mathbb{F}(\alpha) : \mathbb{F}]$ and $e := [\mathbb{K} : \mathbb{F}(\alpha)]$, so $n = de > e$. To give $\varphi \in \mathrm{Emb}_\lambda(\mathbb{K}/\mathbb{L})$, choose

(a) $\mu : \mathbb{F}(\alpha) \rightarrowtail \mathbb{L}$ extending λ, as by the lemma, our number of choices is less than or equal to d, and then
(b) given μ, we choose our $\varphi : \mathbb{K} \rightarrowtail \mathbb{L}$ extending μ. Since $e < n$, by induction, there are at most e.

$$\begin{tikzcd}
\mathbb{K} \arrow[r, dashed, "\varphi"] & \mathbb{L} \\
\mathbb{F}(\alpha) \arrow[u, tail] \arrow[r, two heads, "\mu", "\simeq"'] & \mu(\mathbb{F}(\alpha)) \arrow[u, tail] \\
\mathbb{F} \arrow[u, tail] \arrow[r, two heads, "\simeq", "\lambda"'] & \mathbb{F}' \arrow[u, tail]
\end{tikzcd}$$

Our choices amount to

$$|\mathrm{Emb}_\lambda(\mathbb{K}, \mathbb{F})| = \sum_{\mu \in \mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{F})} \left|\mathrm{Emb}_\mu(\mathbb{K}, \mathbb{L})\right| \leq de = n.$$

We now need to show equality for saturation. Suppose (i) and (ii) hold. We want to show that

(i) $\alpha \in \mathbb{K}$ is separable over $\mathbb{F}$; i.e., $m = m_{\alpha,\mathbb{F}}$ is separable, so that $m' = \lambda(m)$ is a separable polynomial.
(ii) m' splits over $\mathbb{L}$, so $d = |\mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{L})|$. We have that (i) implies $\mathbb{K}/\mathbb{F}(\alpha)$ is separable (remember, this is easy in char 0). Also, if $f \in \mathrm{Irred}(\mathbb{F}(\alpha))$ has a root $\beta \in \mathbb{K}$, then $f' := \mu(f)$ must split over $\mathbb{L}$. Because $f \mid m_{\beta,\mathbb{F}}$, we know $\lambda(m_{\beta,\mathbb{K}})$ splits over $\mathbb{L}$, by the hypothesis. Thus, $\mu(m_{\beta,\mathbb{F}(\alpha)}) = f$, so the hypothesis of the theorem applies to $\mathbb{K}/\mathbb{F}(\alpha)$, meaning $\left|\mathrm{Emb}_\mu(\mathbb{K}, \mathbb{L})\right| = e$. We now need the converse. Suppose

$$|\mathrm{Emb}_\lambda(\mathbb{K}, \mathbb{L})| = n = [\mathbb{K} : \mathbb{F}].$$

Consider $\alpha \in \mathbb{K}$, giving us a tower

$$\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}.$$

Define d to be the degree of the left-hand side degree, and e for the right-hand side degree. Then,

$$0 \leq |\mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{L})| \leq d$$

and

$$0 \leq |\mathrm{Emb}_\lambda(\mathbb{K}, \mathbb{L})| \leq e.$$

Well, we have

$$de = n = |\mathrm{Emb}_\lambda(\mathbb{K}, \mathbb{L})| = \sum_{\mu \in \mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{L})} \left|\mathrm{Emb}_\mu(\mathbb{K}, \mathbb{F}),\right|$$

meaning $|\mathrm{Emb}_\lambda(\mathbb{F}(\alpha), \mathbb{L})| = d$, so $m_{\alpha,\mathbb{F}}$ is separable and so is its image $\lambda(m_{\alpha,\mathbb{F}})$ over $\mathbb{L}$.

