Part IB — Groups, Rings and Modules

Theorems with proof

Based on lectures by O. Randal-Williams

Notes taken by Dexter Chua

Lent 2016

Groups

Basic concepts of group theory recalled from Part IA Groups. Normal subgroups, quotient groups and isomorphism theorems. Permutation groups. Groups acting on sets, permutation representations. Conjugacy classes, centralizers and normalizers. The centre of a group. Elementary properties of finite p-groups. Examples of finite linear groups and groups arising from geometry. Simplicity of A_n.

Sylow subgroups and Sylow theorems. Applications, groups of small order. [8]

Rings

Definition and examples of rings (commutative, with 1). Ideals, homomorphisms, quotient rings, isomorphism theorems. Prime and maximal ideals. Fields. The characteristic of a field. Field of fractions of an integral domain.

Factorization in rings; units, primes and irreducibles. Unique factorization in principal ideal domains, and in polynomial rings. Gauss' Lemma and Eisenstein's irreducibility criterion.

Rings $\mathbb{Z}[\alpha]$ of algebraic integers as subsets of $\mathbb{C}$ and quotients of $\mathbb{Z}[x]$. Examples of Euclidean domains and uniqueness and non-uniqueness of factorization. Factorization in the ring of Gaussian integers; representation of integers as sums of two squares.

Ideals in polynomial rings. Hilbert basis theorem. [10]

Modules

Definitions, examples of vector spaces, abelian groups and vector spaces with an endomorphism. Sub-modules, homomorphisms, quotient modules and direct sums. Equivalence of matrices, canonical form. Structure of finitely generated modules over Euclidean domains, applications to abelian groups and Jordan normal form. [6]

Contents

0 Introduction

1 Groups

1.1 Basic concepts

Lemma. The inverse of an element is unique.

Proof. Let a^{-1}, b be inverses of a. Then

$$b = b \cdot e = b \cdot a \cdot a^{-1} = e \cdot a^{-1} = a^{-1}.$$ □

Lemma. $H \subseteq G$ is a subgroup if H is non-empty and for any $h_1, h_2 \in H$, we have $h_1 h_2^{-1} \in H$.

Theorem (Lagrange's theorem)**.** Let G be a finite group, and $H \leq G$. Then

$$|G| = |H||G : H|,$$

where $|G : H|$ is the number of H-cosets in G.

Lemma. If G is a finite group and $g \in G$ has order n, then $n \mid |G|$.

Proof. Consider the following subset:

$$H = \{e, g, g^2, \cdots, g^{n-1}\}.$$

This is a subgroup of G, because it is non-empty and $g^r g^{-s} = g^{r-s}$ is on the list (we might have to add n to the power of g to make it positive, but this is fine since $g^n = e$). Moreover, there are no repeats in the list: if $g^i = g^j$, with wlog $i \geq j$, then $g^{i-j} = e$. So $i - j < n$. By definition of n, we must have $i - j = 0$, i.e. $i = j$.

Hence Lagrange's theorem tells us $n = |H| \mid |G|$. □

1.2 Normal subgroups, quotients, homomorphisms, isomorphisms

Lemma. If $\phi : G \to H$ is a homomorphism, then

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

Proof. We compute $\phi(g \cdot g^{-1})$ in two ways. On the one hand, we have

$$\phi(g \cdot g^{-1}) = \phi(e) = e.$$

On the other hand, we have

$$\phi(g \cdot g^{-1}) = \phi(g) * \phi(g^{-1}).$$

By the uniqueness of inverse, we must have

$$\phi(g^{-1}) = \phi(g)^{-1}.$$ □

Lemma. For a homomorphism $\phi : G \to H$, the kernel $\ker(\phi)$ is a *normal subgroup*, and the image $\mathrm{im}(\phi)$ is a subgroup of H.

Proof. There is only one possible way we can prove this.

To see $\ker(\phi)$ is a subgroup, let $g, h \in \ker\phi$. Then

$$\phi(g \cdot h^{-1}) = \phi(g) * \phi(h)^{-1} = e * e^{-1} = e.$$

So $gh^{-1} \in \ker\phi$. Also, $\phi(e) = e$. So $\ker(\phi)$ is non-empty. So it is a subgroup.

To show it is normal, let $g \in \ker(\phi)$. Let $x \in G$. We want to show $x^{-1}gx \in \ker(\phi)$. We have

$$\phi(x^{-1}gx) = \phi(x^{-1}) * \phi(g) * \phi(x) = \phi(x^{-1}) * \phi(x) = \phi(x^{-1}x) = \phi(e) = e.$$

So $x^{-1}gx \in \ker(\phi)$. So $\ker(\phi)$ is normal.

Also, if $\phi(g), \phi(h) \in \mathrm{im}(\phi)$, then

$$\phi(g) * \phi(h)^{-1} = \phi(gh^{-1}) \in \mathrm{im}(\phi).$$

Also, $e \in \mathrm{im}(\phi)$. So $\mathrm{im}(\phi)$ is non-empty. So $\mathrm{im}(\phi)$ is a subgroup. □

Lemma. If ϕ is an isomorphism, then the inverse ϕ^{-1} is also an isomorphism.

Theorem (First isomorphism theorem)**.** Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \lhd G$ and

$$\frac{G}{\ker(\phi)} \cong \mathrm{im}(\phi).$$

Proof. We have already proved that $\ker(\phi)$ is a normal subgroup. We now have to construct a homomorphism $f : G/\ker(\phi) \to \mathrm{im}(\phi)$, and prove it is an isomorphism.

Define our function as follows:

$$\begin{aligned} f : \frac{G}{\ker(\phi)} &\to \mathrm{im}(\phi) \\ g\ker(\phi) &\mapsto \phi(g). \end{aligned}$$

We first tackle the obvious problem that this might not be well-defined, since we are picking a representative for the coset. If $g\ker(\phi) = g'\ker(\phi)$, then we know $g^{-1} \cdot g' \in \ker(\phi)$. So $\phi(g^{-1} \cdot g') = e$. So we know

$$e = \phi(g^{-1} \cdot g') = \phi(g)^{-1} * \phi(g').$$

Multiplying the whole thing by $\phi(g)$ gives $\phi(g) = \phi(g')$. Hence this function is well-defined.

Next we show it is a homomorphism. To see f is a homomorphism, we have

$$\begin{aligned} f(g\ker(\phi) \cdot g'\ker(\phi)) &= f(gg'\ker(\phi)) \\ &= \phi(gg') \\ &= \phi(g) * \phi(g') \\ &= f(g\ker(\phi)) * f(g'\ker(\phi)). \end{aligned}$$

So f is a homomorphism. Finally, we show it is a bijection.

To show it is surjective, let $h \in \mathrm{im}(\phi)$. Then $h = \phi(g)$ for some g. So $h = f(g\ker(\phi))$ is in the image of f.

To show injectivity, suppose $f(g\ker(\phi)) = f(g'\ker(\phi))$. So $\phi(g) = \phi(g')$. So $\phi(g^{-1} \cdot g') = e$. Hence $g^{-1} \cdot g' \in \ker(\phi)$, and hence $g\ker(\phi) = g'\ker(\phi)$. So done. □

Theorem (Second isomorphism theorem)**.** Let $H \leq G$ and $K \lhd G$. Then $HK = \{h \cdot k : h \in H, k \in K\}$ is a subgroup of G, and $H \cap K \lhd H$. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. Let $hk, h'k' \in HK$. Then

$$h'k'(hk)^{-1} = h'k'k^{-1}h^{-1} = (h'h^{-1})(hk'k^{-1}h^{-1}).$$

The first term is in H, while the second term is $k'k^{-1} \in K$ conjugated by h, which also has to be in K be normality. So this is something in H times something in K, and hence in HK. HK also contains e, and is hence a group.

To show $H \cap K \lhd H$, consider $x \in H \cap K$ and $h \in H$. Consider $h^{-1}xh$. Since $x \in K$, the normality of K implies $h^{-1}xh \in K$. Also, since $x, h \in H$, closure implies $h^{-1}xh \in H$. So $h^{-1}xh \in H \cap K$. So $H \cap K \lhd H$.

Now we can start to prove the second isomorphism theorem. To do so, we apply the first isomorphism theorem to it. Define

$$\begin{aligned} \phi : H &\to G/K \\ h &\mapsto hK \end{aligned}$$

This is easily seen to be a homomorphism. We apply the first isomorphism theorem to this homomorphism. The image is all K-cosets represented by something in H, i.e.

$$\mathrm{im}(\phi) = \frac{HK}{K}.$$

Then the kernel of ϕ is

$$\ker(\phi) = \{h \in H : hK = eK\} = \{h \in H : h \in K\} = H \cap K.$$

So the first isomorphism theorem says

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$ □

Theorem (Third isomorphism theorem)**.** Let $K \leq L \leq G$ be normal subgroups of G. Then

$$\frac{G}{K} \Big/ \frac{L}{K} \cong \frac{G}{L}.$$

Proof. Define the homomorphism

$$\begin{aligned} \phi : G/K &\to G/L \\ gK &\mapsto gL \end{aligned}$$

As always, we have to check this is well-defined. If $gK = g'K$, then $g^{-1}g' \in K \subseteq L$. So $gL = g'L$. This is also a homomorphism since

$$\phi(gK \cdot g'K) = \phi(gg'K) = gg'L = (gL) \cdot (g'L) = \phi(gK) \cdot \phi(g'K).$$

This clearly is surjective, since any coset gL is the image $\phi(gK)$. So the image is G/L. The kernel is then

$$\ker(\phi) = \{gK : gL = L\} = \{gK : g \in L\} = \frac{L}{K}.$$

So the conclusion follows by the first isomorphism theorem. □

Lemma. An abelian group is simple if and only if it is isomorphic to the cyclic group C_p for some prime number p.

Proof. By Lagrange's theorem, any subgroup of C_p has order dividing $|C_p| = p$. Hence if p is prime, then it has no such divisors, and any subgroup must have order 1 or p, i.e. it is either $\{e\}$ or C_p itself. Hence in particular any normal subgroup must be $\{e\}$ or C_p. So it is simple.

Now suppose G is abelian and simple. Let $e \neq g \in G$ be a non-trivial element, and consider $H = \{\cdots, g^{-2}, g^{-1}, e, g, g^2, \cdots\}$. Since G is abelian, conjugation does nothing, and every subgroup is normal. So H is a normal subgroup. As G is simple, $H = \{e\}$ or $H = G$. Since it contains $g \neq e$, it is non-trivial. So we must have $H = G$. So G is cyclic.

If G is infinite cyclic, then it is isomorphic to $\mathbb{Z}$. But $\mathbb{Z}$ is not simple, since $2\mathbb{Z} \lhd \mathbb{Z}$. So G is a finite cyclic group, i.e. $G \cong C_m$ for some finite m.

If $n \mid m$, then $g^{m/n}$ generates a subgroup of G of order n. So this is a normal subgroup. Therefore n must be m or 1. Hence G cannot be simple unless m has no divisors except 1 and m, i.e. m is a prime. □

Theorem. Let G be any finite group. Then there are subgroups

$$G = H_1 \rhd H_2 \rhd H_3 \rhd H_4 \rhd \cdots \rhd H_n = \{e\}.$$

such that H_i/H_{i+1} is simple.

Proof. If G is simple, let $H_2 = \{e\}$. Then we are done.

If G is not simple, let H_2 be a maximal proper normal subgroup of G. We now claim that G/H_2 is simple.

If G/H_2 is not simple, it contains a proper non-trivial normal subgroup $L \lhd G/H_2$ such that $L \neq \{e\}, G/H_2$. However, there is a correspondence between normal subgroups of G/H_2 and normal subgroups of G containing H_2. So L must be K/H_2 for some $K \lhd G$ such that $K \geq H_2$. Moreover, since L is non-trivial and not G/H_2, we know K is not G or H_2. So K is a larger normal subgroup. Contradiction.

So we have found an $H_2 \lhd G$ such that G/H_2 is simple. Iterating this process on H_2 gives the desired result. Note that this process eventually stops, as $H_{i+1} < H_i$, and hence $|H_{i+1}| < |H_i|$, and all these numbers are finite. □

1.3 Actions of permutations

Lemma. An action of G on X is equivalent to a homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. Let $* : G \times X \to X$ be an action. Define $\phi : G \to \mathrm{Sym}(X)$ by sending g to the function $\phi(g) = (g * \cdot : X \to X)$. This is indeed a permutation — $g^{-1} * \cdot$ is an inverse since

$$\phi(g^{-1})(\phi(g)(x)) = g^{-1} * (g * x) = (g^{-1} \cdot g) * x = e * x = x,$$

and a similar argument shows $\phi(g) \circ \phi(g^{-1}) = \mathrm{id}_X$. So ϕ is at least a well-defined function.

To show it is a homomorphism, just note that

$$\phi(g_1)(\phi(g_2)(x)) = g_1 * (g_2 * x) = (g_1 \cdot g_2) * x = \phi(g_1 \cdot g_2)(x).$$

Since this is true for all $x \in X$, we know $\phi(g_1) \circ \phi(g_2) = \phi(g_1 \cdot g_2)$. Also, $\phi(e)(x) = e * x = x$. So $\phi(e)$ is indeed the identity. Hence ϕ is a homomorphism.

