These are some notes from my Algebra I class. We use the textbook *Abstract Algebra* by Dummit and Foote, and will cover rings, groups, and modules.

Contents

PIDs, UFDs and All That

We always assume here that R is commutative and unital.

Preliminaries

Definition: If $a_1, \dots, a_n \in R$, then the *ideal generated by* $a_1, \dots, a_n$ is given by

$$(a_1, \dots, a_n) \coloneqq \bigcap \{I \mid a_1, \dots, a_n \in I, I \text{ is an ideal in } R\}.$$

An ideal is called *principal* if $I = (a)$ for some $a \in I$. We may write $I = a \cdot R$ in this case. A ring where every ideal is principal is called a *principal ideal domain*.

Definition: If I and J are ideals in R, then IJ is given by

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in I, y_i \in J, n \in \mathbb{N} \right\}.$$

Theorem (Isomorphism Theorems for Rings)**:**

First Isomorphism Theorem: Let $\varphi \colon R \to S$ be a ring homomorphism. Then, $\overline{\varphi} \colon R/\ker(\varphi) \to \operatorname{im}(\varphi)$ is an isomorphism given by $\overline{\varphi}(a + \ker(\varphi)) = \varphi(a)$.

Second Isomorphism Theorem: Let R be a ring, $S \subseteq R$ a subring, and let $I \subseteq R$ be an ideal. Then,

(i) $I + S$ is a subring of R;

(ii) I is an ideal of $I + S$;

(iii) $I \cap S$ is an ideal of S;

(iv) $S/I \cap S \cong I + S/I$.

Third Isomorphism Theorem: Let R be a ring, I, J ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I, and we have $(R/I)/(J/I) \cong R/J$.

Fourth Isomorphism Theorem: If R is a ring and I is an ideal, then there is a one-to-one correspondence between subrings of R/I and subrings of R containing I.

Definition: Let M be an ideal in R.

(i) We say M is prime if $M \neq R$ and, for any $ab \in M$, we have either $a \in M$ or $b \in M$.

(ii) We say M is maximal if $M \neq R$ and if $M \subseteq I \subseteq R$ where I is an ideal, then either $I = M$ or $I = R$.

Theorem: Let M be an ideal in R.

(i) M is prime if and only if R/M is an integral domain.

(ii) M is maximal if and only if R/M is a field.

Proof.

(i) Let M be maximal, with $a + M \in R/M$, $a + M \neq 0 + M$. Then, $a \notin M$, so that the ideal $(a) + M$ strictly contains M. Therefore, $1 + M \in (a) + M$, meaning there is some $r + M$ such that $(r + M)(a + M) = 1 + M$. Thus, an inverse exists.

Now, if R/M is a field, and $M \subsetneq I \subseteq R$, then I/M is an ideal of R/M, and since $I \supsetneq M$, we have $I/M \neq 0 + M$. Since R/M is a field, its only ideals are either $0 + M$ and R/M, so $I/M = R/M$, meaning $I = R$.

(ii) We have $P \subseteq R$ is prime if and only if $ab \in P$ implies $a \in P$ or $b \in P$. Yet, means that $ab + P = 0 + P$ if and only if $a = 0 + P$ or $b = 0 + P$.

□

Chinese Remainder Theorem

Definition: We say two ideals I and J are *coprime* if $I + J = R$, or that there exist $x \in I$ and $y \in J$ such that $x + y = 1$.

Theorem (Chinese Remainder Theorem)**:** Let $I_1, \ldots, I_n$ be pairwise coprime ideals of R. Then, for any $a_1, \ldots, a_n \in R$, there exists $x \in R$ with $x \equiv a_i$ modulo I_i for all i. In other words, there a solution to the system of congruences given by

$$\begin{aligned} x + I_1 &= a_1 + I_1 \\ x + I_2 &= a_2 + I_2 \\ &\vdots \\ x + I_n &= a_n + I_n. \end{aligned}$$

Proof. It suffices to construct elements $y_1, \ldots, y_n$ such that $y_i \equiv 1$ modulo I_i and 0 otherwise. Then, we will be able to set $x = \sum_i a_i y_i$ as our desired solution.

We construct y_1 as follows. From our assumption, $I_1 + I_j = R$ for all $j \geqslant 2$, so for each $j \geqslant 2$, there exists $u_j \in I_1$ and $v_j \in I_j$ such that $u_j + v_j = 1$. Taking the product, we find that

$$\prod_{j=2}^{n} (u_j + v_j) = 1$$

$$= \underbrace{v_2 \cdots v_n}_{=:y_1} \underbrace{+ \cdots + u_2 \cdots u_n}_{=:x_1}.$$

We verify that y_1 does the job, which we can see by the fact that $y_1 \equiv 0$ modulo I_j for $j \neq 1$, as $v_2 \cdots v_j \in I_2 \cdots I_j \subseteq I_j$ for each $j \geqslant 2$. Similarly, each summand in x_1 contains at least one u_j, so $x_1 \equiv 0$ modulo I_1.

The rest of the y_i follow analogously. □

We can restate the Chinese Remainder Theorem in a variety of ways.

Theorem (Chinese Remainder Theorem, Alternative Versions)**:** Let $I_1, \ldots, I_n$ be pairwise coprime ideals.

(i) There exists a surjective homomorphism

$$\begin{aligned} \varphi \colon R &\to R/I_1 \times \cdots \times R/I_n \\ r &\mapsto (r + I_1, \ldots, r + I_n). \end{aligned}$$

This homomorphism induces an isomorphism

$$\overline{\varphi} \colon R/(I_1 \cap \cdots \cap I_n) \to R/I_1 \times \cdots \times R/I_n.$$

(ii) If $I_1, \ldots, I_n$ are pairwise coprime, then

$$R/I_1 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n$$

are isomorphic.

Example: We observe that if $R = \mathbb{Z}$, and $p_1, \ldots, p_r$ are distinct primes with $\ell_1, \ldots, \ell_r$ positive integers, then

$$\mathbb{Z}/p_1^{\ell_1} \cdots p_r^{\ell_r}\mathbb{Z} \cong \mathbb{Z}/p_1^{\ell_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\ell_r}\mathbb{Z}.$$

Example (Polynomial Interpolation)**:** If we let

$$p_i(x) = x - \alpha_i,$$

where $\alpha_i \in \mathbb{F}$, we observe that there is a surjective evaluation homomorphism

$$\mathrm{ev} \colon \frac{\mathbb{F}[x]}{(p_i(x))} \to \mathbb{F},$$

given by $f(x) \mapsto f(\alpha_i)$. In particular, if $\alpha_1, \ldots, \alpha_r$ are distinct, then

$$\frac{\mathbb{F}[x]}{(p_1(x), \ldots, p_r(x))} \cong \mathbb{F} \times \cdots \times \mathbb{F},$$

so that, for all $\beta_1, \ldots, \beta_r \in \mathbb{F}$, there is some $f(x) \in \mathbb{F}[x]$ such that $f(\alpha_i) = \beta_i$ for $i = 1, \ldots, r$.

Field of Fractions and Localization

Given a ring R, how can we find maximal ideals in R? More specifically, given a commutative ring R with 1, and prime ideal $P \subseteq R$, we want to construct a new ring R_P with unique maximal ideal P.

Toward this end, we start by reviewing a useful construction known as the field of fractions.

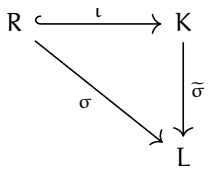
Definition: Let R be an integral domain. We define the field $K = \mathrm{frac}(R)$ to be the unique field with an

injection

$$\begin{aligned} \iota\colon R &\hookrightarrow K \\ 1_R &\mapsto 1_K, \end{aligned}$$

satisfying the following universal property.

Given any embedding into a field, $\sigma\colon R \hookrightarrow L$, such that $1_R \mapsto 1_L$, there is a unique extension $\widetilde{\sigma}\colon K \to L$ such that the following diagram commutes.



In order to construct K, we let $S \subseteq R \times R$ be defined by

$$S = \{(a, b) \mid b \neq 0\}.$$

We impose an equivalence relation on S by saying $(a, b) \sim (c, d)$ if and only if $ad - bc = 0$. Clearly, this relation is reflexive and symmetric. To see that it is transitive, we let $(a, b) \sim (c, d)$, and $(c, d) \sim (e, f)$, meaning $ad - bc = 0$ and $cf - de = 0$. Multiplying the first equation by f and the second equation by b, then subtracting, we get $adf - bde = 0$, meaning $d(af - be) = 0$. Since R admits no zero divisors, this means that $af - be = 0$, so the relation is transitive.

We write $[(a, b)] = \frac{a}{b}$ for K, with operations

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

These operations are well-defined and do satisfy the universal property. Verifying this is a pain, but it can be done.

Now, we may extend this to all unital commutative rings, not just integral domains.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$. We say S is *multiplicative* if

- $1 \in S$;
- $0 \notin S$;
- for any $x, y \in S$, $xy \in S$.

Example:

(i) If R is an integral domain, then $R \setminus \{0\}$ is multiplicative.

(ii) If $z \in R$ is such that z is not nilpotent, then $S = \{z^n \mid n \geqslant 0\}$ is multiplicative.

(iii) If P is a prime ideal, then $S = R \setminus P$ is multiplicative.

We will use (iii) to construct a ring with a unique maximal ideal. First, though, we construct a ring of fractions using multiplicative sets.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$ be multiplicative. We construct a ring $S^{-1}R$ by taking an equivalence relation on $R \times S$ as follows:

$$(a, s) \sim (b, t) \Leftrightarrow \exists s' \in S \text{ such that } s'(at - bs) = 0.$$

We write

$$S^{-1}R = \{[(a, s)] \mid a \in R, s \in S\},$$

and denote

$$[(a, s)] = \frac{a}{s}.$$

This becomes a ring under the operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

We call $S^{-1}R$ the *localization of* R *with respect to* S.