$\square$

$$\begin{tikzcd}
\mathbb{K} \arrow[r, dashed, "\varphi"] & \mathbb{L} \\
\mathbb{F} \arrow[u, hook] \arrow[r, "\lambda", "\simeq"'] & \mathbb{F}' \arrow[u, hook]
\end{tikzcd}$$

Figure 8.1: Diagram for new embedding set

Corollary 8.3.4 *Let $\mathbb{L}/\mathbb{F}$ be finite. Then, $|\mathrm{Aut}(\mathbb{L}/\mathbb{F})| \leq [\mathbb{L} : \mathbb{F}]$, with equality saturated if and only if $\mathbb{L}/\mathbb{F}$ is Galois.*

Proof. We take the theorem with $\mathbb{K} = \mathbb{L}$. $\square$

Remark 8.3.3 We essentially just showed that finite $\mathbb{L}/\mathbb{F}$ is Galois if and only if

$$|\mathrm{Aut}(\mathbb{L}/\mathbb{F})| = [\mathbb{L} : \mathbb{F}].$$

In general, we only have $\leq$.

Definition 8.3.3 (Galois Group) *In the case of a Galois extension, we write* $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) := \mathrm{Aut}(\mathbb{L}/\mathbb{F})$.

Note that if we have $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$, then we get sub extensions $\mathbb{K}/\mathbb{F}$ and $\mathbb{L}/\mathbb{K}$. It turns out that if the big extension is Galois, so is the top sub extension:

$$\begin{tikzcd}
\mathbb{L} \arrow[d, dash, "\text{Galois}"'] \arrow[dd, dash, bend left, "\text{Galois}"] \\
\mathbb{K} \arrow[d, dash, "\text{sep, not norm}"'] \\
\mathbb{F}
\end{tikzcd}$$

Remark 8.3.4 Let $\mathbb{K}$ be an intermediate field. Then, $\mathbb{L}/\mathbb{K}$ is Galois, with

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \leq G,$$

where $H \leq G$ implies

$$\mathbb{L}^H := \{\alpha \in \mathbb{L} : h(\alpha) = \alpha \text{ for all } h \in H\}$$

is an intermediate field.

8.4 Galois Correspondence

Recall that we have $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$. We need one further *lemma*, which says that $G \leq \mathrm{Aut}(\mathbb{L})$ and $|G| < \infty$ implies $[\mathbb{L} : \mathbb{L}^G] = |G|$.[9]

9: We may omit this.

Theorem 8.4.1 (Basic Galois Correspondence) *Let $\mathbb{L}/\mathbb{F}$ be a finite Galois extension. Define $G := \mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Then, we have a correspondence*

$$\{H \leq G\} \longleftrightarrow \left\{ \begin{matrix} \textit{intermediate fields} \\ \textit{of } \mathbb{L}/\mathbb{F} \end{matrix} \right\},$$

with operations of the bijection given by $H \mapsto \mathbb{L}^H$ in the forward direction, and $\mathbb{K} \mapsto \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ in the backward direction.

Remark 8.4.1 (Order Reversal of Galois Correspondence) Note that $H \subseteq H'$ implies $\mathbb{L}^H \supseteq \mathbb{L}^{H'}$. Thus, $\mathbb{K} \subseteq \mathbb{K}'$ implies $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \supseteq \mathrm{Gal}(\mathbb{L}/\mathbb{K}')$.

Proof of Theorem. If we have $H \leq G$, then $\mathbb{L}^H \subseteq \mathbb{L}/\mathbb{F}$, so we have $\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H) \supseteq H$. Then, using the embedding theorem and the technical lemma,

$$\left|\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H)\right| = [\mathbb{L} : \mathbb{L}^H] = |H|.$$

On the other hand, if $\mathbb{K} \subseteq \mathbb{L}/\mathbb{F}$, then $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \leq G$, so $\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} \subseteq \mathbb{L}/\mathbb{F}$. Note that $\mathbb{K} \subseteq \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}$. Well, again via the technical lemma and embedding theorem,

$$[\mathbb{L} : \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}].$$

Then, $\mathbb{K} \subseteq \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} \subseteq \mathbb{L}$, so by the tower law, we are done. $\square$