We now do the same thing backwards. Given a homomorphism $\phi : G \to \mathrm{Sym}(X)$, define a function by $g * x = \phi(g)(x)$. We now check it is indeed a group action. Using the definition of a homomorphism, we know

(i) $g_1 * (g_2 * x) = \phi(g_1)(\phi(g_2)(x)) = (\phi(g_1) \circ \phi(g_2))(x) = \phi(g_1 \cdot g_2)(x) = (g_1 \cdot g_2) * x$.

(ii) $e * x = \phi(e)(x) = \mathrm{id}_X(x) = x$.

So this homomorphism gives a group action. These two operations are clearly inverses to each other. So group actions of G on X are the same as homomorphisms $G \to \mathrm{Sym}(X)$. □

Proposition. $G_X \lhd G$ and $G/G_X \cong G^X$.

Theorem. Let G be a finite group, and $H \leq G$ a subgroup of index n. Then there is a normal subgroup $K \lhd G$ with $K \leq H$ such that G/K is isomorphic to a subgroup of S_n. Hence $|G/K| \mid n!$ and $|G/K| \geq n$.

Proof. We apply the previous example, giving $\phi : G \to \mathrm{Sym}(G/H)$, and let K be the kernel of this homomorphism. We have already shown that $K \leq H$. Then the first isomorphism theorem gives

$$G/K \cong \mathrm{im}\,\phi \leq \mathrm{Sym}(G/H) \cong S_n.$$

Then by Lagrange's theorem, we know $|G/K| \mid |S_n| = n!$, and we also have $|G/K| \geq |G/H| = n$. □

Corollary. Let G be a non-abelian simple group. Let $H \leq G$ be a proper subgroup of index n. Then G is isomorphic to a subgroup of A_n. Moreover, we must have $n \geq 5$, i.e. G cannot have a subgroup of index less than 5.

Proof. The action of G on $X = G/H$ gives a homomorphism $\phi : G \to \mathrm{Sym}(X)$. Then $\ker(\phi) \lhd G$. Since G is simple, $\ker(\phi)$ is either G or $\{e\}$. We first show that it cannot be G. If $\ker(\phi) = G$, then every element of G acts trivially on $X = G/H$. But if $g \in G \setminus H$, which exists since the index of H is not 1, then $g * H = gH \neq H$. So g does not act trivially. So the kernel cannot be the whole of G. Hence $\ker(\phi) = \{e\}$.

Thus by the first isomorphism theorem, we get

$$G \cong \mathrm{im}(\phi) \leq \mathrm{Sym}(X) \cong S_n.$$

We now need to show that G is in fact a subgroup of A_n.

We know $A_n \lhd S_n$. So $\mathrm{im}(\phi) \cap A_n \lhd \mathrm{im}(\phi) \cong G$. As G is simple, $\mathrm{im}(\phi) \cap A_n$ is either $\{e\}$ or $G = \mathrm{im}(\phi)$. We want to show that the second thing happens, i.e. the intersection is not the trivial group. We use the second isomorphism theorem. If $\mathrm{im}(\phi) \cap A_n = \{e\}$, then

$$\mathrm{im}(\phi) \cong \frac{\mathrm{im}(\phi)}{\mathrm{im}(\phi) \cap A_n} \cong \frac{\mathrm{im}(\phi) A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2.$$

So $G \cong \mathrm{im}(\phi)$ is a subgroup of C_2, i.e. either $\{e\}$ or C_2 itself. Neither of these are non-abelian. So this cannot be the case. So we must have $\mathrm{im}(\phi) \cap A_n = \mathrm{im}(\phi)$, i.e. $\mathrm{im}(\phi) \leq A_n$.

The last part follows from the fact that S_1, S_2, S_3, S_4 have no non-abelian simple subgroups, which you can check by going to a quiet room and listing out all their subgroups. □

Theorem (Orbit-stabilizer theorem)**.** Let G act on X. Then for any $x \in X$, there is a bijection between $G \cdot x$ and G/G_x, given by $g \cdot x \leftrightarrow g \cdot G_x$.

In particular, if G is finite, it follows that

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

1.4 Conjugacy, centralizers and normalizers

Proposition. Let G be a finite group. Then

$$|\operatorname{ccl}(x)| = |G : C_G(x)| = |G|/|C_G(x)|.$$

Theorem. The alternating groups A_n are simple for $n \geq 5$ (also for $n = 1, 2, 3$).

Proof. We start with the following claim:

Claim. A_n is generated by 3-cycles.

As any element of A_n is a product of evenly-many transpositions, it suffices to show that every product of two transpositions is also a product of 3-cycles.

There are three possible cases: let a, b, c, d be distinct. Then

(i) $(a\ b)(a\ b) = e$.

(ii) $(a\ b)(b\ c) = (a\ b\ c)$.

(iii) $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.

So we have shown that every possible product of two transpositions is a product of three-cycles.

Claim. Let $H \lhd A_n$. If H contains a 3-cycle, then we $H = A_n$.

We show that if H contains a 3-cycle, then *every* 3-cycle is in H. Then we are done since A_n is generated by 3-cycles. For concreteness, suppose we know $(a\ b\ c) \in H$, and we want to show $(1\ 2\ 3) \in H$.

Since they have the same cycle type, so we have $\sigma \in S_n$ such that $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$. If σ is even, i.e. $\sigma \in A_n$, then we have that $(1\ 2\ 3) \in \sigma^{-1}H\sigma = H$, by the normality of H and we are trivially done.

If σ is odd, replace it by $\bar{\sigma} = \sigma \cdot (4\ 5)$. Here is where we use the fact that $n \geq 5$ (we will use it again later). Then we have

$$\bar{\sigma}(1\ 2\ 3)\bar{\sigma}^{-1} = \sigma(4\ 5)(1\ 2\ 3)(4\ 5)\sigma^{-1} = \sigma(1\ 2\ 3)\sigma^{-1} = (a\ b\ c),$$

using the fact that $(1\ 2\ 3)$ and $(4\ 5)$ commute. Now $\bar{\sigma}$ is even. So $(1\ 2\ 3) \in H$ as above.

What we've got so far is that if $H \lhd A_n$ contains *any* 3-cycle, then it is A_n. Finally, we have to show that every normal subgroup must contain at least one 3-cycle.

Claim. Let $H \lhd A_n$ be non-trivial. Then H contains a 3-cycle.

We separate this into many cases

(i) Suppose H contains an element which can be written in disjoint cycle notation
$$\sigma = (1\ 2\ 3 \cdots r)\tau,$$
for $r \geq 4$. We now let $\delta = (1\ 2\ 3) \in A_n$. Then by normality of H, we know $\delta^{-1}\sigma\delta \in H$. Then $\sigma^{-1}\delta^{-1}\sigma\delta \in H$. Also, we notice that τ does not contain $1, 2, 3$. So it commutes with δ, and also trivially with $(1\ 2\ 3\ \cdots\ r)$. We can expand this mess to obtain
$$\sigma^{-1}\delta^{-1}\sigma\delta = (r\ \cdots\ 2\ 1)(1\ 3\ 2)(1\ 2\ 3\ \cdots\ r)(1\ 2\ 3) = (2\ 3\ r),$$
which is a 3-cycle. So done.

The same argument goes through if $\sigma = (a_1\ a_2\ \cdots\ a_r)\tau$ for any $a_1, \cdots, a_n$.

(ii) Suppose H contains an element consisting of at least two 3-cycles in disjoint cycle notation, say
$$\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$$
We now let $\delta = (1\ 2\ 4)$, and again calculate
$$\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4) = (1\ 2\ 4\ 3\ 6).$$
This is a 5-cycle, which is necessarily in H. By the previous case, we get a 3-cycle in H too, and hence $H = A_n$.

(iii) Suppose H contains $\sigma = (1\ 2\ 3)\tau$, with τ a product of 2-cycles (if τ contains anything longer, then it would fit in one of the previous two cases). Then $\sigma^2 = (1\ 2\ 3)^2 = (1\ 3\ 2)$ is a three-cycle.

(iv) Suppose H contains $\sigma = (1\ 2)(3\ 4)\tau$, where τ is a product of 2-cycles. We first let $\delta = (1\ 2\ 3)$ and calculate
$$u = \sigma^{-1}\delta^{-1}\sigma\delta = (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3),$$
which is again in u. We landed in the same case, but instead of two transpositions times a mess, we just have two transpositions, which is nicer. Now let
$$v = (1\ 5\ 2)u(1\ 2\ 5) = (1\ 3)(4\ 5) \in H.$$
Note that we used $n \geq 5$ again. We have yet again landed in the same case. Notice however, that these are not the same transpositions. We multiply
$$uv = (1\ 4)(2\ 3)(1\ 3)(4\ 5) = (1\ 2\ 3\ 4\ 5) \in H.$$
This is then covered by the first case, and we are done.

So done. Phew. □

1.5 Finite p-groups

Theorem. If G is a finite p-group, then $Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}$ is non-trivial.

Proof. Let G act on itself by conjugation. The orbits of this action (i.e. the conjugacy classes) have order dividing $|G| = p^n$. So it is either a singleton, or its size is divisible by p.

Since the conjugacy classes partition G, we know the total size of the conjugacy classes is $|G|$. In particular,

$$|G| = \text{number of conjugacy class of size 1} + \sum \text{order of all other conjugacy classes.}$$

We know the second term is divisible by p. Also $|G| = p^n$ is divisible by p. Hence the number of conjugacy classes of size 1 is divisible by p. We know $\{e\}$ is a conjugacy class of size 1. So there must be at least p conjugacy classes of size 1. Since the smallest prime number is 2, there is a conjugacy class $\{x\} \neq \{e\}$.

But if $\{x\}$ is a conjugacy class on its own, then by definition $g^{-1}xg = x$ for all $g \in G$, i.e. $xg = gx$ for all $g \in G$. So $x \in Z(G)$. So $Z(G)$ is non-trivial. □

Lemma. For any group G, if $G/Z(G)$ is cyclic, then G is abelian.

In other words, if $G/Z(G)$ is cyclic, then it is in fact trivial, since the center of an abelian group is the abelian group itself.

Proof. Let $g \in Z(G)$ be a generator of the cyclic group $G/Z(G)$. Hence every coset of $Z(G)$ is of the form $g^r Z(G)$. So every element $x \in G$ must be of the form $g^r z$ for $z \in Z(G)$ and $r \in \mathbb{Z}$. To show G is abelian, let $\bar{x} = g^{\bar{r}}\bar{z}$ be another element, with $\bar{z} \in Z(G), \bar{r} \in \mathbb{Z}$. Note that z and $\bar{z}$ are in the center, and hence commute with every element. So we have

$$x\bar{x} = g^r z g^{\bar{r}} \bar{z} = g^r g^{\bar{r}} z\bar{z} = g^{\bar{r}} g^r \bar{z} z = g^{\bar{r}} \bar{z} g^r z = \bar{x}x.$$

So they commute. So G is abelian. □

Corollary. If p is prime and $|G| = p^2$, then G is abelian.

Proof. Since $Z(G) \leq G$, its order must be 1, p or p^2. Since it is not trivial, it can only be p or p^2. If it has order p^2, then it is the whole group and the group is abelian. Otherwise, $G/Z(G)$ has order $p^2/p = p$. But then it must be cyclic, and thus G must be abelian. This is a contradiction. So G is abelian. □

Theorem. Let G be a group of order p^a, where p is a prime number. Then it has a subgroup of order p^b for any $0 \leq b \leq a$.

Proof. We induct on a. If $a = 1$, then $\{e\}, G$ give subgroups of order p^0 and p^1. So done.

Now suppose $a > 1$, and we want to construct a subgroup of order p^b. If $b = 0$, then this is trivial, namely $\{e\} \leq G$ has order 1.

Otherwise, we know $Z(G)$ is non-trivial. So let $x \neq e \in Z(G)$. Since $\text{ord}(x) \mid |G|$, its order is a power of p. If it in fact has order p^c, then $x^{p^{c-1}}$ has order p. So we can suppose, by renaming, that x has order p. We have thus

generated a subgroup $\langle x\rangle$ of order exactly p. Moreover, since x is in the center, $\langle x\rangle$ commutes with everything in G. So $\langle x\rangle$ is in fact a normal subgroup of G. This is the point of choosing it in the center. Therefore $G/\langle x\rangle$ has order p^{a-1}.

Since this is a strictly smaller group, we can by induction suppose $G/\langle x\rangle$ has a subgroup of any order. In particular, it has a subgroup L of order p^{b-1}. By the subgroup correspondence, there is some $K \leq G$ such that $L = K/\langle x\rangle$ and $H \lhd K$. But then K has order p^b. So done. □

1.6 Finite abelian groups

Theorem (Classification of finite abelian groups)**.** Let G be a finite abelian group. Then there exist some $d_1, \cdots, d_r$ such that

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}.$$

Moreover, we can pick d_i such that $d_{i+1} \mid d_i$ for each i, and this expression is unique.

Lemma. If n and m are coprime, then $C_{mn} \cong C_m \times C_n$.

Proof. It suffices to find an element of order nm in $C_m \times C_n$. Then since $C_n \times C_m$ has order nm, it must be cyclic, and hence isomorphic to C_{nm}.

Let $g \in C_m$ have order m; $h \in C_n$ have order n, and consider $(g, h) \in C_m \times C_n$. Suppose the order of (g, h) is k. Then $(g, h)^k = (e, e)$. Hence $(g^k, h^k) = (e, e)$. So the order of g and h divide k, i.e. $m \mid k$ and $n \mid k$. As m and n are coprime, this means that $mn \mid k$.