We can see some basic properties of the localization.

Proposition: Let R be a unital commutative ring, $S \subseteq R$ multiplicative, and let $S^{-1}R$ be the corresponding localization.

- The additive identity in $S^{-1}R$ is $\frac{0}{1}$.
- The additive inverse of $\frac{a}{s}$ in $S^{-1}R$ is $\frac{-a}{s}$.
- For all $a \in R$ and all $s, s' \in S$, we have $\frac{as'}{ss'} = \frac{a}{s}$.
- Every element of the form $\frac{s}{t}$ where both $s, t \in S$ is invertible, with corresponding inverse $\frac{t}{s}$.
- The map $\iota_S : R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$ is an injective ring homomorphism such that $\iota_S(S) \subseteq (S^{-1}R)^\times$, where $(S^{-1}R)^\times$ denotes the group of invertible elements in $S^{-1}R$.

Unique Factorization Domains

Definition: A ring R is called *Noetherian* if, for any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there is some index N such that for all $m \geqslant N$, $I_m = I_N$.

Proposition: The following are equivalent:

- R is Noetherian;
- every ideal in R is finitely generated.

Proof. Let R be Noetherian. Suppose toward contradiction that there exists I that is not finitely generated. Then, I is nonzero, so there is $\alpha_1 \in I$ such that $I_1 = (\alpha_1)$ is nonzero. Since I is not finitely generated, $I \neq I_1$, so there is $\alpha_2 \in I \setminus I_1$, so that $I_2 = (\alpha_1, \alpha_2)$ is such that $I_1 \subseteq I_2$. Inductively, we generate $I_n = (\alpha_1, \ldots, \alpha_n)$ such that $I_{n-1} \subsetneq I_n$, implying that we have a strictly ascending chain of ideals, which is a contradiction.

Suppose every ideal in R is finitely generated. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I = \bigcup I_n$ be their union. By assumption, I is finitely generated, so we have $I = (\alpha_1, \ldots, \alpha_N)$ for some $\alpha_1, \ldots, \alpha_N \in R$. Yet, since I is the union of all these ideals, there is some M such that $\alpha_1, \ldots, \alpha_N \in I_M$, meaning the chain stabilizes. □

Corollary: If R is a principal ideal domain, then R is Noetherian.

Definition: Let R be an integral domain.

(i) Two elements $a, b \in R$ are called *associated* if $a = bu$ for some unit (invertible) element $u \in R$. Equivalently, a and b are associated if $(a) = (b)$

(ii) An element $a \in R$ is called *irreducible* if

- a is not a unit element;
- whenever $a = bc$ for some $b, c \in R$, then one of b or c is a unit.

(iii) An element a is called *prime* if $a \neq 0$, $a \notin R^\times$, and (a) is prime. Equivalently, a is prime if, whenever $a|bc$, it follows that $a|b$ or $a|c$, where divisibility in R is defined traditionally (i.e., there exists $z \in R$ such that $az = b$).

Note: Prime elements are irreducible, but not necessarily vice versa.

The question then arises: when are irreducibles prime?

Definition: We say $a \in R$ with $a \neq 0$, $a \notin R^\times$ has a *unique factorization* into irreducibles if

(i) we may write $a = up_1 \cdots p_r$, where u is a unit and $p_1, \ldots, p_r$ are irreducible;

(ii) for any other such factorization

$$\begin{aligned} a &= u \prod_{i=1}^{r} p_i \\ &= v \prod_{j=1}^{s} q_j, \end{aligned}$$

where p_i, q_j are irreducible and u, v are units, we have

- $r = s$;
- upon permutation of factors, p_i and q_i are associated.

We call R a *unique factorization domain* if, for any $a \in R$ with $a \neq 0$, $a \notin R^\times$, a has unique factorization into irreducibles.

Proposition: If R a Noetherian ring, then every $a \in R$ with $a \neq 0$ and $a \notin R^\times$ admits a factorization into irreducibles.

Proof. First, we show that every such a has an irreducible factor or divisor. If a is itself irreducible, then we are done. Else, there are $b, c \in R$ with $a = bc$ and neither a nor b a unit. In particular, this means that $(a) \subsetneq (b)$. Inductively, if b is not irreducible, then we may find b_2, c_2 such that $b = b_2c_2$, meaning that $(b) \subsetneq (b_2)$, and so on and so forth.

This gives a chain of ideals

$$(a) \subsetneq (b) \subsetneq (b_2) \subsetneq \cdots$$

that eventually stabilizes, meaning that there is some b_N such that b_N is irreducible.

Now, we may show that a admits a factorization. If $a = bc$ with b irreducible (as we showed previously), then if c is not irreducible, we may take $c = b_1c_1$ and create this same chain of ideals

$$(c) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots$$

using the Noetherian condition to end up at an irreducible or a unit. □

The main issue facing general Noetherian rings is that the uniqueness of the factorization may go awry.

Example: For instance, in the ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$, there is not unique factorization. For instance, we may write

$$6 = (2)(3)$$

$$= \left(1+\sqrt{-5}\right)\left(1+\sqrt{-5}\right),$$

where we may see that all of these are irreducible as follows. Define a norm on $\mathbb{Z}\left[\sqrt{-5}\right] \subseteq \mathbb{C}$ by $N\left(a+b\sqrt{-5}\right) = a^2+5b^2$, where this norm is multiplicative as it is inherited from $\mathbb{C}$.

Lemma: If N is a norm on the ring $R = \mathbb{Z}\left[\sqrt{-D}\right]$, where D is a square-free positive integer, then $u \in R$ is an invertible (or unit) element if and only if $N(u) = 1$.

Proof of Lemma. If $v \in R$ is such that $uv = 1$, then $N(uv) = N(u)N(v) = 1$, meaning that both $N(u)$ and $N(v)$ are 1.

Meanwhile, if $N(u) = 1$, then $1 = u\overline{u}$, meaning that $\overline{u} = u^{-1}$. □

We may show that 2 is irreducible relatively quickly. Observe that if there were a factorization of $2 = ab$ into irreducibles, then $4 = N(a)N(b)$ would hold, with neither $N(a)$ nor $N(b)$ being equal to 1. This would mean that $N(a) = 2$ for some $a = x + y\sqrt{-5}$, or that $x^2 + 5y^2 = 2$. Yet, reducing modulo 5, this implies that $x^2 \equiv 2$ modulo 5, yet the only squares in $\mathbb{Z}/5\mathbb{Z}$ are 1 and 4.

Given a factorization, there is a simple way to classify the uniqueness of the factorization.

Proposition: Let $a \in R$ be such that $a \neq 0$ and $a \notin R^\times$. If a admits a factorization

$$a = up_1 \cdots p_r,$$

with $p_1, \ldots, p_n$ *prime*, then this factorization is unique (up to associates).

Proof. Suppose a admits another factorization,

$$a = vq_1 \cdots q_s,$$

where $q_1, \ldots, q_s$ are irreducible and v is a unit. Then, we have

$$up_1 \cdots p_r = vq_1 \cdots q_s,$$

meaning that p_1 divides $vq_1 \cdots q_s$. Since p_1 is prime, $p_1 | q_j$ for some j, meaning that $q_j = v_1 p_1$ for some $v_1 \in R$. Yet, since q_j is irreducible, it follows that v_1 is a unit. By permuting elements, we may say that p_1 and q_1 are associated, so we have

$$up_1 \cdots p_r = vv_1 p_1 q_2 \cdots q_s.$$

Now, since R is a domain, it admits the cancellation property, so we may then write

$$up_2 \cdots p_r = vv_1 q_2 \cdots q_s.$$

Proceeding in this fashion, we observe first that $r \leqslant s$, as else, we would have p_i dividing a unit for R, which is not allowed. Thus, we find

$$u = vv_1 \cdots v_r q_{r+1} \cdots q_s.$$

Similarly, this means there cannot be any more q_j, or else the q_j would be a unit. Thus, these are the same factorizations (up to associates). □

Theorem: If a domain R is a principal ideal domain, then R is a unique factorization domain.

Proof. First, we show that if $a \in R$ is irreducible, then a is prime.

Observe that (a) is then contained in a maximal ideal M, where $M = (p)$ for some $p \in R$ with p not a unit. Since M is maximal, M is prime, so that p is prime, and $(a) \subseteq (p)$. Observe then that $a = pu$ for some $u \in R$; since a is irreducible and p is not a unit, it must be the case that u is a unit. Thus, $(a) = (p)$,

so that a is prime.

Now, since R is a principal ideal domain, every element in R admits a factorization into irreducibles, and all irreducibles are prime. Therefore, the factorization is unique by the above lemma. □

Euclidean Domains

Definition: An integral domain R is called a *Euclidean Domain* if there exists $N\colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ such that for all $a, b \in R$, with $b \neq 0$, there exist $q, r \in R$ such that

- $a = qb + r$;
- either $r = 0$ or $N(r) < N(b)$.

Example:

- Any field admits the vacuous norm, $N(k) = 0$ for all $k \in F \setminus \{0\}$.
- The ring $R = \mathbb{Z}$ is Euclidean with the norm $N(n) = |n|$.
- The ring $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field, is Euclidean with norm $N\colon \mathbb{F}[x] \setminus \{0\} \to \mathbb{N}$ given by $N(f) = \deg(f)$.

Theorem: If R is Euclidean, then R is a principal ideal domain.

Proof. Let $I \subseteq R$ be an ideal. If $I = \{0\}$, then I is principal and we are done.

Else, suppose $I \neq 0$. There exists $\alpha \in I$ with $\alpha \neq 0$, so that $N(\alpha)$ is well-defined. Let $b \in I$ be such that $N(b)$ is minimal for all possible elements of I.