Theorem 8.4.2 (Degree Correspondence) *If $\mathbb{K} \subseteq \mathbb{L}/\mathbb{F}$, then $[\mathbb{L} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$, and with $H \leq G$ corresponding to $\mathbb{K}$, we have $[\mathbb{L} : \mathbb{K}] = |H|$. Finally, $[\mathbb{K} : \mathbb{F}] = |G : H|$, the index of the corresponding groups.*

Theorem 8.4.3 (Lattice Correspondence) *If $H_1 \leftrightarrow \mathbb{K}_1$ and $H_2 \leftrightarrow \mathbb{K}_2$, then $H_1 \cap H_2 \leftrightarrow \mathbb{K}_1\mathbb{K}_2$ and $\langle H_1 \cup H_2 \rangle \leftrightarrow \mathbb{K}_1 \cap \mathbb{K}_2$.*

Proposition 8.4.4

(i) If $g \in G$ and $\mathbb{K} \subseteq \mathbb{L}/\mathbb{F}$, then $\mathbb{K}' = g(\mathbb{K})$ if and only if $H' = gHg^{-1}$, where $H \leftrightarrow \mathbb{K}$ and $H' \leftrightarrow \mathbb{K}'$.[10]
(ii) $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \simeq \mathcal{N}_G(H)/H$.
(iii) $\mathbb{K}/\mathbb{F}$ is Galois if and only if $H \trianglelefteq G$. If so, then $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) \simeq G/H$.

10: That it, we can move between the fields if and only if the corresponding Galois groups are *conjugate*.

Example 8.4.1 Let $f := (x^2-2)(x^2-3) \in \mathbb{Q}[x]$. The roots are $\alpha_{1,2} = \pm\sqrt{2}$ and $\alpha_{3,4} = \pm\sqrt{3}$. We have a field $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then

$$G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle (1\ 2), (3\ 4) \rangle \leq S_4.$$

Note that $\alpha := \sqrt{2} + \sqrt{3}$ is *not* fixed by any of the 3 non-identity elements of G. Thus, $\mathbb{Q}(\alpha) = \mathbb{L}$.

$$\begin{tikzcd}
& \{e\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle(3\ 4)\rangle \arrow[dr, dash, "2"'] & \langle(1\ 2)(3\ 4)\rangle \arrow[d, dash, "2"] & \langle(1\ 2)\rangle \arrow[dl, dash, "2"] \\
& G &
\end{tikzcd}$$

Figure 8.2: Lattice of intermediate subgroups, inverted

$$\begin{tikzcd}
& \mathbb{L} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Figure 8.3: Lattice of intermediate fields

Example 8.4.2 Let $f := x^4 + x^3 + x^2 + x + 1$. We have that $(x-1)f = x^5 - 1$. The roots are $\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$, labeling these $\alpha_1, \ldots, \alpha_4$, respectively. Now, $\mathbb{L} = \mathbb{Q}(\zeta)$, and $[\mathbb{L} : \mathbb{Q}] = \varphi(5) = 4$. If $g \in G$, and $g : \zeta \mapsto \zeta^k$ for some $k \in [4]$, then $g : \zeta^j \mapsto \zeta^{kj}$. Clearly, we have a four-cycle $g : \zeta \mapsto \zeta^2$, meaning $G = \langle(1\ 2\ 3\ 4)\rangle \simeq C_4 \leq S_4$.

$$\begin{tikzcd}
\{e\} \arrow[d, dash, "2"'] & & \mathbb{L} = \mathbb{Q}(\zeta) \arrow[d, dash, "2"'] \\
\langle(1\ 4)(2\ 3)\rangle \arrow[d, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[d, dash, "2"'] \\
G & & \mathbb{Q}
\end{tikzcd}$$

Figure 8.4: Lattice of intermediate groups (left), inverted, and lattice of intermediate fields (right)

How do we find α? We can write $\alpha := \zeta + \zeta^{-1}$, and doing some algebra, we can show that it must satisfy $\alpha^2 + \alpha - 1 = 0$, taking the positive root $\alpha = (1 + \sqrt{5})/2$.