As $k = \text{ord}((g, h))$ and $(g, h) \in C_m \times C_n$ is a group of order mn, we must have $k \mid nm$. So $k = nm$. □

Corollary. For any finite abelian group G, we have

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r},$$

where each d_i is some prime power.

Proof. From the classification theorem, iteratively apply the previous lemma to break each component up into products of prime powers. □

1.7 Sylow theorems

Theorem (Sylow theorems)**.** Let G be a finite group of order $p^a \cdot m$, with p a prime and $p \nmid m$. Then

(i) The set of Sylow p-subgroups of G, given by

$$\text{Syl}_p(G) = \{P \leq G : |P| = p^a\},$$

is non-empty. In other words, G has a subgroup of of order p^a.

(ii) All elements of $\text{Syl}_p(G)$ are conjugate in G.

(iii) The number of Sylow p-subgroups $n_p = |\text{Syl}_p(G)|$ satisfies $n_p \equiv 1 \pmod p$ and $n_p \mid |G|$ (in fact $n_p \mid m$, since p is not a factor of n_p).

Lemma. If $n_p = 1$, then the Sylow p-subgroup is normal in G.

Proof. Let P be the unique Sylow p-subgroup, and let $g \in G$, and consider $g^{-1}Pg$. Since this is isomorphic to P, we must have $|g^{-1}Pg| = p^a$, i.e. it is also a Sylow p-subgroup. Since there is only one, we must have $P = g^{-1}Pg$. So P is normal. □

Corollary. Let G be a non-abelian simple group. Then $|G| \mid \frac{n_p!}{2}$ for every prime p such that $p \mid |G|$.

Proof. The group G acts on $\mathrm{Syl}_p(G)$ by conjugation. So it gives a permutation representation $\phi : G \to \mathrm{Sym}(\mathrm{Syl}_p(G)) \cong S_{n_p}$. We know $\ker\phi \lhd G$. But G is simple. So $\ker(\phi) = \{e\}$ or G. We want to show it is not the whole of G.

If we had $G = \ker(\phi)$, then $g^{-1}Pg = P$ for all $g \in G$. Hence P is a normal subgroup. As G is simple, either $P = \{e\}$, or $P = G$. We know P cannot be trivial since $p \mid |G|$. But if $G = P$, then G is a p-group, has a non-trivial center, and hence G is not non-abelian simple. So we must have $\ker(\phi) = \{e\}$.

Then by the first isomorphism theorem, we know $G \cong \mathrm{im}\,\phi \leq S_{n_p}$. We have proved the theorem without the divide-by-two part. To prove the whole result, we need to show that in fact $\mathrm{im}(\phi) \leq A_{n_p}$. Consider the following composition of homomorphisms:

$$G \xrightarrow{\phi} S_{n_p} \xrightarrow{\mathrm{sgn}} \{\pm 1\}.$$

If this is surjective, then $\ker(\mathrm{sgn}\circ\phi) \lhd G$ has index 2 (since the index is the size of the image), and is not the whole of G. This means G is not simple (the case where $|G| = C_2$ is ruled out since it is abelian).

So the kernel must be the whole G, and $\mathrm{sgn}\circ\phi$ is the trivial map. In other words, $\mathrm{sgn}(\phi(g)) = +1$. So $\phi(g) \in A_{n_p}$. So in fact we have

$$G \cong \mathrm{im}(\phi) \leq A_{n_p}.$$

So we get $|G| \mid \frac{n_p!}{2}$. □

Proof of Sylow's theorem. Let G be a finite group with $|G| = p^a m$, and $p \nmid m$.

(i) We need to show that $\mathrm{Syl}_p(G) \neq \emptyset$, i.e. we need to find some subgroup of order p^a. As always, we find something clever for G to act on. We let

$$\Omega = \{X \text{ sub}\textit{set} \text{ of } G : |X| = p^a\}.$$

We let G act on Ω by

$$g * \{g_1, g_2, \cdots, g_{p^a}\} = \{gg_1, gg_2, \cdots, gg_{p^a}\}.$$

Let $\Sigma \leq \Omega$ be an orbit.

We first note that if $\{g_1, \cdots, g_{p^a}\} \in \Sigma$, then by the definition of an orbit, for every $g \in G$,

$$gg_1^{-1} * \{g_1, \cdots, g_{p^a}\} = \{g, gg_1^{-1}g_2, \cdots, gg_1^{-1}g_{p^a}\} \in \Sigma.$$

The important thing is that this set contains g. So for each g, Σ contains a set X which contains g. Since each set X has size p^a, we must have

$$|\Sigma| \geq \frac{|G|}{p^a} = m.$$

Suppose $|\Sigma| = m$. Then the orbit-stabilizer theorem says the stabilizer H of any $\{g_1, \cdots, g_{p^a}\} \in \Sigma$ has index m, hence $|H| = p^a$, and thus $H \in \mathrm{Syl}_p(G)$.

So we need to show that not every orbit Σ can have size $> m$. Again, by the orbit-stabilizer, the size of any orbit divides the order of the group, $|G| = p^a m$. So if $|\Sigma| > m$, then $p \mid |\Sigma|$. Suppose we can show that $p \nmid |\Omega|$. Then not every orbit Σ can have size $> m$, since Ω is the disjoint union of all the orbits, and thus we are done.

So we have to show $p \nmid |\Omega|$. This is just some basic counting. We have

$$|\Omega| = \binom{|G|}{p^a} = \binom{p^a m}{p^a} = \prod_{j=0}^{p^a-1} = \frac{p^a m - j}{p^a - j}.$$

Now note that the largest power of p dividing $p^a m - j$ is the largest power of p dividing j. Similarly, the largest power of p dividing $p^a - j$ is also the largest power of p dividing j. So we have the same power of p on top and bottom for each item in the product, and they cancel. So the result is not divisible by p.

This proof is not straightforward. We first needed the clever idea of letting G act on Ω. But then if we are given this set, the obvious thing to do would be to find something in Ω that is also a group. This is not what we do. Instead, we find an orbit whose stabilizer is a Sylow p-subgroup.

(ii) We instead prove something stronger: if $Q \leq G$ is a p-subgroup (i.e. $|Q| = p^b$, for b not necessarily a), and $P \leq G$ is a Sylow p-subgroup, then there is a $g \in G$ such that $g^{-1}Qg \leq P$. Applying this to the case where Q is another Sylow p-subgroup says there is a g such that $g^{-1}Qg \leq P$, but since $g^{-1}Qg$ has the same size as P, they must be equal.

We let Q act on the set of cosets of G/P via

$$q * gP = qgP.$$

We know the orbits of this action have size dividing $|Q|$, so is either 1 or divisible by p. But they can't all be divisible by p, since $|G/P|$ is coprime to p. So at least one of them have size 1, say $\{gP\}$. In other words, for every $q \in Q$, we have $qgP = gP$. This means $g^{-1}qg \in P$. This holds for every element $q \in Q$. So we have found a g such that $g^{-1}Qg \leq P$.

(iii) Finally, we need to show that $n_p \cong 1 \pmod p$ and $n_p \mid |G|$, where $n_p = |\mathrm{Syl}_P(G)|$.

The second part is easier — by Sylow's second theorem, the action of G on $\mathrm{Syl}_p(G)$ by conjugation has one orbit. By the orbit-stabilizer theorem, the size of the orbit, which is $|\mathrm{Syl}_p(G)| = n_p$, divides $|G|$. This proves the second part.

For the first part, let $P \in \mathrm{Syl}_P(G)$. Consider the action by conjugation of P on $\mathrm{Syl}_p(G)$. Again by the orbit-stabilizer theorem, the orbits each have size 1 or size divisible by p. But we know there is one orbit of size 1, namely $\{P\}$ itself. To show $n_p = |\mathrm{Syl}_P(G)| \cong 1 \pmod p$, it is enough to show there are no other orbits of size 1.

Suppose $\{Q\}$ is an orbit of size 1. This means for every $p \in P$, we get

$$p^{-1}Qp = Q.$$

In other words, $P \leq N_G(Q)$. Now $N_G(Q)$ is itself a group, and we can look at its Sylow p-subgroups. We know $Q \leq N_G(Q) \leq G$. So $p^a \mid |N_G(Q)| \mid p^a m$. So p^a is the biggest power of p that divides $|N_G(Q)|$. So Q is a Sylow p-subgroup of $N_G(Q)$.

Now we know $P \leq N_G(Q)$ is *also* a Sylow p-subgroup of $N_G(Q)$. By Sylow's second theorem, they must be conjugate in $N_G(Q)$. But conjugating anything in Q by something in $N_G(Q)$ does nothing, by definition of $N_G(Q)$. So we must have $P = Q$. So the only orbit of size 1 is $\{P\}$ itself. So done. □

2 Rings

2.1 Definitions and examples

2.2 Homomorphisms, ideals, quotients and isomorphisms

Lemma. A homomorphism $\phi : R \to S$ is injective if and only if $\ker \phi = \{0_R\}$.

Proof. A ring homomorphism is in particular a group homomorphism $\phi : (R, +, 0_R) \to (S, +, 0_S)$ of abelian groups. So this follows from the case of groups. □

Lemma. If $\phi : R \to S$ is a homomorphism, then $\ker(\phi) \lhd R$.

Proof. Since $\phi : (R, +, 0_R) \to (S, +, 0_S)$ is a group homomorphism, the kernel is a subgroup of $(R, +, 0_R)$.

For the second part, let $a \in \ker(\phi)$, $b \in R$. We need to show that their product is in the kernel. We have

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0 \cdot \phi(b) = 0.$$

So $a \cdot b \in \ker(\phi)$. □

Proposition. The quotient ring is a ring, and the function

$$\begin{aligned} R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

is a ring homomorphism.

Proof. We know the group $(R/I, +, 0_{R/I})$ is well-defined, since I is a (normal) subgroup of R. So we only have to check multiplication is well-defined.

Suppose $r_1 + I = r_1' + I$ and $r_2 + I = r_2' + I$. Then $r_1' - r_1 = a_1 \in I$ and $r_2' - r_2 = a_2 \in I$. So

$$r_1' r_2' = (r_1 + a_1)(r_2 + a_2) = r_1 r_2 + r_1 a_2 + r_2 a_1 + a_1 a_2.$$

By the strong closure property, the last three objects are in I. So $r_1' r_2' + I = r_1 r_2 + I$.

It is easy to check that $0_R + I$ and $1_R + I$ are indeed the zero and one, and the function given is clearly a homomorphism. □

Proposition (Euclidean algorithm for polynomials)**.** Let $\mathbb{F}$ be a field and $f, g \in \mathbb{F}[X]$. Then there is some $r, q \in \mathbb{F}[X]$ such that

$$f = gq + r,$$

with $\deg r < \deg g$.

Proof. Let $\deg(f) = n$. So

$$f = \sum_{i=0}^{n} a_i X^i,$$

and $a_n \neq 0$. Similarly, if $\deg g = m$, then

$$g = \sum_{i=0}^{m} b_i X^i,$$

with $b_m \neq 0$. If $n < m$, we let $q = 0$ and $r = f$, and done.

Otherwise, suppose $n \geq m$, and proceed by induction on n.

We let

$$f_1 = f - a_n b_m^{-1} X^{n-m} g.$$

This is possible since $b_m \neq 0$, and $\mathbb{F}$ is a field. Then by construction, the coefficients of X^n cancel out. So $\deg(f_1) < n$.

If $n = m$, then $\deg(f_1) < n = m$. So we can write

$$f = (a_n b_m^{-1} X^{n-m})g + f_1,$$

and $\deg(f_1) < \deg(f)$. So done. Otherwise, if $n > m$, then as $\deg(f_1) < n$, by induction, we can find r_1, q_1 such that

$$f_1 = gq_1 + r_1,$$

and $\deg(r_1) < \deg g = m$. Then

$$f = a_n b_m^{-1} X^{n-m} g + q_1 g + r_1 = (a_n b_m^{-1} X^{n-m} + q_1)g + r_1.$$

So done. □

Theorem (First isomorphism theorem)**.** Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \lhd R$, and

$$\frac{R}{\ker(\phi)} \cong \mathrm{im}(\phi) \leq S.$$

Proof. We have already seen $\ker(\phi) \lhd R$. Now define

$$\begin{aligned} \Phi : R/\ker(\phi) &\to \mathrm{im}(\phi) \\ r + \ker(\phi) &\mapsto \phi(r). \end{aligned}$$

This well-defined, since if $r + \ker(\phi) = r' + \ker(\phi)$, then $r - r' \in \ker(\phi)$. So $\phi(r - r') = 0$. So $\phi(r) = \phi(r')$.