We claim that $I = (b)$. Let $a \in I$ be arbitrary, and perform Euclidean division on a by b, yielding

$$a = qb + r,$$

where $r = 0$ or $N(r) < N(b)$.

If $r \neq 0$, then $N(r) < N(b)$, but $r = a - bq \in I$, which would contradict minimality of $N(b)$, so that $r = 0$, and thus $a = bq \in (b)$. □

Theorem: The Gaussian integers, $\mathbb{Z}[i]$, are Euclidean with norm

$$N(a + bi) = a^2 + b^2.$$

Proof. Observe that N is multiplicative. If we let $\alpha = a + bi$ and $\beta = c + di$ with $\alpha, \beta \neq 0$, we want to show that there exist γ and δ such that $\alpha = \beta\gamma + \delta$ and $\delta = 0$ or $N(\delta) < N(\beta)$.

Consider $\frac{\alpha}{\beta} \in \mathbb{C}$, so that

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{(a + bi)(c - di)}{c^2 + d^2} \\ &= \frac{(a + bi)(c - di)}{N(\beta)} \\ &=: x + yi,\end{aligned}$$

so that $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$.

Now, we can find $x_0, y_0 \in \mathbb{Z}$ such that $|x - x_0| \leqslant \frac{1}{2}$ and $|y - y_0| \leqslant \frac{1}{2}$. Setting $\delta = x_0 + y_0 i$, we have that $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$. We claim that if $\delta \neq 0$, then $N(\delta) < N(\beta)$.

Observe that since N is multiplicative, this condition is equivalent to $N\left(\frac{\delta}{\beta}\right) < 1$. We observe that

$$\begin{aligned} N\left(\frac{\delta}{\beta}\right) &= N\left(\frac{\alpha - \beta\gamma}{\beta}\right) \\ &= N\left(\frac{\alpha}{\beta} - \gamma\right) \\ &= (x - x_0)^2 + (y - y_0)^2 \\ &\leqslant \frac{1}{2} \\ &< 1. \end{aligned}$$

□

Remark: While the remainder in Euclidean division for $\mathbb{Z}$ and $\mathbb{F}[x]$ *is* unique, this is not the case for general Euclidean domains. For instance, if we want to divide $a = 1 + i$ by $b = 2$ in $\mathbb{Z}[i]$ with our previously specified norm, we find that

$$\begin{aligned} 1 + i &= 2 \cdot 0 + (1 + i) \\ &= 2 \cdot 1 + (-1 + i), \end{aligned}$$

both of which satisfy the conditions for Euclidean division.

Now, in any PID (really, any UFD), we can talk about a greatest common divisor. In a principal ideal domain, the GCD for $a, b \in R$ is given by the unique (up to associates) element d such that

$$(a, b) = (d).$$

Meanwhile, greatest common divisors in a UFD are slightly more complicated. If we have two elements $a, b \in R$ with prime factorizations

$$\begin{aligned} a &= up_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} \\ b &= vp_1^{w_1} p_2^{w_2} \cdots p_n^{w_n}, \end{aligned}$$

then the greatest common divisor is given by

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(v_i, w_i)}.$$

This is defined up to associates, similar to how the factorization of any element is defined up to associates.

Unique Factorization in Polynomial Rings

Our goal is to prove that if R is a UFD, then $R[x]$ is a UFD.

We do this by first discussing irreducibility in $R[x]$, including a full characterization of irreducible elements.

Definition: Assume R is a unique factorization domain, and let $0 \neq f(x) \in R[x]$. Writing

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

we define the *content* of f, written $c(f)$, to be

$$c(f) = \gcd(a_0, a_1, \ldots, a_n).$$

Proposition (Gauss's Lemma)**:** Let R be a UFD, and let $f(x), g(x) \in R[x]$ be nonzero polynomials. Then,

$$c(fg) = c(f)\, c(g).$$

Proof. For any nonzero polynomial $h \in R[x]$, we may write

$$h(x) = c(h)z(x),$$

where $c(z) = 1$, simply by factoring. Thus, writing

$$\begin{aligned} f(x) &= c(f)u(x) \\ g(x) &= c(g)v(x), \end{aligned}$$

where $c(u) = c(v) = 1$, hence

$$\begin{aligned} c(fg) &= c(c(f)\,c(g)uv) \\ &= c(f)\,c(g)\,c(uv). \end{aligned}$$

We want to show that $c(u(x)v(x)) = 1$ (up to associates).

Suppose not. Since $c(uv)$ is nonzero and (assumed to be) not a unit, we may find a prime p such that $p \mid c(uv)$. That is, we may find p such that p divides all coefficients of $u(x)v(x)$.

Consider now the reduction homomorphism

$$\pi\colon R[x] \to (R/(p))[x],$$

where we reduce all coefficients modulo (p). Since p is prime, (p) is prime, so that $R/(p)$ is an integral domain, meaning that $(R/(p))[x]$ is an integral domain.

Since $c(u) = c(v) = 1$, it follows that $\pi(u(x)) \neq 0$ and $\pi(v(x)) \neq 0$, as at least one coefficient in $u(x)$ or $v(x)$ is not divisible by p. Thus, in $(R/(p))[x]$ is a domain, it follows that $\pi(u(x))\pi(v(x)) \neq 0$. Yet, since π is a homomorphism, it follows that $0 = \pi(u(x)v(x)) = \pi(u(x))\pi(v(x))$, since we assumed that p divides all the coefficients of $u(x)v(x)$. □

Corollary (Gauss's Lemma, Redux)**:** Let R be a UFD, and let $F = \text{frac}(R)$. Let $f(x) \in R[x]$, and assume $f(x)$ is reducible in $F[x]$. Then, $f(x)$ is reducible in $R[x]$.

Proof. Let $f(x)$ be reducible in $F[x]$, so that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are nonconstant polynomials in $F[x]$.

By factoring, we have

$$\begin{aligned} g(x) &= \frac{a}{b}u(x) \\ h(x) &= \frac{c}{d}v(x), \end{aligned}$$

where $a, b, c, d \in R \setminus \{0\}$, $u(x), v(x) \in R[x]$, and $c(u) = c(v) = 1$.

Substituting this information into the expression for $f(x)$, we have

$$\begin{aligned} f(x) &= \frac{ac}{bd}u(x)v(x) \\ bdf(x) &= acu(x)v(x), \end{aligned}$$

so that

$$bd\,c(f) = ac\,c(u)\,c(v).$$

meaning

$$bd\,c(f) = ac.$$

In particular, this means that $\frac{ac}{bd}$ is a valid representative for $c(f)$, so that $\frac{ac}{bd} \in R$. Therefore,

$$f(x) = \left(\frac{ac}{bd}u(x)\right)v(x),$$

both nonconstant and in $R[x]$, meaning $f(x)$ has a nontrivial factorization in $R[x]$, and thus f is reducible. □

Corollary (Classification of Irreducibles)**:** Let R be a UFD, let $F = \text{frac}(R)$, and let $f(x) \neq 0 \in R[x]$.

(i) If $f(x)$ is constant, then f is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in R.

(ii) If $f(x)$ is not constant, then f is irreducible in $R[x]$ if and only if $c(f) = 1$ and $f(x)$ is irreducible in $F[x]$.

Proof.

(i) Observe that $R[x]$ and R have the same units (since R is an integral domain, and so admits no nilpotent elements), meaning that the product of two nonzero polynomials is a constant if and only if the polynomials themselves are constant.

(ii) Let f be nonconstant. If f is irreducible in $R[x]$, then we may write

$$f(x) = c(f)u(x),$$

where $u(x)$ is nonconstant and has $c(u) = 1$. Yet, since f is irreducible, it also follows that $c(f) = 1$. Additionally, f is irreducible in $F[x]$ by the contrapositive of Gauss's Lemma.

If f is irreducible in $F[x]$, and has content 1, then for any factorization

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

where $g(x), h(x) \in F[x]$, either g or h must be a constant. Now, since f is contained in $R[x]$, we may take a common denominator to yield

$$f(x) = au(x),$$

where $u(x)$ is nonconstant and has content 1, with $a \in R$. Since f has content 1, it follows that a is a unit element, meaning that any factorization of f must contain a unit, so that f is irreducible in $R[x]$.

□

Theorem: If R is a UFD, then $R[x]$ is a UFD.

Proof. Let $F = \text{frac}(R)$, and let $f(x) \in R[x]$ be a nonzero, non-unit element. If $f(x) \in R$, then f is a product of irreducibles in R by part (i) of the classification, meaning the product is automatically unique up to permutation and associates as R is a UFD.

Now, if f is nonconstant, then $f(x) \in F[x]$ is nonzero and non-unit, as the units in $F[x]$ are the elements of F. Since $F[x]$ is a principal ideal domain (as $F[x]$ is a Euclidean domain, following from the division algorithm), $F[x]$ is a UFD, so we may write

$$f(x) = \prod_{i=1}^{n} g_i(x),$$

where the $g_i(x)$ are irreducible in $F[x]$. Writing

$$g_i(x) = \frac{a_i}{b_i}u_i(x),$$

where the $u_i(x) \in R[x]$ with $c(u_i) = 1$ for each i, we have

$$\prod_{i=1}^{n} \frac{a_i}{b_i} \in R,$$

as $f(x) \in R[x]$, so we may write

$$f(x) = \prod_{i=1}^{n} \frac{a_i}{b_i} \prod_{i=1}^{n} u_i(x).$$

Each of the $u_i(x)$ are irreducible in $R[x]$ by the classification, and the product $\prod_{i=1}^{n} \frac{a_i}{b_i} \in R$ is either a unit or a product of irreducibles. This gives the existence of such a factorization for f.