Example 8.4.3 Let $f := x^2 - 2 \in \mathbb{Q}x$. Take $\alpha_1 = \alpha$, $\alpha_2 = \alpha\omega$, and $\alpha_3 = \alpha\omega^2$. Then, $G = S_3$.

Example 8.4.4 Define the polynomial $f := x^6+x^5+x^4+x^3+x^2+x+1 \in \mathrm{Irred}(\mathbb{Q})$. If we write $\zeta := \zeta_7$, then the roots are $\alpha_k := \zeta^k$, for $k \in [6]$.[11]

11: Then, $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/7)^\times \simeq C_6 \leq S_6$. Our best way to do this is $\varphi(\zeta) = \zeta^3 \leftrightarrow (1\ 3\ 2\ 6\ 4\ 5) =: \varphi$.

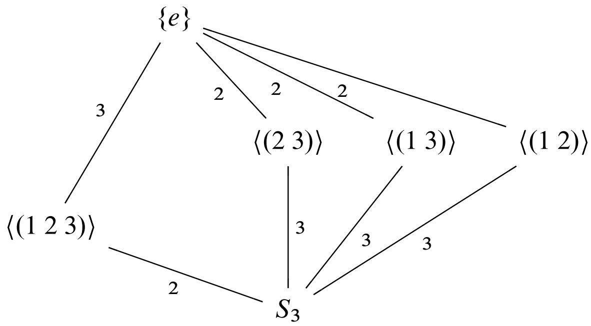

Figure 8.5: Lattice of intermediate subgroups, inverted

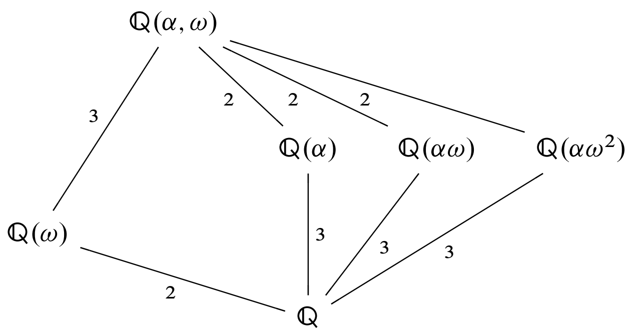

Figure 8.6: Lattice of intermediate field

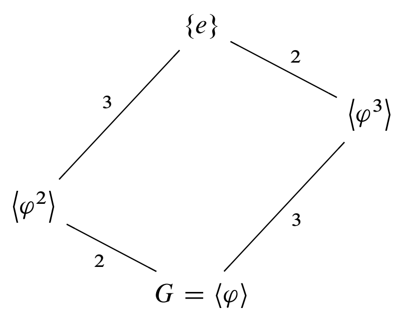

Figure 8.7: Lattice of subgroups, inverted

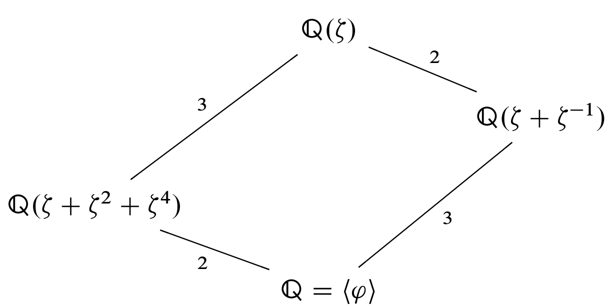

Figure 8.8: Lattice of intermediate fields