We don't have to check this is bijective and additive, since that comes for free from the (proof of the) isomorphism theorem of groups. So we just have to check it is multiplicative. To show Φ is multiplicative, we have

$$\begin{aligned} \Phi((r + \ker(\phi))(t + \ker(\phi))) &= \Phi(rt + \ker(\phi)) \\ &= \phi(rt) \\ &= \phi(r)\phi(t) \\ &= \Phi(r + \ker(\phi))\Phi(t + \ker(\phi)). \end{aligned}$$ □

Theorem (Second isomorphism theorem)**.** Let $R \leq S$ and $J \lhd S$. Then $J \cap R \lhd R$, and

$$\frac{R + J}{J} = \{r + J : r \in R\} \leq \frac{S}{J}$$

is a subring, and

$$\frac{R}{R \cap J} \cong \frac{R + J}{J}.$$

Proof. Define the function

$$\begin{aligned}\phi : R &\to S/J\\ r &\mapsto r + J.\end{aligned}$$

Since this is the quotient map, it is a ring homomorphism. The kernel is

$$\ker(\phi) = \{r \in R : r + J = 0, \text{ i.e. } r \in J\} = R \cap J.$$

Then the image is

$$\mathrm{im}(\phi) = \{r + J : r \in R\} = \frac{R + J}{J}.$$

Then by the first isomorphism theorem, we know $R \cap J \lhd R$, and $\frac{R+J}{J} \leq S$, and

$$\frac{R}{R \cap J} \cong \frac{R + J}{J}.$$ □

Theorem (Third isomorphism theorem)**.** Let $I \lhd R$ and $J \lhd R$, and $I \subseteq J$. Then $J/I \lhd R/I$ and

$$\left(\frac{R}{I}\right) / \left(\frac{J}{I}\right) \cong \frac{R}{J}.$$

Proof. We define the map

$$\begin{aligned}\phi : R/I &\to R/J\\ r + I &\mapsto r + J.\end{aligned}$$

This is well-defined and surjective by the groups case. Also it is a ring homomorphism since multiplication in R/I and R/J are "the same". The kernel is

$$\ker(\phi) = \{r + I : r + J = 0, \text{ i.e. } r \in J\} = \frac{J}{I}.$$

So the result follows from the first isomorphism theorem. □

2.3 Integral domains, field of factions, maximal and prime ideals

Lemma. Let R be a finite ring which is an integral domain. Then R is a field.

Proof. Let $a \in R$ be non-zero, and consider the ring homomorphism

$$\begin{aligned}a \cdot - : R &\to R\\ b &\mapsto a \cdot b\end{aligned}$$

We want to show this is injective. For this, it suffices to show the kernel is trivial. If $r \in \ker(a \cdot -)$, then $a \cdot r = 0$. So $r = 0$ since R is an integral domain. So the kernel is trivial.

Since R is finite, $a \cdot -$ must also be surjective. In particular, there is an element $b \in R$ such that $a \cdot b = 1_R$. So a has an inverse. Since a was arbitrary, R is a field. □

Lemma. Let R be an integral domain. Then $R[X]$ is also an integral domain.

Proof. We need to show that the product of two non-zero elements is non-zero. Let $f, g \in R[X]$ be non-zero, say

$$f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$
$$g = b_0 + b_1X + \cdots + b_mX^m \in R[X],$$

with $a_n, b_m \neq 0$. Then the coefficient of X^{n+m} in fg is a_nb_m. This is non-zero since R is an integral domain. So fg is non-zero. So $R[X]$ is an integral domain. □

Theorem. Every integral domain has a field of fractions.

Proof. The construction is exactly how we construct the rationals from the integers — as equivalence classes of pairs of integers. We let

$$S = \{(a, b) \in R \times R : b \neq 0\}.$$

We think of $(a, b) \in S$ as $\frac{a}{b}$. We define the equivalence relation $\sim$ on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

We need to show this is indeed a equivalence relation. Symmetry and reflexivity are obvious. To show transitivity, suppose

$$(a, b) \sim (c, d), \quad (c, d) \sim (e, f),$$

i.e.

$$ad = bc, \quad cf = de.$$

We multiply the first equation by f and the second by b, to obtain

$$adf = bcf, \quad bcf = bed.$$

Rearranging, we get

$$d(af - be) = 0.$$

Since d is in the denominator, $d \neq 0$. Since R is an integral domain, we must have $af - be = 0$, i.e. $af = be$. So $(a, b) \sim (e, f)$. This is where being an integral domain is important.

Now let

$$F = S/\sim$$

be the set of equivalence classes. We now want to check this is indeed the field of fractions. We first want to show it is a field. We write $\frac{a}{b} = [(a, b)] \in F$, and define the operations by

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

These *are* well-defined, and make $(F, +, \cdot, \frac{0}{1}, \frac{1}{1})$ into a ring. There are many things to check, but those are straightforward, and we will not waste time doing that here.

Finally, we need to show every non-zero element has an inverse. Let $\frac{a}{b} \neq 0_F$, i.e. $\frac{a}{b} \neq \frac{0}{1}$, or $a \cdot 1 \neq b \cdot 0 \in R$, i.e. $a \neq 0$. Then $\frac{b}{a} \in F$ is defined, and

$$\frac{b}{a} \cdot \frac{a}{b} = \frac{ba}{ba} = 1_F.$$

So $\frac{a}{b}$ has a multiplicative inverse. So F is a field.

We now need to construct a subring of F that is isomorphic to R. To do so, we need to define an injective isomorphism $\phi : R \to F$. This is given by

$$\begin{aligned} \phi : R &\to F \\ r &\mapsto \frac{r}{1}. \end{aligned}$$

This is a ring homomorphism, as one can check easily. The kernel is the set of all $r \in R$ such that $\frac{r}{1} = 0$, i.e. $r = 0$. So the kernel is trivial, and ϕ is injective. Then by the first isomorphism theorem, $R \cong \mathrm{im}(\phi) \subseteq F$.

Finally, we need to show everything is a quotient of two things in R. We have

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1},$$

as required. □

Lemma. A (non-zero) ring R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. ($\Rightarrow$) Let $I \lhd R$ and R be a field. Suppose $x \neq 0 \in I$. Then as x is a unit, $I = R$.

($\Leftarrow$) Suppose $x \neq 0 \in R$. Then (x) is an ideal of R. It is not $\{0\}$ since it contains x. So $(x) = R$. In other words $1_R \in (x)$. But (x) is defined to be $\{x \cdot y : y \in R\}$. So there is some $u \in R$ such that $x \cdot u = 1_R$. So x is a unit. Since x was arbitrary, R is a field. □

Lemma. An ideal $I \lhd R$ is maximal if and only if R/I is a field.

Proof. R/I is a field if and only if $\{0\}$ and R/I are the only ideals of R/I. By the ideal correspondence, this is equivalent to saying I and R are the only ideals of R which contains I, i.e. I is maximal. So done. □

Lemma. An ideal $I \lhd R$ is prime if and only if R/I is an integral domain.

Proof. Let I be prime. Let $a+I, b+I \in R/I$, and suppose $(a+I)(b+I) = 0_{R/I}$. By definition, $(a + I)(b + I) = ab + I$. So we must have $ab \in I$. As I is prime, either $a \in I$ or $b \in I$. So $a + I = 0_{R/I}$ or $b + I = 0_{R/I}$. So R/I is an integral domain.

Conversely, suppose R/I is an integral domain. Let $a, b \in R$ be such that $ab \in I$. Then $(a + I)(b + I) = ab + I = 0_{R/I} \in R/I$. Since R/I is an integral domain, either $a + I = 0_{R/I}$ or $b + I = 0_{R/i}$, i.e. $a \in I$ or $b \in I$. So I is a prime ideal. □

Proposition. Every maximal ideal is a prime ideal.

Proof. $I \lhd R$ is maximal implies R/I is a field implies R/I is an integral domain implies I is prime. □

Alternative proof. Let I be a maximal ideal, and suppose $a, b \notin I$ but $ab \in I$. Then by maximality, $I + (a) = I + (b) = R = (1)$. So we can find some $p, q \in R$ and $n, m \in I$ such that $n + ap = m + bq = 1$. Then

$$1 = (n + ap)(m + bq) = nm + apm + bqn + abpq \in I,$$

since $n, m, ab \in I$. This is a contradiction. □

Lemma. Let R be an integral domain. Then its characteristic is either 0 or a prime number.

Proof. Consider the unique map $\phi : \mathbb{Z} \to R$, and $\ker(\phi) = n\mathbb{Z}$. Then n is the characteristic of R by definition.

By the first isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} = \text{im}(\phi) \leq R$. So $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. So $n\mathbb{Z} \lhd \mathbb{Z}$ is a prime. So $n = 0$ or a prime number. □

2.4 Factorization in integral domains

Lemma. A principal ideal (r) is a prime ideal in R if and only if $r = 0$ or r is prime.

Proof. ($\Rightarrow$) Let (r) be a prime ideal. If $r = 0$, then done. Otherwise, as prime ideals are proper, i.e. not the whole ring, r is not a unit. Now suppose $r \mid a \cdot b$. Then $a \cdot b \in (r)$. But (r) is prime. So $a \in (r)$ or $b \in (r)$. So $r \mid a$ or $r \mid b$. So r is prime.

($\Leftarrow$) If $r = 0$, then $(0) = \{0\} \lhd R$, which is prime since R is an integral domain. Otherwise, let $r \neq 0$ be prime. Suppose $a \cdot b \in (r)$. This means $r \mid a \cdot b$. So $r \mid a$ or $r \mid b$. So $a \in (r)$ and $b \in (r)$. So (r) is prime. □

Lemma. Let $r \in R$ be prime. Then it is irreducible.

Proof. Let $r \in R$ be prime, and suppose $r = ab$. Since $r \mid r = ab$, and r is prime, we must have $r \mid a$ or $r \mid b$. wlog, $r \mid a$. So $a = rc$ for some $c \in R$. So $r = ab = rcb$. Since we are in an integral domain, we must have $1 = cb$. So b is a unit. □

Proposition. Let R be a Euclidean domain. Then R is a principal ideal domain.

Proof. Let R have a Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. We let $I \lhd R$ be a non-zero ideal, and let $b \in I \setminus \{0\}$ be an element with $\phi(b)$ minimal. Then for any $a \in I$, we write

$$a = bq + r,$$

with $r = 0$ or $\phi(r) < \phi(b)$. However, any such r must be in I since $r = a - bq \in I$. So we cannot have $\phi(r) < \phi(b)$. So we must have $r = 0$. So $a = bq$. So $a \in (b)$. Since this is true for all $a \in I$, we must have $I \subseteq (b)$. On the other hand, since $b \in I$, we must have $(b) \subseteq I$. So we must have $I = (b)$. □

Lemma. Let R be a principal ideal domain. If $p \in R$ is irreducible, then it is prime.

Proof. Let $p \in R$ be irreducible, and suppose $p \mid a \cdot b$. Also, suppose $p \nmid a$. We need to show $p \mid b$.

Consider the ideal $(p, a) \lhd R$. Since R is a principal ideal domain, there is some $d \in R$ such that $(p, a) = (d)$. So $d \mid p$ and $d \mid a$.

Since $d \mid p$, there is some q_1 such that $p = q_1 d$. As p is irreducible, either q_1 or d is a unit.

If q_1 is a unit, then $d = q_1^{-1} p$, and this divides a. So $a = q_1^{-1} p x$ for some x. This is a contradiction, since $p \nmid a$.

Therefore d is a unit. So $(p, a) = (d) = R$. In particular, $1_R \in (p, a)$. So suppose $1_R = rp + sa$, for some $r, s \in R$. We now take the whole thing and multiply by b. Then we get

$$b = rpb + sab.$$

We observe that ab is divisible by p, and so is p. So b is divisible by p. So done. □

Lemma. Let R be a principal ideal domain. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals. Then there is some $N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for some $n \geq N$.

Proof. The obvious thing to do when we have an infinite chain of ideals is to take the union of them. We let

$$I = \bigcup_{n \geq 1}^{\infty} I_n,$$

which is again an ideal. Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. We know $a \in I = \bigcup_{n=0}^{\infty} I_n$. So $a \in I_N$ for some N. Then we have

$$(a) \subseteq I_N \subseteq I = (a)$$

So we must have $I_N = I$. So $I_n = I_N = I$ for all $n \geq N$. □

Proposition. Let R be a principal ideal domain. Then R is a unique factorization domain.

Proof. We first need to show any (non-unit) $r \in R$ is a product of irreducibles.

Suppose $r \in R$ cannot be factored as a product of irreducibles. Then it is certainly not irreducible. So we can write $r = r_1 s_1$, with r_1, s_1 both non-units. Since r cannot be factored as a product of irreducibles, wlog r_1 cannot be factored as a product of irreducibles (if both can, then r would be a product of irreducibles). So we can write $r_1 = r_2 s_2$, with r_2, s_2 not units. Again, wlog r_2 cannot be factored as a product of irreducibles. We continue this way.

By assumption, the process does not end, and then we have the following chain of ideals:

$$(r) \subseteq (r_1) \subseteq (r_2) \subseteq \cdots \subseteq (r_n) \subseteq \cdots$$

But then we have an ascending chain of ideals. By the ascending chain condition, these are all eventually equal, i.e. there is some n such that $(r_n) = (r_{n+1}) = (r_{n+2}) = \cdots$. In particular, since $(r_n) = (r_{n+1})$, and $r_n = r_{n+1} s_{n+1}$, then s_{n+1} is a unit. But this is a contradiction, since s_{n+1} is not a unit. So r must be a product of irreducibles.

To show uniqueness, we let $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, with p_i, q_i irreducible. So in particular $p_1 \mid q_1 \cdots q_m$. Since p_1 is irreducible, it is prime. So p_1 divides

some q_i. We reorder and suppose $p_1 \mid q_1$. So $q_1 = p_1 \cdot a$ for some a. But since q_1 is irreducible, a must be a unit. So p_1, q_1 are associates. Since R is a principal ideal domain, hence integral domain, we can cancel p_1 to obtain

$$p_2 p_3 \cdots p_n = (aq_2) q_3 \cdots q_m.$$

We now rename aq_2 as q_2, so that we in fact have

$$p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m.$$

We can then continue to show that p_i and q_i are associates for all i. This also shows that $n = m$, or else if $n = m + k$, saw, then $p_{k+1} \cdots p_n = 1$, which is a contradiction. □

Lemma. Let R be a unique factorization domain. Then greatest common divisors exists, and is unique up to associates.