To see uniqueness, if

$$\begin{aligned} f(x) &= \left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{m} p_i(x)\right) \\ &= \left(\prod_{j=1}^{\ell} b_j\right)\left(\prod_{j=1}^{m} q_j(x)\right) \end{aligned}$$

are factorizations where a_i, b_j are irreducible in R, and p_i, q_j are nonconstant and irreducible with content 1, then we may take the content of both sides, yielding

$$\begin{aligned} c\left(\left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{k} p_i(x)\right)\right) &= \prod_{i=1}^{k} a_i \\ c\left(\left(\prod_{j=1}^{\ell} b_j\right)\left(\prod_{j=1}^{\ell} q_j(x)\right)\right) &= \prod_{j=1}^{\ell} b_j. \end{aligned}$$

Since contents are only well-defined up to associates, the most we can say is that

$$\prod_{i=1}^{k} a_i = u \prod_{j=1}^{\ell} b_j,$$

where $u \in R^\times$. Since there is at least one q_j, we may replace q_1 by uq_1, then divide, so that we find

$$\prod_{i=1}^{k} a_i = \prod_{j=1}^{\ell} b_j.$$

Since both of these are products of irreducibles in R, it follows that $k = \ell$ and, after permutation of factors, $b_i = u_i a_i$ for some $u_i \in R^\times$. Additionally, we also have the equality

$$\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j.$$

Since all of these factors are irreducible in $F[x]$, and $F[x]$ is a PID, we find that $n = m$ and, upon permutation of factors, we have $q_i(x) = \gamma_i p_i(x)$ for some $\gamma_i \in F \setminus \{0\}$. Write

$$\gamma_i = \frac{c_i}{d_i},$$

where $c_i, d_i \in R \setminus \{0\}$, so that

$$d_i q_i(x) = c_i p_i(x).$$

Taking the content of both sides, we then get that $v_i d_i = c_i$ for some $v_i \in R^\times$, so that $\gamma_i = v_i \in R^\times$, meaning that p_i and q_i are associates in $R[x]$. □

Unique factorization in polynomial rings having the rigidity laid out in the classification theorem makes for very useful criteria to understand irreducibility.

Theorem (Eisenstein's Criterion)**:** Let R be a UFD, and let $p \in R$ be a prime element. If we write $f(x) \in R[x]$ as

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

then if

- $a_0 \neq 0$;
- $p \nmid a_n$;
- $p | a_i$ for $0 \leqslant i \leqslant n-1$;
- and $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $F[x]$. If, in addition, $c(f) = 1$, then f is irreducible in $R[x]$.

Remark: This is the more general formulation of the case when $R = \mathbb{Z}$ and f is monic that we see in undergrad abstract algebra.

Proof. Suppose toward contradiction that f is reducible in $F[x]$, where we may write

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in R[x]$ nonconstant as in the proof of Gauss's Lemma. The reduction map $\pi\colon R[x] \to (R/(p))[x]$ is a homomorphism, so that

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x).$$

Thus, by our assumptions, we have

$$\overline{f}(x) = \overline{a_n} x^n,$$

with $\overline{a_n} \neq \overline{0}$. Since the degree of $\overline{f}$ remains the same upon reduction, it follows that $\overline{g}$ and $\overline{h}$ have the same degrees as they had originally.

Observe that in a domain, the product of the highest-degree terms is the highest-degree term of the product, and similarly for the lowest-degree terms. Therefore, we must have $\overline{g}(x)$ and $\overline{h}(x)$ are monomials, as their product is a monomial. Writing

$$\overline{g}(x) = \beta x^k$$
$$\overline{h}(x) = \gamma x^\ell,$$

with $\gamma, \beta \in R$ and $k = \deg(g)$, $\ell = \deg(h)$, we then get

$$g(x) = bx^k + pu(x)$$
$$h(x) = cx^\ell + pv(x),$$

where $k, \ell > 0$ and $u(x), v(x) \in R[x]$. Then,

$$f(x) = \big(bx^k + pu(x)\big)\big(cx^\ell + pv(x)\big),$$

whence the constant term of this product is divisible by p^2. □

Modules

For this section, a ring R may not be commutative nor unital.

Basic Definitions

Definition: Let R be a ring. A *left* R*-module* is a set M with operations

$$\begin{aligned} +\colon M \times M &\to M \\ (m, n) &\mapsto m + n \\ .\colon R \times M &\to M \\ (r, m) &\mapsto r \cdot m, \end{aligned}$$

satisfying the following axioms:

(M0) $(M, +)$ is an abelian group;

(M1) $(r + s) \cdot m = r \cdot m + s \cdot m$ for all $r, s \in R$ and $m \in M$;

(M2) $(rs) \cdot m = r \cdot (s \cdot m)$ for all $r, s \in R$ and $m \in M$;

(M3) $r \cdot (m + n) = r \cdot m + r \cdot n$ for all $r \in R$ and $m, n \in M$;

(M4) if R is unital, then $1 \cdot m = m$ for all $m \in M$.

A *submodule* $N \leqslant M$ of an R-module M is an abelian subgroup such that $r \cdot n \in N$ for all $r \in R$ and $n \in N$.

Definition: If $N \leqslant M$ is a submodule, then the *quotient module* M/N is formed by taking equivalence classes of the form $m + N$, where $m + N = k + N$ if $m - k \in N$.

Definition: An R-module homomorphism between M and N is a map $\varphi\colon M \to N$ such that φ is R-linear, in the sense that

$$\varphi(r \cdot m + s \cdot k) = r \cdot \varphi(m) + s \cdot \varphi(k).$$

The set of all homomorphisms between R-modules M and N is denoted $\hom_R(M, N)$, and forms an R-module itself under pointwise operations.

The set of all R-module *endomorphisms* is denoted

$$\operatorname{end}_R(M) \coloneqq \hom_R(M, M),$$

and forms a ring under pointwise operations and composition.

The space of R-module *automorphisms* is denoted

$$\operatorname{aut}_R(M) \coloneqq (\operatorname{end}_R(M))^\times.$$

Modules admit the most "natural" form of the isomorphism theorems, as we only need to concern ourselves with submodules, rather than encountering issues like normal subgroups or ideals.

Theorem (Isomorphism Theorems for Modules)**:**

First Isomorphism Theorem: If $\varphi\colon M \to N$ is a homomorphism of R-modules, there is an induced isomorphism

$$\overline{\varphi}\colon M/\ker(\varphi) \to \operatorname{im}(\varphi),$$

given by $\overline{\varphi}(m + \ker(\varphi)) = \varphi(m)$.

Second Isomorphism Theorem: If A and B are submodules of M, then there is an isomorphism

$$\frac{A+B}{A} \cong \frac{A}{A \cap B},$$

where

$$A + B = \{m + n \mid m \in A, n \in B\}.$$

Third Isomorphism Theorem: If $A, B \leqslant M$ are submodules with $A \subseteq B$, then there is an isomorphism

$$M/B \cong \frac{M/A}{B/A}.$$

Fourth Isomorphism Theorem: If $B \leqslant M$ is a submodule, then there is a one to one correspondence between the set of submodules of M/B and the set of submodules of M containing B.

Some Special R-Modules

There are three special cases of R-modules that we will discuss here. The first one is pretty straightforward, while the other two are a bit more complex and will enable us to understand some particularly deep results later down the line.

Example: If F is a field, then the F-modules are precisely the vector spaces over F. This is because F-vector spaces and F-modules have the exact same axioms.

Example: We claim that there is a one to one correspondence between $\mathbb{Z}$-modules and abelian groups.

One direction follows from applying a "forgetful functor" on M, taking $M \mapsto (M, +)$, simply discarding the $\mathbb{Z}$-module structure of M. In fact, this can apply to all R-modules.

In the reverse direction, if $(M, +)$ is an abelian group, then we can specify a compatible action by $\mathbb{Z}$ onto M by taking

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ times}} & n > 0 \\ 0 & n = 0. \\ \underbrace{-a - \cdots - a}_{-n \text{ times}} & n < 0 \end{cases}$$

The last example is the most intriguing. In fact, as we will see towards the end, it ties directly to the Jordan Canonical Form, as we will see once we discuss the structure of finitely generated ideals over a principal ideal domain.

Example: We want to understand the $F[x]$ modules, where F is a field.

Now, first, observe that since constants are elements of $F[x]$, it immediately follows that if V is a $F[x]$ module, then V admits a compatible structure with respect to F, meaning that V is in fact a vector space.

Now, observe that the action of $p(x) \in F[x]$ on $v \in V$ is fully determined by x, as

$$x^n \cdot v = x \cdot (x \cdot (\cdots x \cdot v)).$$

If we consider a single linear transformation $T \colon V \to V$, then by defining $T^n = T \circ \cdots \circ T$, we observe that for any $v \in V$, the map

$$p(T)(v) = \left(a_n T^n + a_{n-1} T^{n-1} + \cdots a_n T + a_0\right) v$$

is an action on $v \in V$; we may then consider the pair (V, T) to be the corresponding $F[x]$-module. The

reverse direction follows from defining $T\colon V \to V$ by $Tv = x \cdot v$.

Observe then that the $F[x]$-submodules of a $F[x]$-module V are precisely the T-invariant subspaces of V.

Free Modules and Direct Sums

Definition: Let R be a ring, M an R-module, $X \subseteq M$. Then, we call

$$R \cdot X = \{r \cdot x \mid r \in R, x \in X\}$$

the submodule *generated by* X. We also write $\langle X \rangle$.

Definition:

- We say $X \subseteq M$ is R-*linearly independent* if

$$a_1 \cdot x_1 + \cdots + a_n \cdot x_n = 0$$

for any $x_1, \ldots, x_n \in X$ and $a_1, \ldots, a_n \in R$ implies that $a_1, \ldots, a_n = 0$.

- A subset X of M is called an R-*basis* if X is R-linearly independent and $\langle X \rangle = M$.
- We say M is a *free* R-module if M admits a basis.

Theorem: Every $\mathbb{F}$-vector space V has a basis. Furthermore, the following hold:

- if X is a generating set for V, then X contains a basis;
- if X is a linearly independent subset of V, then X can be extended to a basis.

Example: This does not always hold if we are not dealing with vector spaces. For instance, $\mathbb{Z}$ is a free $\mathbb{Z}$-module, but $\{2\}$ is a $\mathbb{Z}$-linearly independent subset that cannot be extended to a basis for $\mathbb{Z}$. This follows from the fact that $\{2, n\}$ for any $n \neq 2$ is $\mathbb{Z}$-dependent.

Similarly, $\{2, 3\}$ is a generating set for $\mathbb{Z}$ as $\gcd(2, 3) = 1$, yet X does not contain any $\mathbb{Z}$-bases.

Definition (External Direct Sum)**:**

(a) Let $M_1, \ldots, M_r$ be R-modules. The *external direct sum* $M_1 \oplus \cdots \oplus M_n$ is a module with coordinate-wise operations consisting of elements $(m_1, \ldots, m_r)$ with $m_i \in M_i$.

(b) If $\{M_i\}_{i \in I}$ is an indexed family of R-modules, then the external direct sum of $\{M_i\}_{i \in I}$ is defined as

$$\bigoplus_{i \in I} M_i := \left\{ f\colon I \to \coprod_{i \in I} M_i \;\middle|\; f(i) \in M_i, f \text{ is finitely supported} \right\}.$$

Theorem: Let M be a free R-module, Σ a cardinal number. The following are equivalent

(i) M has a basis with cardinality Σ;

(ii) $M \cong \bigoplus_{i \in \Sigma} R$ as R-modules.

Proof. Let M have an R-basis indexed by Σ, written $\{m_i\}_{i \in \Sigma}$. Then, for every $y \in M$, we may write

$$y = \sum_{i \in \Sigma} r_i \cdot m_i,$$

where $r_i = 0$ for all but finitely many such $i \in \Sigma$.

Now, consider the map

$$\varphi : M \to \bigoplus_{i \in \Sigma} R$$
$$\sum_{i \in \Sigma} r_i \cdot m_i \mapsto \left\{ f_y : \Sigma \to R \;\middle|\; f_y(i) = r_i \right\}.$$

Since the expression is unique, it follows that φ is well-defined, and is an R-module homomorphism that is injective by the definition of a basis. Furthermore, we can define an inverse for φ by defining

$$\psi : \bigoplus_{i \in \Sigma} R \to M$$
$$f \mapsto \sum_{i \in \Sigma} f(i) \cdot m_i.$$

Therefore, $M \cong \bigoplus_{i \in \Sigma} R$.

Now, if $M \cong \bigoplus_{i \in \Sigma} R$, then letting

$$X = \{ e_i \mid e_i : \Sigma \to R, e_i(i) = 1, e_i(j) = 0 \text{ for all } j \neq i \},$$

we claim that X is an R-basis of $\bigoplus_{i \in \Sigma} R$. Toward this end, we only need to verify that X spans R. If $f \in \bigoplus_{i \in \Sigma} R$, then f is a finitely supported function from Σ to R, so we may write

$$f = \sum_{k=1}^{n} f(i_k) \cdot e_{i_k}.$$

□

Corollary: If M and N are free modules with bases of the same cardinality, then $M \cong N$.

We now turn our focus towards other ways to build up a large family of modules.

Definition: If $\{M_i\}_{i \in I}$ is a collection of R-modules, then the *direct product*,

$$M = \prod_{i \in I} M_i$$

is the Cartesian product of the M_i with coordinatewise operations.

Theorem (Universal Property of Products)**:** Let $\{M_i\}_{i \in I}$ be a family of R-modules, and let

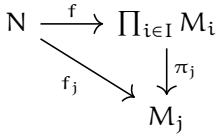
$$M = \prod_{i \in I} M_i$$

be the direct product.

(i) We have that M admits a family of projection homomorphisms

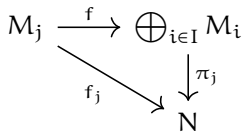
$$\pi_j : M \to M_j$$
$$(m_i)_{i \in I} \mapsto m_j.$$

(ii) Given an R-module N with R-module homomorphisms $f_j : N \to M_j$, there exists a unique R-module homomorphism $f : N \to M$ such that $\pi_j \circ f = f_j$.



Theorem (Universal Property of Direct Sum)**:** Let $\{M_i\}_{i\in I}$ be a family of R-modules, and let $L = \bigoplus_{i\in I} M_i$ be the direct sum.

Then, for an R-module N and a family of R-module homomorphisms $g_j : M_j \to N$, there exists a unique R-module homomorphism $g : L \to N$ such that $g \circ \iota_j = g_j$, where ι_j is the inclusion of M_j into L, given by $m_j \mapsto (0, 0, \dots, m_j, 0, 0, \dots)$.



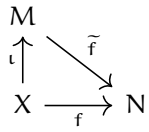
Proposition: Let $\{M_i\}_{i\in I}$ be a family of R-submodules of a fixed R-module M. The following are equivalent:

(i) the sum $\sum_{i\in I} M_i$ is a direct sum;

(ii) for all $j \in I$ and all $i_1, \dots, i_n \in I \setminus \{j\}$,

$$M_j \cap \left(\sum_{k=1}^{n} M_{i_k} \right) = \{0\}.$$

Theorem (Universal Property of Free Modules)**:** Let M be a free R-module with basis X. Then, for any R-module N and set map $f : X \to N$, there exists a unique R-module homomorphism $\widetilde{f} : M \to N$ such that $\widetilde{f}|_X = f$.



Corollary: Every R-module is a quotient of a free module.

Proof. Let M be an R-module, and let $F = R[M]$ be the free module generated by the elements of M. Then, it follows that $\mathrm{id} : M \to M$ is a bijective set map, which then extends to a surjective module homomorphism $q : F \to M$. By the first isomorphism theorem, it follows that $M \cong F/\ker(q)$. □

Definition: We call the module $\ker(q)$ the *module of relations* for M. Generally speaking, we seek to understand the minimal such module.

Noetherian Properties

For this subsection, we fix a unital, commutative ring R. Recall that R is Noetherian if and only if every ascending chain of ideals stabilizes, if and only if every ideal is finitely generated.

We can give a similar description for Noetherian *modules*. We will use this in the proof of a much-celebrated theorem related to polynomial rings.

Proposition: Let M be an R-module. The following are equivalent:

(i) Every submodule of M is finitely generated;

(ii) every ascending chain of submodules stabilizes;

(iii) every nonempty set of submodules has a maximal element.

Proposition: Let M be a Noetherian R-module, with $N \leqslant M$. Then, both N and M/N are Noetherian.

Proof. Let $N' \leqslant N$; then, $N' \leqslant M$, whence N' is finitely generated, so N is Noetherian.

Meanwhile, recall that all R-submodules of M/N correspond to modules of the form N'/N, where $N \leqslant N' \leqslant M$, by the Fourth Isomorphism Theorem. Therefore, N' is finitely generated, so N'/N is finitely generated. □

Proposition: Suppose $N \leqslant M$ and M/N are Noetherian. Then, so too is M.

Proof. Let $K \leqslant M$ be an R-submodule. We will show that K is finitely generated.

Consider $K \cap N \leqslant N$. Since N is Noetherian, $K \cap N$ is finitely generated, so it admits generators $x_1, \ldots, x_n$. Similarly, since $\frac{K+N}{N} \leqslant M/N$ is a submodule of the Noetherian module M/N, so there are generators $y_1 + N, \ldots, y_m + N$ of $\frac{K+N}{N}$.

In particular, since each of the y_i can be written as $k_i + n_i$, with $y_i + N = k_i + N$, we may say without loss of generality that each of the y_i are elements of K.

We claim now that $\langle x_1, \ldots, x_n, y_1, \ldots, y_m \rangle = K$. We call this generating set X. In particular, we observe already that $\langle X \rangle \leqslant K$, so we only need to show the other inclusion.

Let $z \in K$. Then, $z \in K + N$, meaning $z + N \in \frac{K+N}{N}$. Therefore, we have $r_1, \ldots, r_m$ such that $z + N = r_1 \cdot y_1 + N + \cdots + r_m \cdot y_m + N$. In particular, this means that $\left(z - \sum_{i=1}^{m} r_i \cdot y_i\right) \in N \cap K$. Since $\langle x_1, \ldots, x_n \rangle = K \cap N$, we have $s_1, \ldots, s_n \in R$ such that

$$z - (r_1 \cdot y_1 + \cdots + r_m \cdot y_m) = s_1 \cdot x_1 + \cdots + s_n \cdot x_n.$$

Thus, $\langle X \rangle = K$. □

Theorem: If R is a Noetherian ring, then any finitely generated R-module is Noetherian.

Proof. We start by proving that every finitely generated free R-module is Noetherian. Then, if M is an arbitrary finitely generated module, then M is a quotient of a finitely generated free module, and the Noetherian property is inherited under quotients.

We prove by induction on the rank. If F is free of rank n, then $F \cong R^n$. If $n = 1$, then $F \cong R$ as R-modules. Since the submodules of R are exactly the ideals, F is Noetherian as an R-module as every ideal of R is finitely generated.

Inductively, if $F \cong R^n$, then the submodule $R \cong R \times \{0\}^{n-1}$ is Noetherian, and

$$R^{n-1} \cong \frac{R^n}{R \times \{0\}^{n-1}}$$

is Noetherian by the inductive hypothesis. Thus, R^n is Noetherian by the previous proposition. □

Theorem (Hilbert Basis Theorem)**:** If R is a Noetherian ring, then $R[x]$ is Noetherian.