Proof. We construct the greatest common divisor using the good-old way of prime factorization.

We let $p_1, p_2, \cdots, p_m$ be a list of all irreducible factors of a_i, such that no two of these are associates of each other. We now write

$$a_i = u_i \prod_{j=1}^{m} p_j^{n_{ij}},$$

where $n_{ij} \in \mathbb{N}$ and u_i are units. We let

$$m_j = \min_i \{n_{ij}\},$$

and choose

$$d = \prod_{j=1}^{m} p_j^{m_j}.$$

As, by definition, $m_j \leq n_{ij}$ for all i, we know $d \mid a_i$ for all i.

Finally, if $d' \mid a_i$ for all i, then we let

$$d' = v \prod_{j=1}^{m} p_j^{t_j}.$$

Then we must have $t_j \leq n_{ij}$ for all i, j. So we must have $t_j \leq m_j$ for all j. So $d' \mid d$.

Uniqueness is immediate since any two greatest common divisors have to divide each other. □

2.5 Factorization in polynomial rings

Lemma (Gauss' lemma)**.** Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.

Lemma. Let R be a UFD. If $f, g \in R[X]$ are primitive, then so is fg.

Proof. We let

$$f = a_0 + a_1X + \cdots + a_nX^n,$$
$$g = b_0 + b_1X + \cdots + b_mX^m,$$

where $a_n, b_m \neq 0$, and f, g are primitive. We want to show that the content of fg is a unit.

Now suppose fg is not primitive. Then $c(fg)$ is not a unit. Since R is a UFD, we can find an irreducible p which divides $c(fg)$.

By assumption, $c(f)$ and $c(g)$ are units. So $p \nmid c(f)$ and $p \nmid c(g)$. So suppose $p \mid a_0$, $p \mid a_1$, $\ldots$, $p \mid a_{k-1}$ but $p \nmid a_k$. Note it is possible that $k = 0$. Similarly, suppose $p \mid b_0, p \mid b_1, \cdots, p \mid b_{\ell-1}, p \nmid b_\ell$.

We look at the coefficient of $X^{k+\ell}$ in fg. It is given by

$$\sum_{i+j=k+\ell} a_ib_j = a_{k+\ell}b_0 + \cdots + a_{k+1}b_{\ell-1} + a_kb_\ell + a_{k-1}b_{\ell+1} + \cdots + a_0b_{\ell+k}.$$

By assumption, this is divisible by p. So

$$p \mid \sum_{i+j=k+\ell} a_ib_j.$$

However, the terms $a_{k+\ell}b_0 + \cdots + a_{k+1}b_{\ell-1}$, is divisible by p, as $p \mid b_j$ for $j < \ell$. Similarly, $a_{k-1}b_{\ell+1} + \cdots + a_0b_{\ell+k}$ is divisible by p. So we must have $p \mid a_kb_\ell$. As p is irreducible, and hence prime, we must have $p \mid a_k$ or $p \mid b_\ell$. This is a contradiction. So $c(fg)$ must be a unit. □

Corollary. Let R be a UFD. Then for $f, g \in R[X]$, we have that $c(fg)$ is an associate of $c(f)c(g)$.

Proof. We can write $f = c(f)f_1$ and $g = c(g)g_1$, with f_1 and g_1 irreducible. Then

$$fg = c(f)c(g)f_1g_1.$$

Since f_1g_1 is primitive, so $c(f)c(g)$ is a gcd of the coefficients of fg, and so is $c(fg)$, by definition. So they are associates. □

Lemma (Gauss' lemma)**.** Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.

Proof. We will show that a primitive $f \in R[X]$ is reducible in $R[X]$ if and only if f is reducible in $F[X]$.

One direction is almost immediately obvious. Let $f = gh$ be a product in $R[X]$ with g, h not units. As f is primitive, so are g and h. So both have degree > 0. So g, h are not units in $F[X]$. So f is reducible in $F[X]$.

The other direction is less obvious. We let $f = gh$ in $F[X]$, with g, h not units. So g and h have degree > 0, since F is a field. So we can clear denominators by finding $a, b \in R$ such that $(ag), (bh) \in R[X]$ (e.g. let a be the product of denominators of coefficients of g). Then we get

$$abf = (ag)(bh),$$

and this is a factorization in $R[X]$. Here we have to be careful — (ag) is one thing that lives in $R[X]$, and is not necessarily a product in $R[X]$, since g might not be in $R[X]$. So we should just treat it as a single symbol.

We now write

$$(ag) = c(ag)g_1,$$
$$(bh) = c(bh)h_1,$$

where g_1, h_1 are primitive. So we have

$$ab = c(abf) = c((ag)(bh)) = u \cdot c(ag)c(bh),$$

where $u \in R$ is a unit, by the previous corollary. But also we have

$$abf = c(ag)c(gh)g_1h_1 = u^{-1}abg_1h_1.$$

So cancelling ab gives

$$f = u^{-1}g_1h_1 \in R[X].$$

So f is reducible in $R[X]$. □

Proposition. Let R be a UFD, and F be its field of fractions. Let $g \in R[X]$ be primitive. We let

$$J = (g) \lhd R[X], \quad I = (g) \lhd F[X].$$

Then

$$J = I \cap R[X].$$

In other words, if $f \in R[X]$ and we can write it as $f = gh$, with $h \in F[X]$, then in fact $h \in R[X]$.

Proof. The strategy is the same — we clear denominators in the equation $f = gh$, and then use contents to get that down in $R[X]$.

We certainly have $J \subseteq I \cap R[X]$. Now let $f \in I \cap R[X]$. So we can write

$$f = gh,$$

with $h \in F[X]$. So we can choose $b \in R$ such that $bh \in R[X]$. Then we know

$$bf = g(bh) \in R[X].$$

We let

$$(bh) = c(bh)h_1,$$

for $h_1 \in R[X]$ primitive. Thus

$$bf = c(bh)gh_1.$$

Since g is primitive, so is gh_1. So $c(bh) = uc(bf)$ for u a unit. But bf is really a product in $R[X]$. So we have

$$c(bf) = c(b)c(f) = bc(f).$$

So we have

$$bf = ubc(f)gh_1.$$

Cancelling b gives

$$f = g(uc(f)h_1).$$

So $g \mid f$ in $R[X]$. So $f \in J$. □

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

Proof. We know $R[X]$ has a notion of degree. So we will combine this with the fact that R is a UFD.

Let $f \in R[X]$. We can write $f = c(f)f_1$, with f_1 primitive. Firstly, as R is a UFD, we may factor

$$c(f) = p_1 p_2 \cdots p_n,$$

for $p_i \in R$ irreducible (and also irreducible in $R[X]$). Now we want to deal with f_1.

If f_1 is not irreducible, then we can write

$$f_1 = f_2 f_3,$$

with f_2, f_3 both not units. Since f_1 is primitive, f_2, f_3 also cannot be constants. So we must have $\deg f_2, \deg f_3 > 0$. Also, since $\deg f_2 + \deg f_3 = \deg f_1$, we must have $\deg f_2, \deg f_3 < \deg f_1$. If f_2, f_3 are irreducible, then done. Otherwise, keep on going. We will eventually stop since the degrees have to keep on decreasing. So we can write it as

$$f_1 = q_1 \cdots q_m,$$

with q_i irreducible. So we can write

$$f = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m,$$

a product of irreducibles.

For uniqueness, we first deal with the p's. We note that

$$c(f) = p_1 p_2 \cdots p_n$$

is a unique factorization of the content, up to reordering and associates, as R is a UFD. So cancelling the content, we only have to show that primitives can be factored uniquely.

Suppose we have two factorizations

$$f_1 = q_1 q_2 \cdots q_m = r_1 r_2 \cdots r_\ell.$$

Note that each q_i and each r_i is a factor of the primitive polynomial f_1, so are also primitive. Now we do (maybe) the unexpected thing. We let F be the field of fractions of R, and consider $q_i, r_i \in F[X]$. Since F is a field, F is a Euclidean domain, hence principal ideal domain, hence unique factorization domain.

By Gauss' lemma, since the q_i and r_i are irreducible in $R[X]$, they are also irreducible in $F[X]$. As $F[X]$ is a UFD, we find that $\ell = m$, and after reordering, r_i and q_i are associates, say

$$r_i = u_i q_i,$$

with $u_i \in F[X]$ a unit. What we want to say is that r_i is a unit times q_i in $R[X]$. Firstly, note that $u_i \in F$ as it is a unit. Clearing denominators, we can write

$$a_i r_i = b_i q_i \in R[X].$$

Taking contents, since r_i, q_i are primitives, we know a_i and b_i are associates, say

$$b_i = v_i a_i,$$

with $v_i \in R$ a unit. Cancelling a_i on both sides, we know $r_i = v_i q_i$ as required. □

Proposition (Eisenstein's criterion)**.** Let R be a UFD, and let

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

be primitive with $a_n \neq 0$. Let $p \in R$ be irreducible (hence prime) be such that

(i) $p \nmid a_n$;

(ii) $p \mid a_i$ for all $0 \leq i < n$;

(iii) $p^2 \nmid a_0$.

Then f is irreducible in $R[X]$, and hence in $F[X]$ (where F is the field of fractions of F).

Proof. Suppose we have a factorization $f = gh$ with

$$g = r_0 + r_1 X + \cdots + r_k X^k$$
$$h = s_0 + s_1 X + \cdots + s_\ell X^\ell,$$

for $r_k, s_\ell \neq 0$.

We know $r_k s_\ell = a_n$. Since $p \nmid a_n$, so $p \nmid r_k$ and $p \nmid s_\ell$. We can also look at bottom coefficients. We know $r_0 s_0 = a_0$. We know $p \mid a_0$ and $p^2 \nmid a_0$. So p divides exactly one of r_0 and s_0. wlog, $p \mid r_0$ and $p \nmid s_0$.

Now let j be such that

$$p \mid r_0, \quad p \mid r_1, \cdots, \quad p \mid r_{j-1}, \quad p \nmid r_j.$$

We now look at a_j. This is, by definition,

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1 + r_j s_0.$$

We know $r_0, \cdots, r_{j-1}$ are all divisible by p. So

$$p \mid r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1.$$

Also, since $p \nmid r_j$ and $p \nmid s_0$, we know $p \nmid r_j s_0$, using the fact that p is prime. So $p \nmid a_j$. So we must have $j = n$.

We also know that $j \leq k \leq n$. So we must have $j = k = n$. So $\deg g = n$. Hence $\ell = n - h = 0$. So h is a constant. But we also know f is primitive. So h must be a unit. So this is not a proper factorization. □

2.6 Gaussian integers

Proposition. A prime number $p \in \mathbb{Z}$ is prime in $\mathbb{Z}[i]$ if and only if $p \neq a^2 + b^2$ for $a, b \in \mathbb{Z} \setminus \{0\}$.

Proof. If $p = a^2 + b^2$, then $p = (a + ib)(a - ib)$. So p is not irreducible.

Now suppose $p = uv$, with u, v not units. Taking norms, we get $p^2 = N(u)N(v)$. So if u and v are not units, then $N(u) = N(v) = p$. Writing $u = a + ib$, then this says $a^2 + b^2 = p$. □

Lemma. Let p be a prime number. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field with p elements. Let $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ be the group of invertible elements under multiplication. Then $\mathbb{F}_p^\times \cong C_{p-1}$.

Proof. Certainly $\mathbb{F}_p^\times$ has order $p-1$, and is abelian. We know from the classification of finite abelian groups that if $\mathbb{F}_p^\times$ is not cyclic, then it must contain a subgroup $C_m \times C_m$ for $m > 1$ (we can write it as $C_d \times C_{d'} \times \cdots$, and that $d' \mid d$. So C_d has a subgroup isomorphic to $C_{d'}$).

We consider the polynomial $X^m - 1 \in \mathbb{F}_p[x]$, which is a UFD. At best, this factors into m linear factors. So $X^m - 1$ has at most m distinct roots. But if $C_m \times C_m \leq \mathbb{F}_p^\times$, then we can find m^2 elements of order diving m. So there are m^2 elements of $\mathbb{F}_p$ which are roots of $X^m - 1$. This is a contradiction. So $\mathbb{F}_p^\times$ is cyclic. □

Proposition. The primes in $\mathbb{Z}[i]$ are, up to associates,

(i) Prime numbers $p \in \mathbb{Z} \leq \mathbb{Z}[i]$ such that $p \equiv 3 \pmod 4$.

(ii) Gaussian integers $z \in \mathbb{Z}[i]$ with $N(z) = z\bar{z} = p$ for some prime p such that $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. We first show these are primes. If $p \equiv 3 \pmod 4$, then $p \neq a^2 + b^2$, since a square number mod 4 is always 0 or 1. So these are primes in $\mathbb{Z}[i]$.