Proof. Let $I \subseteq R[x]$ be a nonzero ideal. Define the set

$$J = \left\{ a \in R \;\middle|\; \text{there exists } f(x) \in I \text{ with leading coefficient } a \right\}.$$

We claim that J is an ideal of R. Towards this end, let $a \in J$ and $r \in R$, with $a \neq 0$. Then, there exists $f(x) \in I$ with $f(x) = ax^n + \text{LOT}$. We observe that $rf(x) \in I$, whence $rax^n + \text{LOT} \in I$, so that $ra \in J$.

Now, let $a, b \in J$, and let $f(x) = ax^n + \text{LOT}$ and $g(x) = bx^m + \text{LOT}$, with $f(x), g(x) \in I$. Without

loss of generality, $n \geqslant m$, so we may multiply $x^{n-m}g(x) \in I$ to take $x^{n-m}g(x) = bx^n + \text{LOT}$, so that $f(x) - x^{n-m}g(x) \in I$ and thus $a - b \in J$.

Now, since R is Noetherian, and $J \subseteq R$ is an ideal, we have $J = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in R$. We may find corresponding elements of I, which we write $f_i(x) = a_i x^{d_i} + \text{LOT}$. Set $d = \max\{d_i \mid 1 \leqslant i \leqslant r\}$. Consider the R-module

$$\begin{aligned} M &= \left(R + Rx + \cdots + Rx^{d-1}\right) \cap I \\ &= \left\{\text{polynomials in } I \text{ with degree less than } d-1\right\} \cup \{0\}. \end{aligned}$$

Note that M is finitely generated as an R-module, as $M \leqslant R + Rx + \cdots + Rx^{d-1}$ and the latter is Noetherian as an R-module as it is a finitely generated module over a Noetherian ring.

We may write $M = (g_1(x), \ldots, g_s(x))$ as a result. We claim that

$$I = (f_1(x), \ldots, f_r(x), g_1(x), \ldots, g_s(x)).$$

Write $I_0 = (f_1(x), \ldots, f_r(x))$. We claim that if $f(x) \in I$ is such that $\deg(f) > d - 1$, then there exists $h(x) \in I_0$ such that $\deg(f - h) < \deg(f)$. This will allow us to take $p(x) \in I$ and decompose it into constituent parts by repeatedly applying the claim to yield an element $h \in I_0$ with $\deg(p - h) \leqslant d - 1$, or $p(x) - h(x) = 0$, which yields an element of I_0 and an element of M.

Now, let $f(x) \in I$ have degree $n \geqslant d$. In particular, $n \geqslant d_i$ for all $i = 1, \ldots, r$. Writing

$$f(x) = cx^n + \text{LOT},$$

we then have a leading coefficient $c = \ell_1 a_1 + \cdots + \ell_r a_r$ with $\ell_1, \ldots, \ell_r \in R$. We take

$$h(x) = \ell_1 x^{n-d_1} f_1(x) + \cdots + \ell_r x^{n-d_r} f_r(x),$$

and observe that h has leading term equal to cx^n. Thus, $\deg(f - h) < \deg(f)$. The rest follows from induction. □

The Hilbert Basis Theorem and the theorem on finitely generated modules over Noetherian rings together allow us to create a large family of Noetherian modules. For instance, if R is Noetherian, then

$$\left(\frac{R[x_1, \ldots, x_n]}{I}\right)[y_1, \ldots, y_m]$$

is Noetherian.

A Taste of Homological Algebra

Definition: A sequence of R-modules homomorphisms

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called *exact* if $\ker(g) = \text{im}(f)$. More generally, a sequence of R-module homomorphisms

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} A_n$$

is called exact if $\ker(f_{i+1}) = \text{im}(f_i)$ for each i.

Definition: The special case of an exact sequence is one of the following form.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Here, f is injective, g is surjective, and $\ker(g) = \text{im}(f)$. We call such sequences *short exact* sequences.

Example:

(a) The sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

is a short exact sequence.

(b) If M is an R-module, then M slots into a short exact sequence of R-modules given by the following.

$$0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0$$

Here, F is free and N is the module of relations.

If $f\colon M \to N$ is an R-module homomorphism, and P is a fixed R-module, then there is a canonical induced homomorphism

$$\begin{aligned} f_*\colon \hom(P,M) &\to \hom(P,N) \\ \left[P \xrightarrow{\varphi} M\right] &\mapsto \left[P \xrightarrow{\varphi} M \xrightarrow{f} N\right] \end{aligned}$$

given by $f_*(\varphi) = f \circ \varphi$.

Proposition: Suppose we start with a short exact sequence of R-modules.

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

Then, the sequence

$$0 \longrightarrow \hom(P,L) \xrightarrow{f_*} \hom(P,M) \xrightarrow{g_*} \hom(P,N)$$

is exact for all R-modules P.

Remark: The converse also holds.

Proof. Suppose the sequence of R-modules is exact. Then, f is injective, g is surjective, and $\operatorname{im}(f) = \ker(g)$. We start by showing that f_* is injective.

Toward this end, let $\varphi \in \ker(f_*)$. Then, for all $x \in P$, we have $f(\varphi(x)) = 0$, whence $\varphi(x) = 0$, so φ is zero.

Next, we observe that $\operatorname{im}(f_*) \subseteq \ker(g_*)$, as $g_* \circ f_* = (g \circ f)_* = 0$ as the original sequence is exact. Now, if $\varphi \in \ker(g_*)$, then $\varphi\colon P \to M$ is an R-module homomorphism such that $g \circ \varphi = 0$. If $p \in P$, then $g(\varphi(p)) = 0$, meaning that $\varphi(p) \in \ker(g)$. Since f is injective and $\ker(g) = \operatorname{im}(f)$, we have that there is unique $a \in L$ such that $\varphi(p) = f(a)$. Define $\psi\colon P \to L$ by $p \mapsto a$. Observe that since f is a homomorphism, so too is ψ. □

Note that g_* may not be surjective. The cases for P where g_* *is* surjective are special to have their own definition.

Definition: An R-module P is called *projective* if, for all short exact sequences of R-modules

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \xrightarrow{0} 0$$

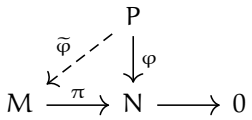
the sequence

$$0 \longrightarrow \hom(P,L) \xrightarrow{f_*} \hom(P,M) \xrightarrow{g_*} \hom(P,N) \xrightarrow{0} 0$$

is also exact.

Equivalently, this means that for all surjections $M \xrightarrow{\pi} N \to 0$, and all homomorphisms $\varphi\colon P \to N$, there is

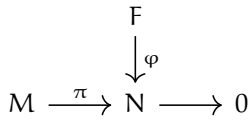
some $\widetilde{\varphi}\colon P \to M$ such that $\pi \circ \widetilde{\varphi} = \varphi$.



Our goal now is to determine exactly when an R-module is projective. As it turns out, there is a very tidy characterization.

Lemma: Every free module is projective.

Proof. Let F be a free R-module with basis X, and let $M \xrightarrow{\pi} N \to 0$ be a surjection of R-modules. Suppose we have a homomorphism φ satisfying the following diagram.



Restricting φ to X, we see that since π is surjective, we may find $m_x \in M$ such that $\pi(m_x) = \varphi(x)$ for each x. Defining a set map $\widetilde{\varphi}\colon X \to M$ mapping $x \mapsto m_x$, we observe that there is then an R-module homomorphism $\overline{\varphi}\colon F \to M$ uniquely extending $\widetilde{\varphi}$, by the universal property of free modules. □

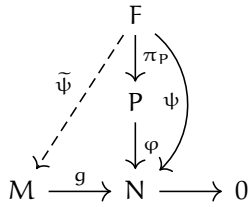
Theorem (Characterization of Projective Modules)**:** An R-module P is projective if and only if P is a direct summand of a free module. That is, if and only if there exists a free R-module F and an R-module Q such that

$$F \cong P \oplus Q$$

as an external direct sum.

We can show one direction right now.

Proof of the Reverse Direction. Suppose $F = P \oplus Q$ as an internal direct sum for some R-module Q and a free R-module P. Then, F is equipped with a projection map $\pi_P\colon F \to P$ taking $p \oplus q$ to p, and an inclusion map $\iota_P\colon P \hookrightarrow F$ mapping $p \mapsto p \oplus 0$. We then take the following diagram of homomorphisms, where $\varphi\colon P \to N$ is the homomorphism we want to extend to g.



Now, we observe that by definition, we have $g \circ \widetilde{\psi} = \varphi \circ \pi_P$, so we may define $\widetilde{\varphi}\colon P \to M$ by taking

$$\widetilde{\varphi} = \widetilde{\psi} \circ \iota_P.$$

This maps $p \mapsto p \oplus 0 \mapsto \widetilde{\psi}(p \oplus 0) = \varphi(p)$. □

For the reverse direction, we need to be able to characterize when exactly a module is a direct sum of submodules.

Definition: Let $f\colon M \to N$ be an R-module homomorphism. Then, we say $s\colon N \to M$ is a *splitting* (or *section*) if $f \circ s = \mathrm{id}_N$. In other words, a splitting is a right-inverse.

We observe automatically that if f has a splitting, then f is surjective and s is injective, by the equivalent characterization of surjective maps as those being with (necessarily injective) right-inverses.

Lemma: If $f\colon M \to N$ admits a splitting $s\colon N \to M$, then $M \cong s(N) \oplus \ker(f) \cong N \oplus \ker(f)$.

Proof. First, we show that $s(N) + \ker(f) = M$. Letting $m \in M$, then we set $m' = m - s(f(m))$. Then,

$$\begin{aligned} f(m') &= f(m) - f(s(f(m))) \\ &= f(m) - (f \circ s)(f(m)) \\ &= f(m) - f(m) \\ &= 0, \end{aligned}$$

so $m' \in \ker(f)$, and $M \subseteq s(N) + \ker(f)$.