On the other hand, if $N(z) = p$, and $z = uv$, then $N(u)N(v) = p$. So $N(u)$ is 1 or $N(v)$ is 1. So u or v is a unit. Note that we did not use the condition that $p \not\equiv 3 \pmod 4$. This is not needed, since $N(z)$ is always a sum of squares, and hence $N(z)$ cannot be a prime that is 3 mod 4.

Now let $z \in \mathbb{Z}[i]$ be irreducible, hence prime. Then $\bar{z}$ is also irreducible. So $N(z) = z\bar{z}$ is a factorization of $N(z)$ into irreducibles. Let $p \in \mathbb{Z}$ be an ordinary prime number dividing $N(z)$, which exists since $N(z) \neq 1$.

Now if $p \equiv 3 \pmod 4$, then p itself is prime in $\mathbb{Z}[i]$ by the first part of the proof. So $p \mid N(z) = z\bar{z}$. So $p \mid z$ or $p \mid \bar{z}$. Note that if $p \mid \bar{z}$, then $p \mid z$ by taking complex conjugates. So we get $p \mid z$. Since both p and z are both irreducible, they must be equal up to associates.

Otherwise, we get $p = 2$ or $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 4$, then $p - 1 = 4k$ for some $k \in \mathbb{Z}$. As $\mathbb{F}_p^\times \cong C_{p-1} = C_{4k}$, there is a unique element of order 2 (this is true for any cyclic group of order $4k$ — think $\mathbb{Z}/4k\mathbb{Z}$). This must be $[-1] \in \mathbb{F}_p$. Now let $a \in \mathbb{F}_p^\times$ be an element of order 4. Then a^2 has order 2. So $[a^2] = [-1]$.

This is a complicated way of saying we can find an a such that $p \mid a^2 + 1$. Thus $p \mid (a + i)(a - i)$. In the case where $p = 2$, we know by checking directly that $2 = (1 + i)(1 - i)$.

In either case, we deduce that p (or 2) is not prime (hence irreducible), since it clearly does not divide $a \pm i$ (or $1 \pm i$). So we can write $p = z_1 z_2$, for $z_1, z_2 \in \mathbb{Z}[i]$ not units. Now we get

$$p^2 = N(p) = N(z_1)N(z_2).$$

As the z_i are not units, we know $N(z_1) = N(z_2) = p$. By definition, this means $p = z_1\bar{z}_1 = z_2\bar{z}_2$. But also $p = z_1 z_2$. So we must have $\bar{z}_1 = z_2$.

Finally, we have $p = z_1\bar{z}_1 \mid N(z) = z\bar{z}$. All these z, z_i are irreducible. So z must be an associate of z_1 (or maybe $\bar{z}_1$). So in particular $N(z) = p$. □

Corollary. An integer $n \in \mathbb{Z}_{\geq 0}$ may be written as $x^2 + y^2$ (as the sum of two squares) if and only if "when we write $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ as a product as distinct primes, then $p_i \equiv 3 \pmod 4$ implies n_i is even".

Proof. If $n = x^2 + y^2$, then we have

$$n = (x + iy)(x - iy) = N(x + iy).$$

Let $z = x + iy$. So we can write $z = \alpha_1 \cdots \alpha_q$ as a product of irreducibles in $\mathbb{Z}[i]$. By the proposition, each α_i is either $\alpha_i = p$ (a genuine prime number with $p \equiv 3 \pmod 4$), or $N(\alpha_i) = p$ is a prime number which is either 2 or $\equiv 1 \pmod 4$. We now take the norm to obtain

$$N = x^2 + y^2 = N(z) = N(\alpha_1)N(\alpha_2)\cdots N(\alpha_q).$$

Now each $N(\alpha_i)$ is either p^2 with $p \equiv 3 \pmod 4$, or is just p for $p = 2$ or $p \equiv 1 \pmod 4$. So if p^m is the largest power of p divides n, we find that n must be even if $p \equiv 3 \pmod 4$.

Conversely, let $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ be a product of distinct primes. Now for each p_i, either $p_i \equiv 3 \pmod 4$, and n_i is even, in which case

$$p_i^{n_i} = (p_i^2)^{n_i/2} = N(p_i^{n_i/2});$$

or $p_i = 2$ or $p_i \equiv 1 \pmod 4$, in which case, the above proof shows that $p_i = N(\alpha_i)$ for some α_i. So $p_i^n = N(\alpha_i^n)$.

Since the norm is multiplicative, we can write n as the norm of some $z \in \mathbb{Z}[i]$. So

$$n = N(z) = N(x + iy) = x^2 + y^2,$$

as required. □

2.7 Algebraic integers

Proposition. Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then the ideal

$$I = \ker(\phi : \mathbb{Z}[X] \to \mathbb{C}, f \mapsto f(\alpha))$$

is principal, and equal to (f_α) for some irreducible monic f_α.

Proof. By definition, there is a monic $f \in \mathbb{Z}[X]$ such that $f(a) = 0$. So $f \in I$. So $I \neq 0$. Now let $f_\alpha \in I$ be such a polynomial of minimal degree. We may suppose that f_α is primitive. We want to show that $I = (f_\alpha)$, and that f_α is irreducible.

Let $h \in I$. We pretend we are living in $\mathbb{Q}[X]$. Then we have the Euclidean algorithm. So we can write

$$h = f_\alpha q + r,$$

with $r = 0$ or $\deg r < \deg f_\alpha$. This was done over $\mathbb{Q}[X]$, not $\mathbb{Z}[X]$. We now clear denominators. We multiply by some $a \in \mathbb{Z}$ to get

$$ah = f_\alpha(aq) + (ar),$$

where now $(aq), (ar) \in \mathbb{Z}[X]$. We now evaluate these polynomials at α. Then we have

$$ah(\alpha) = f_\alpha(\alpha)aq(\alpha) + ar(\alpha).$$

We know $f_\alpha(\alpha) = h(\alpha) = 0$, since f_α and h are both in I. So $ar(\alpha) = 0$. So $(ar) \in I$. As $f_\alpha \in I$ has minimal degree, we cannot have $\deg(r) = \deg(ar) < \deg(f_a)$. So we must have $r = 0$.

Hence we know

$$ah = f_\alpha \cdot (aq)$$

is a factorization in $\mathbb{Z}[X]$. This is almost right, but we want to factor h, not ah. Again, taking contents of everything, we get

$$ac(h) = c(ah) = c(f_\alpha(aq)) = c(aq),$$

as f_α is primitive. In particular, $a \mid c(aq)$. This, by definition of content, means (aq) can be written as $a\bar{q}$, where $\bar{q} \in \mathbb{Z}[X]$. Cancelling, we get $q = \bar{q} \in \mathbb{Z}[X]$. So we know

$$h = f_\alpha q \in (f_\alpha).$$

So we know $I = (f_\alpha)$.

To show f_α is irreducible, note that

$$\frac{\mathbb{Z}[X]}{(f_\alpha)} \cong \frac{\mathbb{Z}[X]}{\ker \phi} \cong \mathrm{im}(\phi) = \mathbb{Z}[\alpha] \leq \mathbb{C}.$$

Since $\mathbb{C}$ is an integral domain, so is $\mathrm{im}(\phi)$. So we know $\mathbb{Z}[X]/(f_\alpha)$ is an integral domain. So (f_α) is prime. So f_α is prime, hence irreducible.

If this final line looks magical, we can unravel this proof as follows: suppose $f_\alpha = pq$ for some non-units pq. Then since $f_\alpha(\alpha) = 0$, we know $p(\alpha)q(\alpha) = 0$. Since $p(\alpha), q(\alpha) \in \mathbb{C}$, which is an integral domain, we must have, say, $p(\alpha) = 0$. But then $\deg p < \deg f_\alpha$, so $p \notin I = (f_\alpha)$. Contradiction. □

Lemma. Let $\alpha \in \mathbb{Q}$ be an algebraic integer. Then $\alpha \in \mathbb{Z}$.

Proof. Let $f_\alpha \in \mathbb{Z}[X]$ be the minimal polynomial, which is irreducible. In $\mathbb{Q}[X]$, the polynomial $X - \alpha$ must divide f_α. However, by Gauss' lemma, we know $f \in \mathbb{Q}[X]$ is irreducible. So we must have $f_\alpha = X - \alpha \in \mathbb{Z}[X]$. So α is an integer. □

2.8 Noetherian rings

Proposition. A ring is Noetherian if and only if every ideal is finitely generated.

Proof. We start with the easier direction — from concrete to abstract.

Suppose every ideal of R is finitely generated. Given the chain $I_1 \subseteq I_2 \subseteq \cdots$, consider the ideal

$$I = I_1 \cup I_2 \cup I_3 \cup \cdots.$$

This is obviously an ideal, and you will check this manually in example sheet 2.

We know I is finitely generated, say $I = (r_1, \cdots, r_n)$, with $r_i \in I_{k_i}$. Let

$$K = \max_{i=1,\cdots,n} \{k_i\}.$$

Then $r_1, \cdots, r_n \in I_K$. So $I_K = I$. So $I_K = I_{K+1} = I_{K+2} = \cdots$.

To prove the other direction, suppose there is an ideal $I \lhd R$ that is not finitely generated. We pick $r_1 \in I$. Since I is not finitely generated, we know $(r_1) \neq I$. So we can find some $r_2 \in I \setminus (r_1)$.

Again $(r_1, r_2) \neq I$. So we can find $r_3 \in I \setminus (r_1, r_2)$. We continue on, and then can find an infinite strictly ascending chain

$$(r_1) \subseteq (r_1, r_2) \subseteq (r_1, r_2, r_3) \subseteq \cdots.$$

So R is not Noetherian. □

Proposition. Let R be a Noetherian ring and I be an ideal of R. Then R/I is Noetherian.

Proof. Whenever we see quotients, we should think of them as the image of a homomorphism. Consider the quotient map

$$\begin{aligned}\pi : R &\to R/I\\ x &\mapsto x + I.\end{aligned}$$

We can prove this result by finitely generated or ascending chain condition. We go for the former. Let $J \lhd R/I$ be an ideal. We want to show that J is finitely generated. Consider the inverse image $\pi^{-1}(J)$. This is an ideal of R, and is hence finitely generated, since R is Noetherian. So $\pi^{-1}(J) = (r_1, \cdots, r_n)$ for some $r_1, \cdots, r_n \in R$. Then J is generated by $\pi(r_1), \cdots, \pi(r_n)$. So done. □

Theorem (Hilbert basis theorem)**.** Let R be a Noetherian ring. Then so is $R[X]$.

Proof. The proof is not too hard, but we will need to use *both* the ascending chain condition and the fact that all ideals are finitely-generated.

Let $I \lhd R[X]$ be an ideal. We want to show it is finitely generated. Since we know R is Noetherian, we want to generate some ideals of R from I.

How can we do this? We can do the silly thing of taking all constants of I, i.e. $I \cap R$. But we can do better. We can consider all linear polynomials, and take their leading coefficients. Thinking for a while, this is indeed an ideal.

In general, for $n = 0, 1, 2, \cdots$, we let

$$I_n = \{r \in R : \text{there is some } f \in I \text{ such that } f = rX^n + \cdots\} \cup \{0\}.$$

Then it is easy to see, using the strong closure property, that each ideal I_n is an ideal of R. Moreover, they form a chain, since if $f \in I$, then $Xf \in I$, by strong closure. So $I_n \subseteq I_{n+1}$ for all n.

By the ascending chain condition of R, we know there is some N such that $I_N = I_{N+1} = \cdots$. Now for each $0 \leq n \leq N$, since R is Noetherian, we can write

$$I_n = (r_1^{(n)}, r_2^{(n)}, \cdots, r_{k(n)}^{(n)}).$$

Now for each $r_i^{(n)}$, we choose some $f_i^{(n)} \in I$ with $f_i^{(n)} = r_i^{(n)} X^n + \cdots$.

We now claim the polynomials $f_i^{(n)}$ for $0 \leq n \leq N$ and $1 \leq i \leq k(n)$ generate I.

Suppose not. We pick $g \in I$ of minimal degree not generated by the $f_i^{(n)}$.

There are two possible cases. If $\deg g = n \leq N$, suppose

$$g = rX^n + \cdots.$$

We know $r \in I_n$. So we can write

$$r = \sum_i \lambda_i r_i^{(n)}$$

for some $\lambda_i \in R$, since that's what generating an ideal means. Then we know

$$\sum_i \lambda_i f_i^{(n)} = rX^n + \cdots \in I.$$

But if g is not in the span of the $f_i^{(j)}$, then so isn't $g - \sum_i \lambda_i f_i^{(n)}$. But this has a lower degree than g. This is a contradiction.

Now suppose $\deg g = n > N$. This might look scary, but it is not, since $I_n = I_N$. So we write the same proof. We write

$$g = rX^n + \cdots .$$

But we know $r \in I_n = I_N$. So we know

$$r = \sum_I \lambda_i r_i^{(N)}.$$

Then we know

$$X^{n-N} \sum_i \lambda_i f_i^{(n)} = rX^N + \cdots \in I.$$

Hence $g - X^{n-N} \sum \lambda_i f_i^{(N)}$ has smaller degree than g, but is not in the span of $f_i^{(j)}$. □

3 Modules

3.1 Definitions and examples

Theorem (First isomorphism theorem)**.** Let $f : M \to N$ be an R-module homomorphism. Then

$$\ker f = \{m \in M : f(m) = 0\} \leq M$$

is an R-submodule of M. Similarly,

$$\operatorname{im} f = \{f(m) : m \in M\} \leq N$$

is an R-submodule of N. Then

$$\frac{M}{\ker f} \cong \operatorname{im} f.$$

Theorem (Second isomorphism theorem)**.** Let $A, B \leq M$. Then

$$A + B = \{m \in M : m = a + b \text{ for some } a \in A, b \in B\} \leq M,$$

and

$$A \cap B \leq M.$$

We then have

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

Theorem (Third isomorphism theorem)**.** Let $N \leq L \leq M$. Then we have

$$\frac{M}{L} \cong \left(\frac{M}{N}\right) / \left(\frac{L}{N}\right).$$

Lemma. An R-module M is finitely-generated if and only if there is a surjective R-module homomorphism $f : R^k \twoheadrightarrow M$ for some finite k.