Next, we show that $s(N) \cap \ker(f) = 0$. If $m \in s(N) \cap \ker(f)$, then $m = s(n)$ for some $n \in N$, and $f(m) = f(s(n)) = n = 0$, whence $m = 0$. □

Definition: We say the sequence

$$0 \longrightarrow L \xrightarrow{f} M \underset{s}{\overset{g}{\rightleftarrows}} N \longrightarrow 0$$

splits if g has a splitting, so by the lemma and exactness, we have $M \cong L \oplus N$.

Lemma: Let $M \xrightarrow{g} P \to 0$ be a surjection of R-modules with P projective. Then, g admits a splitting.

Proof. Using the projectivity of P in the following diagram, we obtain our desired section s such that $g \circ s = \mathrm{id}$.

$$\begin{array}{ccccc} M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & \overset{s}{\nwarrow} & \uparrow{\scriptstyle \mathrm{id}} & & \\ & & P & & \end{array}$$

□

Now, we can finally prove the forward direction of the characterization.

Proof of the Forward Direction. Let P be projective. From the universal property of R-modules, we know that there is a surjective R-module homomorphism $F \xrightarrow{\pi} P \to 0$. Thus, π splits, and we are done. □

Groups

We begin our discussion of group theory with group actions.

Definition: Let X be a set, and let G be a group. A (left) G-*action* on X is a map

$$\begin{aligned} \mu \colon G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

that satisfies

- $e \cdot x = x$ for all $x \in X$
- $g \cdot (h \cdot x) = (gh) \cdot x$.

We call X a G-set.

Definition: A group action induces a homomorphism

$$\begin{aligned} \rho \colon G &\to \mathrm{Sym}(X) \\ g &\mapsto \pi_g, \end{aligned}$$

where $\pi_g(x) = g \cdot x$. This is known as the *permutation representation* of the action.

Definition: We say the action of G on X is *faithful* if the induced map ρ is injective.

Remark: Any action ρ admits a faithful action by "modding out" by the kernel,

$$\ker(\rho) := \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}.$$

Then, the action of $G/\ker(\rho)$ on X is given by $(g\ker(\rho)) \cdot x = g \cdot x$.

Definition: For an element $x \in X$, we define the *stabilizer* of x to be

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Definition: For $x \in X$, the *orbit* of x is given by

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

Definition: An action is called *transitive* if there is one orbit for the action.

The orbits in fact partition X under the equivalence relation $x \sim y$ whenever there is $g \in G$ such that $g \cdot x = y$. The set of all distinct orbits is then denoted

$$\begin{aligned} X/G &= \{G \cdot x_i \mid i \in I\} \\ &= \bigsqcup_{i \in I} G \cdot x_i. \end{aligned}$$

Lemma (Orbits and Stabilizers)**:** Let $x \in X$ be fixed. There exists a bijection between the set of all left cosets G/G_x and the orbit $G \cdot x$. In particular, if X and G are finite, then $|G \cdot x| = [G : G_x]$.

Proof. Consider the map $f_x : G \to G \cdot x$ given by $g \mapsto g \cdot x$. By definition of the orbit, f_x is necessarily surjective. For $g \in G$ and $h \in G_x$, we observe that

$$\begin{aligned} f_x(gh) &= gh \cdot x \\ &= g \cdot (h \cdot x) \\ &= g \cdot x \\ &= f_x(g). \end{aligned}$$

Therefore, by the first isomorphism theorem, f_x induces a well-defined map $\overline{f_x} : G/G_x \to G \cdot x$ that is surjective. We claim that $\overline{f_x}$ is in fact injective.

Suppose $f_x(g_1) = f_x(g_2)$. Then, $g_1 \cdot x = g_2 \cdot x$, or that $g_2^{-1}g_1 \cdot x = x$, meaning that $g_2^{-1}g_1 \in G_x$, or that the cosets $g_1G_x = g_2G_x$. □

Corollary: Let G be a finite group acting on a finite set X, and let $\{x_1, \ldots, x_r\}$ be distinct representatives for X/G.

(i)

$$\begin{aligned} |X| &= \sum_{i=1}^{r} |G \cdot x_i| \\ &= \sum_{i=1}^{r} [G : G_{x_i}] \\ &= \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}. \end{aligned}$$

(ii)

$$|G| = |G \cdot x||G_x|$$

for all $x \in X$.

Canonical Examples of Group Actions

Example (Symmetric Polynomials)**:** Let $R = F[x_1, \dots, x_n]$. We let S_n act on R by permuting the indices, given by

$$\sigma \cdot x_i = x_{\sigma(i)}$$
$$\sigma \cdot k = k$$

for all x_i and all $k \in F$. We claim that this is a faithful action.

If $\sigma \in S_n$ is such that $\sigma \in \ker(\rho)$, then $\sigma \cdot f(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ for all $f \in F[x_1, \dots, x_n]$. In particular, this means that $\sigma \cdot x_i = x_i$ for all i, and $\sigma \cdot k = k$, whence $\sigma(i) = i$ for all i, so $\sigma = e$.

Therefore, we get the injective group homomorphism $\rho \colon S_n \to \text{Sym}(R)$. In this case, every $\rho(\sigma) \colon R \to R$ is in fact a ring automorphism. We say that S_n acts on R by ring automorphisms.

Definition: The fixed points of the action $\rho \colon S_n \to \text{Sym}(R)$ are known as the *symmetric polynomials*.

Definition (Elementary Symmetric Polynomials)**:** The elementary symmetric polynomials are defined as follows.

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ s_2 &= \sum_{i<j} x_i x_j \\ s_3 &= \sum_{i<j<k} x_i x_j x_k \\ &\vdots \\ s_n &= x_1 \cdots x_n. \end{aligned}$$

The fundamental theorem of symmetric polynomials holds that every symmetric polynomial $f \in F[x_1, \dots, x_n]$ has a unique expression as $g(s_1, \dots, s_n)$. In other words,

$$F[x_1, \dots, x_n]^{S_n} = F[s_1, \dots, s_n].$$

A version of this can in fact be proven using Galois theory, but we will prove it using a more "pedestrian" approach.

To see existence, we start by reducing to the homogeneous case, by observing that we may separate any $f \in F[x_1, \dots, x_n]$ into polynomials with the property that

$$f(\lambda x_1, \dots, \lambda x_n) = \lambda^d f(x_1, \dots, x_n),$$

where d is the degree of the homogeneous polynomial. In particular, we may uniquely write

$$f = p_1 + \cdots + p_r,$$

where each of the p_i is homogeneous with degree d_i, and $d_1 > d_2 > \cdots > d_r$. If f is symmetric, then for any $\sigma \in S_n$, $\sigma \cdot p_i$ is also homogeneous of the same degree, with

$$\begin{aligned} f &= \sigma \cdot p_1 = \cdots + \sigma \cdot p_r \\ &= p_1 + \cdots + p_r \end{aligned}$$

by uniqueness, so that each of the homogeneous components of f is symmetric.

Example: Given a regular geometric shape (such as a square, circle, triangle, cube, etc.), we consider the group G consisting of all isometries $S \to S$.

For example, if S is a square, then the group of isometries is D_4. We claim that the group D_4 has order 8, consisting of the set of combinations of the four pure rotations and four reflections about the symmetry axes of the square. To see this, let $V = \{a, b, c, d\}$ be the set of vertices of the square, and let G act on V. We observe that this action is transitive, so that $|G \cdot a| = 4$. Meanwhile the stabilizer of A consists of the identity map and the reflection about the diagonal axis of symmetry that passes through a. In particular, this means that $|\text{stab}_G(a)| = 2$, whence $|G| = 8$.

In the general case, we can define the group D_n to be the set of rotations $r_1, \ldots, r_n$ with an angle of $\frac{2\pi k}{n}$ together with the reflections about the symmetry axes, $s_1, \ldots, s_n$, subject to the relations that

$$\begin{aligned} r_1^n &= e \\ s_1^2 &= e \\ s_1 r_1 s_1^{-1} &= r_1^{-1}. \end{aligned}$$

Example: If G is a group, then G can in fact act on itself. The most canonical way of doing so is via left-multiplication, giving $g \cdot h = gh$.

Via the permutation representation, this induces a homomorphism

$$\rho \colon G \to \text{Sym}(G),$$

and since the action is faithful, this is injective. Immediately, we obtain *Cayley's Theorem*, which states that every group is isomorphic to a subgroup of a permutation group. This is known as the left-regular permutation representation of G.

We can extend this regular permutation to cosets. If $H \leqslant G$, then G acts on the coset space G/H by $g \cdot aH = gaH$. This action is transitive, and computing the stabilizer gives $gaH = aH$ if and only if $a^{-1}ga \in H$, if and only if $g \in aHa^{-1}$. In particular, this means that $g \in G_{aH}$ if and only if gaH is a conjugate of H.

Given the permutation representation homomorphism $\rho \colon G \to \text{Sym}(G/H)$, we see that

$$\ker(\rho) = \bigcap_{a \in G} aHa^{-1},$$

which is necessarily normal.

Example: The action of G on itself by conjugation, given by $g \mapsto \iota_g$, where

$$\iota_g(y) = gyg^{-1}$$

is an action of the group on itself by automorphisms. The image $G \to \text{aut}(G)$ under this action is known as the *inner automorphism group* of G.

The orbit of an element x under conjugation is known as the *conjugacy class* of x, and will be written $K_G(x)$. The stabilizers are known as the *centralizer* of x, and are written as $Z_G(x)$. The kernel of the permutation representation for conjugation is the *center* of the group G, and is written $Z(G)$.

We observe that if G is a finite group with $g_1, \ldots, g_r$ representatives for the conjugacy classes, then

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : Z_G(g_i)].$$

It is possible to extend conjugation naturally to $P(G)$, by taking $g \cdot A = gAg^{-1}$. The stabilizers are denoted as $N_G(T)$. If H is an actual subgroup of G, then $N_G(H)$ is known as the *normalizer* of H in G. Similarly, by applying orbit-stabilizer, we find that $[G : N_G(H)]$ is the number of distinct subgroups conjugate to H.

The Sylow Theorems

Let G be a finite group with $|G| = p^m r$, where p is a prime, $m \geqslant 1$, and $p \nmid r$.

Definition: A p-Sylow subgroup of G is a subgroup of order p^m. That is, a p-Sylow subgroup of G is a maximal p-subgroup of G.

There are three Sylow theorems. They are very useful.

Theorem (Sylow Theorems)**:** Let G be a finite group with $|G| = p^m r$.

(1) A p-Sylow subgroup exists.

(2) If P and Q are p-Sylow subgroups, then there is $g \in G$ such that $Q = gPg^{-1}$.

(3) Let n_p denote the number of p-Sylow subgroups. Then, we have

$$n_p \equiv 1 \bmod p$$
$$n_p \mid r.$$

Semidirect Products

Definition: Let $\{G_i\}_{i \in I}$ be a family of groups.

The direct product $\prod_{i \in I} G_i$ is a group with coordinatewise operations and underlying set $\{(g_i)_{i \in I} \mid g_i \in G_i\}$.

It turns out that there is no analogue to the external direct sum for groups. This follows from the fact that if we have homomorphisms $f_1 \colon G_1 \to H$ and $f_2 \colon G_2 \to H$, then we would need to glue the homomorphisms by

$$f(g_1, g_2) = f_1(g_1) f_2(g_2).$$

In particular, we get

$$\begin{aligned} f((g_1, g_2)(h_1, h_2)) &= f(g_1 h_1, g_2 h_2) \\ &= f_1(g_1) f_1(h_1) f_2(g_2) f_2(h_2) \\ &= f_1(g_1) f_2(g_2) f_1(h_1) f_2(h_2) \end{aligned}$$

if and only if $f_1(h_1)$ and $f_2(g_2)$ commute for all $h_1 \in G_1$ and $g_2 \in G_2$.

We start by trying to find a scenario where we in fact can construct $G \cong H \times N$ for some subgroups H and N.

Lemma: Let G be a group, $H, N \leqslant G$.

(a) If both N and H are normal, and $N \cap H = \{e\}$, then $nh = hn$ for all $n \in N$ and $h \in H$.

(b) If N is normal, then NH is a subgroup of G.

Proof.

(a) We let $[h, n] = hnh^{-1}n^{-1}$. Since $H \cap N = \{e\}$, and the commutator is contained in both H and N, it follows that $hnh^{-1}n^{-1} = e$, whence $hn = nh$.

(b) Let N be normal, $h_1, h_2 \in H$, $n_1, n_2 \in N$. Then,

$$(n_1 h_1)(n_2 h_2) = n_1 \left(h_1 n_2 h_1^{-1}\right)(h_1 h_2)$$

$$\in NH,$$

so NH is closed under multiplication. Similarly,

$$\begin{aligned}(nh)^{-1} &= h^{-1}n^{-1}\\ &= \left(h^{-1}n^{-1}h\right)h^{-1}\\ &\in NH,\end{aligned}$$

so NH is a subgroup.

□

Theorem: Let G be a group, H, N normal, and suppose that

(i) $H \cap N = \{e\}$;

(ii) $G = NH$.

Then, $G \cong NH$.

Proof. The map $N \times H \to G$ given by $(n, h) \mapsto nh$ is a group homomorphism since H and N commute elementwise. By (ii), the map is surjective, and by (i), the map is injective. □

An interesting nonexample is the case of S_3. We observe that the groups $N = \langle(1,2,3)\rangle$ and $H = \langle(1,2)\rangle$ have $N \cap H = \{e\}$, $S_3 = NH$, but $N \cong \mathbb{Z}/3\mathbb{Z}$ and $H \cong \mathbb{Z}/2\mathbb{Z}$, meaning that $S_3 \ncong N \times H$. Instead, we have a different construction.

Definition: Let N and H be groups. Suppose we have a group homomorphism

$$f\colon H \to \text{aut}(N).$$

The *semidirect product* with respect to f is given by

$$G = N \rtimes_f H,$$

with underlying set $N \times H$ and operations given by

$$\begin{aligned}(n_1, h_1) \cdot (n_2, h_2) &= (n_1 f(h_1)(n_2), h_1 h_2)\\ (n, h)^{-1} &= \left(f\left(h^{-1}\right)\left(n^{-1}\right), h^{-1}\right).\end{aligned}$$

The semidirect product in fact allows us another tool for classifying groups. This often appears in Galois theory.

To start, we can use the Sylow theorems to see that groups of order pq with p, q primes are not simple groups. In fact, there is a unique q-Sylow subgroup of G, which we call Q, which is then normal in G. Since Q is also prime, we have $Q \cong \mathbb{Z}/q\mathbb{Z}$.

We consider now the group homomorphism

$$\begin{aligned}f\colon G &\to \text{aut}(Q)\\ g &\mapsto \iota_g,\end{aligned}$$

where ι_g is the inner automorphism given by $\iota_g(x) = gxg^{-1}$. Since Q is normal, f is well-defined. Furthermore, since Q is abelian, $Q \leqslant \ker(f)$, whence f induces a homomorphism $\bar{f}\colon G/Q \to \text{aut}(Q)$.

We have that $\text{aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, which is cyclic of order $q-1$. Meanwhile $|G/Q| = p$, which is prime, so we may express $\bar{f}\colon \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times$.

First, if $p \nmid q-1$, then Lagrange's Theorem implies that $\bar{f}$ is trivial. In particular, $\left|\ker\left(\bar{f}\right)\right| = 1$, in which case

we would have $\operatorname{im}\left(\overline{f}\right) \leqslant (\mathbb{Z}/q\mathbb{Z})^\times$, which cannot happen as $p \nmid q-1$, meaning that we have $\left|\ker\left(\overline{f}\right)\right| = p$, meaning $\overline{f}$ is trivial.

If $\overline{f}$ is trivial, then f is in fact trivial, so $gxg^{-1} = x$ for all $g \in G$, meaning $Q \leqslant Z(G)$. This yields a surjection $G/Q \to G/Z(G)$, and since G/Q is cyclic, so too is $G/Z(G)$, whence $G/Z(G)$ is cyclic, hence G is abelian. In particular, this gives

$$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Meanwhile, if $p|q-1$, then there is a nontrivial homomorphism $f\colon \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times$. There are then $p-1$ distinct nontrivial automorphisms, from which we may take $Q \rtimes_f P$.

We claim that the various choices for f yield isomorphic groups.

Proposition: Let $P = \mathbb{Z}/p\mathbb{Z}$ and $Q = \mathbb{Z}/q\mathbb{Z}$ with p, q prime and $q \equiv 1$ modulo p. If

$$f, g\colon P \to \operatorname{aut}(Q)$$

are nontrivial homomorphisms, then $Q \rtimes_f P$ and $Q \rtimes_g P$ are isomorphic.

Proof. Since f and g are both nontrivial, it follows that f and g are injective (again by Lagrange's Theorem), meaning that since $\operatorname{aut}(Q)$ is cyclic, there is a unique subgroup of order p, giving $\operatorname{im}(f) \cong \operatorname{im}(g)$.

Fix a generator for P, called $P = \langle s \rangle$. Since $f(s)$ and $g(s)$ are both generators for $\operatorname{im}(f)$ and $\operatorname{im}(g)$, there is some ℓ such that $g(s) = f(s)^\ell$. In particular, this means that $g(v) = f(v)^\ell$ for all $v \in P$.

Define the homomorphism $\varphi\colon Q \rtimes_g P \to Q \rtimes_f P$ by $(x, y) \mapsto \left(x, y^\ell\right)$. As a map of sets, φ is bijective since $\gcd(\ell, p) = 1$.

Now, we show that φ is a homomorphism.

$$\begin{aligned}
\varphi((x_1, y_1)(x_2, y_2)) &= \varphi(x_1 g(y_1)(x_2), y_1 y_2) \\
&= \left(x_1 g(y_1)(x_2), y_1^\ell y_2^\ell\right) \\
&= \left(x_1 f\left(y_1^\ell\right)(x_2), y_1^\ell y_2^\ell\right) \\
&= \left(x_1, y_1^\ell\right)\left(x_2, y_2^\ell\right).
\end{aligned}$$

□

Conjugacy in S_n and A_n

To understand conjugacy in S_n and A_n, we recall some properties of the symmetric group.

(1) Elements of S_n are called permutations, and are written as

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

(2) An element of the form (i_1, i_2) is called a transposition, and an element of teh form $(i_1, \ldots, i_k)$ is called a k-cycle.

(3) Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

(4) Disjoint cycles commute with each other.

(5) The order of a k-cycle is k, and the order of

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_r,$$

with respective lengths $k_1, \ldots, k_r$ is $o(\sigma) = \operatorname{lcm}(k_1, \ldots, k_r)$.

(6) Every $\sigma \in S_n$ can be written as a product of transpositions.

Definition: A permutation is called *even* if it can be written as an expression

$$\sigma = \tau_1 \cdots \tau_{2k}$$

as an even number of transpositions. We define the *alternating group*, A_n, to be the set of even permutations.

Theorem: We have $[S_n : A_n] = 2$, and every transposition is odd.

Proof. Consider the function

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j).$$

Letting S_n act on $\mathbb{Z}[x_1, \ldots, x_n]$ by permuting the indices, we note that $\sigma \cdot f = \pm f$. The sign of the permutation σ is defined to be k such that

$$\sigma(f) = \operatorname{sgn}(\sigma) f$$

As a result, we find that transpositions are odd, and sgn is surjective, so $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$. □