Proof. If

$$M = Rm_1 + Rm_2 + \cdots + Rm_k,$$

we define $f : R^k \to M$ by

$$(r_1, \cdots, r_k) \mapsto r_1 m_1 + \cdots + r_k m_k.$$

It is clear that this is an R-module homomorphism. This is by definition surjective. So done.

Conversely, given a surjection $f : R^k \twoheadrightarrow M$, we let

$$m_i = f(0, 0, \cdots, 0, 1, 0, \cdots, 0),$$

where the 1 appears in the ith position. We now claim that

$$M = Rm_1 + Rm_2 + \cdots + Rm_k.$$

So let $m \in M$. As f is surjective, we know

$$m = f(r_1, r_2, \cdots, r_k)$$

for some r_i. We then have

$$\begin{aligned} & f(r_1, r_2, \cdots, r_k) \\ &= f((r_1, 0, \cdots, 0) + (0, r_2, 0, \cdots, 0) + \cdots + (0, 0, \cdots, 0, r_k)) \\ &= f(r_1, 0, \cdots, 0) + f(0, r_2, 0, \cdots, 0) + \cdots + f(0, 0, \cdots, 0, r_k) \\ &= r_1 f(1, 0, \cdots, 0) + r_2 f(0, 1, 0, \cdots, 0) + \cdots + r_k f(0, 0, \cdots, 0, 1) \\ &= r_1 m_1 + r_2 m_2 + \cdots + r_k m_k. \end{aligned}$$

So the m_i generate M. □

Corollary. Let $N \leq M$ and M be finitely-generated. Then M/N is also finitely generated.

Proof. Since m is finitely generated, we have some surjection $f : R^k \twoheadrightarrow M$. Moreover, we have the surjective quotient map $q : M \twoheadrightarrow M/N$. Then we get the following composition

$$R^k \xrightarrow{f} M \xrightarrow{q} M/N,$$

which is a surjection, since it is a composition of surjections. So M/N is finitely generated. □

3.2 Direct sums and free modules

Proposition. For a subset $S = \{m_1, \cdots, m_k\} \subseteq M$, the following are equivalent:

(i) S generates M freely.

(ii) S generates M and the set S is independent.

(iii) Every element of M is *uniquely* expressible as

$$r_1 m_1 + r_2 m_2 + \cdots + r_k m_k$$

for some $r_i \in R$.

Proof. The fact that (ii) and (iii) are equivalent is something we would expect from what we know from linear algebra, and in fact the proof is the same. So we only show that (i) and (ii) are equivalent.

Let S generate M freely. If S is not independent, then we can write

$$r_1 m_1 + \cdots + r_k m_k = 0,$$

with $r_i \in M$ and, say, r_1 non-zero. We define the set function $\psi : S \to R$ by sending $m_1 \mapsto 1_R$ and $m_i \mapsto 0$ for all $i \neq 1$. As S generates M freely, this extends to an R-module homomorphism $\theta : M \to R$.

By definition of a homomorphism, we can compute

$$\begin{aligned} 0 &= \theta(0) \\ &= \theta(r_1 m_1 + r_2 m_2 + \cdots + r_k m_k) \\ &= r_1 \theta(m_1) + r_2 \theta(m_2) + \cdots + r_k \theta(m_k) \\ &= r_1. \end{aligned}$$

This is a contradiction. So S must be independent.

To prove the other direction, suppose every element can be uniquely written as $r_1m_1 + \cdots + r_km_k$. Given any set function $\psi : S \to N$, we define $\theta : M \to N$ by

$$\theta(r_1m_1 + \cdots + r_km_k) = r_1\psi(m_1) + \cdots + r_k\psi(m_k).$$

This is well-defined by uniqueness, and is clearly a homomorphism. So it follows that S generates M freely. □

Proposition (Invariance of dimension/rank)**.** Let R be a non-zero ring. If $R^n \cong R^m$ as R-modules, then $n = m$.

Proposition. If $I \lhd R$ is an ideal and M is an R-module, then M/IM is an R/I module in a natural way.

Proposition. Every non-zero ring has a maximal ideal.

Proof. We observe that an ideal $I \lhd R$ is proper if and only if $1_R \notin I$. So every increasing union of proper ideals is proper. Then by *Zorn's lemma*, there is a maximal ideal (Zorn's lemma says if an arbitrary union of increasing things is still a thing, then there is a maximal such thing, roughly). □

Proposition (Invariance of dimension/rank)**.** Let R be a non-zero ring. If $R^n \cong R^m$ as R-modules, then $n = m$.

Proof. Let I be a maximal ideal of R. Suppose we have $R^n \cong R^m$. Then we must have

$$\frac{R^n}{IR^n} \cong \frac{R^m}{IR^m},$$

as R/I modules.

But staring at it long enough, we figure that

$$\frac{R^n}{IR^n} \cong \left(\frac{R}{I}\right)^n,$$

and similarly for m. Since R/I is a field, the result follows by linear algebra. □

3.3 Matrices over Euclidean domains

Theorem (Smith normal form)**.** An $m \times n$ matrix over a Euclidean domain R is equivalent to a diagonal matrix

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

with the d_i all non-zero and

$$d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_r.$$

Proof. Throughout the process, we will keep calling our matrix A, even though it keeps changing in each step, so that we don't have to invent hundreds of names for these matrices.

If $A = 0$, then done! So suppose $A \neq 0$. So some entry is not zero, say, $A_{ij} \neq 0$. Swapping the ith and first row, then jth and first column, we arrange that $A_{11} \neq 0$. We now try to reduce A_{11} as much as possible. We have the following two possible moves:

(i) If there is an A_{1j} not divisible by A_{11}, then we can use the Euclidean algorithm to write
$$A_{1j} = qA_{11} + r.$$
By assumption, $r \neq 0$. So $\phi(r) < \phi(A_{11})$ (where ϕ is the Euclidean function).

So we subtract q copies of the first column from the jth column. Then in position $(1, j)$, we now have r. We swap the first and jth column such that r is in position $(1, 1)$, and we have strictly reduced the value of ϕ at the first entry.

(ii) If there is an A_{i1} not divisible by A_{11}, we do the same thing, and this again reduces $\phi(A_{11})$.

We keep performing these until no move is possible. Since the value of $\phi(A_{11})$ strictly decreases every move, we stop after finitely many applications. Then we know that we must have A_{11} dividing all A_{ij} and A_{i1}. Now we can just subtract appropriate multiples of the first column from others so that $A_{1j} = 0$ for $j \neq 1$. We do the same thing with rows so that the first row is cleared. Then we have a matrix of the form
$$A = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix}.$$
We would like to say "do the same thing with C", but then this would get us a regular diagonal matrix, not necessarily in Smith normal form. So we need some preparation.

(iii) Suppose there is an entry of C not divisible by d, say A_{ij} with $i, j > 1$.
$$A = \begin{pmatrix} d & 0 & \cdots & 0 & \cdots & 0 \\ 0 & & & & & \\ \vdots & & & & & \\ 0 & & & A_{ij} & & \\ \vdots & & & & & \\ 0 & & & & & \end{pmatrix}$$
We suppose
$$A_{ij} = qd + r,$$
with $r \neq 0$ and $\phi(r) < \phi(d)$. We add column 1 to column j, and subtract q times row 1 from row i. Now we get r in the (i, j)th entry, and we want

to send it back to the $(1,1)$ position. We swap row i with row 1, swap column j with row 1, so that r is in the $(1,1)$th entry, and $\phi(r) < \phi(d)$.

Now we have messed up the first row and column. So we go back and do (i) and (ii) again until the first row and columns are cleared. Then we get

$$A = \begin{pmatrix} d' & 0 & \cdots & 0 \\ 0 & & & \\ 0 & & C' & \\ 0 & & & \end{pmatrix},$$

where

$$\phi(d') \leq \phi(r) < \phi(d).$$

As this strictly decreases the value of $\phi(A_{11})$, we can only repeat this finitely many times. When we stop, we will end up with a matrix

$$A = \begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix},$$

and d divides *every* entry of C. Now we apply the entire process to C. When we do this process, notice all allowed operations don't change the fact that d divides every entry of C.

So applying this recursively, we obtain a diagonal matrix with the claimed divisibility property. □

Lemma. Let A and B be equivalent matrices. Then

$$\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$$

for all k.

Proof. It suffices to show that changing A by a row or column operation does not change the Fitting ideal. Since taking the transpose does not change the determinant, i.e. $\mathrm{Fit}_k(A) = \mathrm{Fit}_k(A^T)$, it suffices to consider the row operations.

The most difficult one is taking linear combinations. Let B be the result of adding c times the ith row to the jth row, and fix C a $k \times k$ minor of A. Suppose the resultant matrix is C'. We then want to show that $\det C' \in \mathrm{Fit}_k(A)$.

If the jth row is outside of C, then the minor $\det C$ is unchanged. If both the ith and jth rows are in C, then the submatrix C changes by a row operation, which does not affect the determinant. These are the boring cases.

Suppose the jth row is in C and the ith row is not. Suppose the ith row is $f_1, \cdots, f_k$. Then C is changed to C', with the jth row being

$$(C_{j1} + cf_1, C_{j_2} + cf_2, \cdots, C_{jk} + cf_k).$$

We compute $\det C'$ by expanding along this row. Then we get

$$\det C' = \det C + c \det D,$$

where D is the matrix obtained by replacing the jth row of C with $(f_1, \cdots, f_k)$.

The point is that $\det C$ is definitely a minor of A, and $\det D$ is still a minor of A, just another one. Since ideals are closed under addition and multiplications, we know

$$\det(C') \in \mathrm{Fit}_k(A).$$

The other operations are much simpler. They just follow by standard properties of the effect of swapping rows or multiplying rows on determinants. So after any row operation, the resultant submatrix C' satisfies

$$\det(C') \in \mathrm{Fit}_k(A).$$

Since this is true for all minors, we must have

$$\mathrm{Fit}_k(B) \subseteq \mathrm{Fit}_k(A).$$

But row operations are invertible. So we must have

$$\mathrm{Fit}_k(A) \subseteq \mathrm{Fit}_k(B)$$

as well. So they must be equal. So done. □

Corollary. If A has Smith normal form

$$B = \begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix},$$

then

$$\mathrm{Fit}_k(A) = (d_1 d_2 \cdots d_k).$$

So d_k is unique up to associates.

Lemma. Let R be a principal ideal domain. Then any submodule of R^m is generated by at most m elements.

Proof. Let $N \leq R^m$ be a submodule. Consider the ideal

$$I = \{r \in R : (r, r_2, \cdots, r_m) \in N \text{ for some } r_2, \cdots, r_m \in R\}.$$

It is clear this is an ideal. Since R is a principle ideal domain, we must have $I = (a)$ for some $a \in R$. We now choose an

$$n = (a, a_2, \cdots, a_m) \in N.$$

Then for any vector $(r_1, r_2, \cdots, r_m) \in N$, we know that $r_1 \in I$. So $a \mid r_1$. So we can write

$$r_1 = ra.$$

Then we can form

$$(r_1, r_2, \cdots, r_m) - r(a, a_2, \cdots, a_m) = (0, r_2 - ra_2, \cdots, r_m - ra_m) \in N.$$

This lies in $N' = N \cap (\{0\} \times R^{m-1}) \leq R^{m-1}$. Thus everything in N can be written as a multiple of n plus something in N'. But by induction, since $N' \leq R^{m-1}$, we know N' is generated by at most $m-1$ elements. So there are $n_2, \cdots, n_m \in N'$ generating N'. So $n, n_2, \cdots, n_m$ generate N. □

Theorem. Let R be a Euclidean domain, and let $N \leq R^m$ be a submodule. Then there exists a basis $v_1, \cdots, v_m$ of R^m such that N is generated by $d_1 v_1, d_2 v_2, \cdots, d_r v_r$ for some $0 \leq r \leq m$ and some $d_i \in R$ such that

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Proof. By the previous lemma, N is generated by some elements $x_1, \cdots, x_n$ with $n \leq m$. Each x_i is an element of R^m. So we can think of it as a column vector of length m, and we can form a matrix

$$A = \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ x_1 & x_2 & \cdots & x_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}.$$

We've got an $m \times n$ matrix. So we can put it in Smith normal form! Since there are fewer columns than there are rows, this is of the form

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \\ & & & & & & 0 \\ & & & & & & \vdots \\ & & & & & & 0 \end{pmatrix}$$

Recall that we got to the Smith normal form by row and column operations. Performing row operations is just changing the basis of R^m, while each column operation changes the generators of N.

So what this tells us is that there is a new basis $v_1, \cdots, v_m$ of R^m such that N is generated by $d_1 v_1, \cdots, d_r v_r$. By definition of Smith normal form, the divisibility condition holds. □

Corollary. Let R be a Euclidean domain. A submodule of R^m is free of rank at most m. In other words, the submodule of a free module is free, and of a smaller (or equal) rank.

Proof. Let $N \leq R^m$ be a submodule. By the above, there is a basis $v_1, \cdots, v_n$ of R^m such that N is generated by $d_1 v_1, \cdots, d_r v_r$ for $r \leq m$. So it is certainly generated by at most m elements. So we only have to show that $d_1 v_1, \cdots, d_r v_r$ are independent. But if they were linearly dependent, then so would be $v_1, \cdots, v_m$. But $v_1, \cdots, v_n$ are a basis, hence independent. So $d_1 v_1, \cdots, d_r v_r$ generate N *freely*. So

$$N \cong R^r.$$

□

Theorem (Classification of finitely-generated modules over a Euclidean domain)**.** Let R be a Euclidean domain, and M be a finitely generated R-module. Then

$$M \cong \frac{R}{(d_1)} \oplus \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus R \oplus \cdots \oplus R$$

for some $d_i \neq 0$, and

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Proof. Since M is finitely-generated, there is a surjection $\phi : R^m \to M$. So by the first isomorphism, we have

$$M \cong \frac{R^m}{\ker \phi}.$$

Since $\ker \phi$ is a submodule of R^m, by the previous theorem, there is a basis $v_1, \cdots, v_m$ of R^m such that $\ker \phi$ is generated by $d_1 v_1, \cdots, d_r v_r$ for $0 \leq r \leq m$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. So we know

$$M \cong \frac{R^m}{((d_1, 0, \cdots, 0), (0, d_2, 0, \cdots, 0), \cdots, (0, \cdots, 0, d_r, 0, \cdots, 0))}.$$

This is just

$$\frac{R}{(d_1)} \oplus \frac{R}{(d_2)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus \cdots \oplus R,$$

with $m - r$ copies of R. □

Corollary (Classification of finitely-generated abelian groups)**.** Any finitely-generated abelian group is isomorphic to

$$C_{d_1} \times \cdots \times C_{d_r} \times C_\infty \times \cdots \times C_\infty,$$

where $C_\infty \cong \mathbb{Z}$ is the infinite cyclic group, with

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Proof. Let $R = \mathbb{Z}$, and apply the classification of finitely generated R-modules. □

Corollary. If A is a finite abelian group, then

$$A \cong C_{d_1} \times \cdots \times C_{d_r},$$

with

$$d_1 \mid d_2 \mid \cdots \mid d_r.$$

Lemma (Chinese remainder theorem)**.** Let R be a Euclidean domain, and $a, b \in R$ be such that $\gcd(a, b) = 1$. Then

$$\frac{R}{(ab)} \cong \frac{R}{(a)} \times \frac{R}{(b)}$$

as R-modules.

Proof. Consider the R-module homomorphism

$$\phi : \frac{R}{(a)} \times \frac{R}{(b)} \to \frac{R}{(ab)}$$

by

$$(r_1 + (a), r_2 + (b)) \mapsto br_1 + ar_2 + (ab).$$

To show this is well-defined, suppose

$$(r_1 + (a), r_2 + (b)) = (r_1' + (a), r_2' + (b)).$$

Then

$$\begin{aligned} r_1 &= r_1' + xa \\ r_2 &= r_2' + yb. \end{aligned}$$

So

$$br_1 + ar_2 + (ab) = br_1' + xab + ar_2' + yab + (ab) = br_1' + ar_2' + (ab).$$

So this is indeed well-defined. It is clear that this is a module map, by inspection.

We now have to show it is surjective and injective. So far, we have not used the hypothesis, that $\gcd(a, b) = 1$. As we know $\gcd(a, b) = 1$, by the Euclidean algorithm, we can write

$$1 = ax + by$$

for some $x, y \in R$. So we have

$$\phi(y + (a), x + (b)) = by + ax + (ab) = 1 + (ab).$$

So $1 \in \operatorname{im} \phi$. Since this is an R-module map, we get

$$\phi(r(y + (a), x + (b))) = r \cdot (1 + (ab)) = r + (ab).$$

The key fact is that $R/(ab)$ as an R-module is generated by 1. Thus we know ϕ is surjective.

Finally, we have to show it is injective, i.e. that the kernel is trivial. Suppose

$$\phi(r_1 + (a), r_2 + (b)) = 0 + (ab).$$

Then

$$br_1 + ar_2 \in (ab).$$

So we can write

$$br_1 + ar_2 = abx$$

for some $x \in R$. Since $a \mid ar_2$ and $a \mid abx$, we know $a \mid br_1$. Since a and b are coprime, unique factorization implies $a \mid r_1$. Similarly, we know $b \mid r_2$.

$$(r_1 + (a), r_2 + (b)) = (0 + (a), 0 + (b)).$$

So the kernel is trivial. □

Theorem (Prime decomposition theorem)**.** Let R be a Euclidean domain, and M be a finitely-generated R-module. Then

$$M \cong N_1 \oplus N_2 \oplus \cdots \oplus N_t,$$

where each N_i is either R or is $R/(p^n)$ for some prime $p \in R$ and some $n \geq 1$.

Proof. We already know

$$M \cong \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus \cdots \oplus R.$$

So it suffices to show that each $R/(d_1)$ can be written in that form. We let

$$d = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

with p_i distinct primes. So each $p_i^{n_i}$ is coprime to each other. So by the lemma iterated, we have

$$\frac{R}{(d_1)} \cong \frac{R}{(p_1^{n_1})} \oplus \cdots \oplus \frac{R}{(p_k^{n_k})}.$$ □

3.4 Modules over $\mathbb{F}[X]$ and normal forms for matrices

Lemma. If V is a finite-dimensional vector space, then V_α is a finitely-generated $\mathbb{F}[X]$-module.

Proof. If $\mathbf{v}_1, \cdots, \mathbf{v}_n$ generate V as an $\mathbb{F}$-module, i.e. they span V as a vector space over $\mathbb{F}$, then they also generate V_α as an $\mathbb{F}[X]$-module, since $\mathbb{F} \leq \mathbb{F}[X]$. □

Theorem (Rational canonical form)**.** Let $\alpha : V \to V$ be a linear endomorphism of a finite-dimensional vector space over $\mathbb{F}$, and V_α be the associated $\mathbb{F}[X]$-module. Then

$$V_\alpha \cong \frac{\mathbb{F}[X]}{(f_1)} \oplus \frac{\mathbb{F}[X]}{(f_2)} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{(f_s)},$$

with $f_1 \mid f_2 \mid \cdots \mid f_s$. Thus there is a basis for V in which the matrix for α is the block diagonal

$$\begin{pmatrix} c(f_1) & 0 & \cdots & 0 \\ 0 & c(f_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c(f_s) \end{pmatrix}$$

Proof. We already know that V_α is a finitely-generated $\mathbb{F}[X]$-module. By the structure theorem of $\mathbb{F}[X]$-modules, we know

$$V_\alpha \cong \frac{\mathbb{F}[X]}{(f_1)} \oplus \frac{\mathbb{F}[X]}{(f_2)} \oplus \cdots \oplus \frac{\mathbb{F}[X]}{(f_s)} \oplus 0.$$

We know there are no copies of $\mathbb{F}[X]$, since $V_\alpha = V$ is finite-dimensional over $\mathbb{F}$, but $\mathbb{F}[X]$ is not. The divisibility criterion also follows from the structure theorem. Then the form of the matrix is immediate. □

Lemma. The prime elements of $\mathbb{C}[X]$ are the $X - \lambda$ for $\lambda \in \mathbb{C}$ (up to multiplication by units).

Proof. Let $f \in \mathbb{C}[X]$. If f is constant, then it is either a unit or 0. Otherwise, by the fundamental theorem of algebra, it has a root λ. So it is divisible by $X - \lambda$. So if f is irreducible, it must have degree 1. And clearly everything of degree 1 is prime. □

Theorem (Jordan normal form)**.** Let $\alpha : V \to V$ be an endomorphism of a vector space V over $\mathbb{C}$, and V_α be the associated $\mathbb{C}[X]$-module. Then

$$V_\alpha \cong \frac{\mathbb{C}[X]}{((X-\lambda_1)^{a_1})} \oplus \frac{\mathbb{C}[X]}{((X-\lambda_2)^{a_2})} \oplus \cdots \oplus \frac{\mathbb{C}[X]}{((X-\lambda_t)^{a_t})},$$

where $\lambda_i \in \mathbb{C}$ do *not* have to be distinct. So there is a basis of V in which α has matrix

$$\begin{pmatrix} J_{a_1}(\lambda_1) & & & 0 \\ & J_{a_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{a_t}(\lambda_t) \end{pmatrix},$$

where

$$J_m(\lambda) = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}$$

is an $m \times m$ matrix.

Proof. Apply the prime decomposition theorem to V_α. Then all primes are of the form $X - \lambda$. We then use our second example at the beginning of the chapter to get the form of the matrix. □

Theorem (Cayley-Hamilton theorem)**.** Let M be a finitely-generated R-module, where R is some commutative ring. Let $\alpha : M \to M$ be an R-module homomorphism. Let A be a matrix representation of α under some choice of generators, and let $p(t) = \det(tI - A)$. Then $p(\alpha) = 0$.

Proof. We consider M as an $R[X]$-module with action given by

$$(f(X))(m) = f(\alpha)m.$$

Suppose $e_1, \cdots, e_n$ span M, and that for all i, we have

$$\alpha(e_i) = \sum_{j=1}^{n} a_{ij} e_j.$$

Then

$$\sum_{j=1}^{n} (X\delta_{ij} - a_{ij}) e_j = 0.$$

We write C for the matrix with entries

$$c_{ij} = X\delta_{ij} - a_{ij} \in \mathbb{F}[X].$$

We now use the fact that

$$\mathrm{adj}(C)C = \det(C)I,$$

which we proved in IB Linear Algebra (and the proof did not assume that the underlying ring is a field). Expanding this out, we get the following equation (in $\mathbb{F}[X]$).

$$\chi_\alpha(X)I = \det(XI - A)I = (\mathrm{adj}(XI - A))(XI - A).$$

Writing this in components, and multiplying by e_k, we have

$$\chi_\alpha(X)\delta_{ik}e_k = \sum_{j=1}^{n}(\mathrm{adj}(XI - A)_{ij})(X\delta_{jk} - a_{jk})e_k.$$

Then for each i, we sum over k to obtain

$$\sum_{k=1}^{n}\chi_\alpha(X)\delta_{ik}e_k = \sum_{j,k=1}^{n}(\mathrm{adj}(XI - A)_{ij})(X\delta_{jk} - a_{jk})e_k = 0,$$

by our choice of a_{ij}. But the left hand side is just $\chi_\alpha(X)e_i$. So $\chi_\alpha(X)$ acts trivially on all of the generators e_i. So it in fact acts trivially. So $\chi_\alpha(\alpha)$ is the zero map (since acting by X is the same as acting by α, by construction). □

3.5 Conjugacy of matrices*

Lemma. Let $\alpha, \beta : V \to V$ be two linear maps. Then $V_\alpha \cong V_\beta$ as $\mathbb{F}[X]$-modules if and only if α and β are conjugate as linear maps, i.e. there is some $\gamma : V \to V$ such that $\alpha = \gamma^{-1}\beta\gamma = \alpha$.

Proof. Let $\gamma : V_\beta \to V_\alpha$ be an $\mathbb{F}[X]$-module isomorphism. Then for $\mathbf{v} \in V$, we notice that if $\beta(\mathbf{v})$ is just $X \cdot \mathbf{v}$ in V_β, and $\alpha(\mathbf{v})$ is just $X \cdot \mathbf{v}$ in V_α. So we get

$$\beta \circ \gamma(\mathbf{v}) = X \cdot (\gamma(\mathbf{v})) = \gamma(X \cdot \mathbf{v}) = \gamma \circ \alpha(\mathbf{v}),$$

using the definition of an $\mathbb{F}[X]$-module homomorphism.

So we know

$$\beta\gamma = \gamma\alpha.$$

So

$$\alpha = \gamma^{-1}\beta\gamma.$$

Conversely, let $\gamma : V \to V$ be a linear isomorphism such that $\gamma^{-1}\beta\gamma = \alpha$. We now claim that $\gamma : V_\alpha \to V_\beta$ is an $\mathbb{F}[X]$-module map. We just have to check that

$$\begin{aligned}
\gamma(f \cdot \mathbf{v}) &= \gamma(f(\alpha)(\mathbf{v})) \\
&= \gamma(a_0 + a_1\alpha + \cdots + a_n\alpha^n)(\mathbf{v}) \\
&= \gamma(a_0\mathbf{v}) + \gamma(a_1\alpha(\mathbf{v})) + \gamma(a_2\alpha^2(\mathbf{v})) + \cdots + \gamma(a_n\alpha^n(\mathbf{v})) \\
&= (a_0 + a_1\beta + a_2\beta^2 + \cdots + a_n\beta^n)(\gamma(\mathbf{v})) \\
&= f \cdot \gamma(\mathbf{v}).
\end{aligned}$$

□

Corollary. There is a bijection between conjugacy classes of $n \times n$ matrices over $\mathbb{F}$ and sequences of monic polynomials $d_1, \cdots, d_r$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$ and $\deg(d_1, \cdots, d_r) = n$.