

Groups, Rings, and Modules

Notes made by Finley Cooper

7th September 2025

Contents

1	Review of IA Groups	3
1.1	Definitions	3
1.2	Cosets	4
1.3	Normal subgroups	4
1.4	Groups actions and permutations	8
1.5	Conjugacy, centralisers, and normalisers	10
1.6	Simplicity of A_n for $n \geq 5$	10
1.7	Finite p -groups	11
1.8	Finite abelian groups	12
1.9	Sylow Theorems	13
2	Rings	15
2.1	Definitions and examples	15
2.2	Homomorphisms, ideals, and quotients	16
2.3	Integral domains	20
2.4	Factorisation in integral domains	22
2.5	Factorisation in polynomial rings	26
2.6	Gaussian integers	29
2.7	Algebraic integers	31
2.8	Hilbert's basis theorem	32
3	Modules	34
3.1	Definitions and examples	34
3.2	Direct sums and free modules	37
3.3	Matrices over Euclidean domains	39
3.4	Modules over \mathbb{F} and forms of matrices	44

1 Review of IA Groups

1.1 Definitions

We'll start with some simple definitions covered in IA Groups

Definition. A group is a *triple*, (G, \circ, e) consisting of a set G , a binary operation $\circ : G \times G \rightarrow G$ and an identity element $e \in G$ where we have the following three properties,

- (i) $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$
- (ii) $\forall a \in G, a \circ e = e \circ a = a$
- (iii) $\forall a \in G, \exists a^{-1} \in G, a \circ a^{-1} = a^{-1} \circ a = e$

We say that the *order* of the group (G, \circ, e) is the size of the set G

Proposition. Inverses are unique.

Proof. Basic algebraic manipulation, covered in Part IA Groups.

Definition. If G is a group, then a subset $H \subseteq G$ is a *subgroup* if the following hold,

- (i) $e \in H$
- (ii) If $a, b \in H$ then $a \circ b \in H$
- (iii) (H, \circ, e) forms a group.

Now we'll give simple test for a subset being a subgroup

Lemma. A non-empty subset, H , of a group G is a subgroup if and only if $\forall h_1, h_2 \in H$ we have that $h_1 h_2^{-1} \in H$

Proof. Again covered in Part IA Groups

Definition. A group G is abelian if $\forall g_1, g_2 \in G$ we have that $g_1 g_2 = g_2 g_1$

Let's look at some examples of groups.

- (i) The integers under addition, $(\mathbb{Z}, +)$
- (ii) The integers modulo n under addition $(\mathbb{Z}_n, +_n)$
- (iii) The rational numbers under addition $(\mathbb{Q}, +)$
- (iv) The set of all bijections from $\{1, \dots, n\}$ to itself with the operation given by functional composition, S_n
- (v) The set of all bijections from a set X to itself under functional composition is a group $\text{Sym}(X)$
- (vi) The dihedral group, D_{2n} the set of symmetries of the regular n -gon
- (vii) The general linear group over \mathbb{R} , $\text{GL}(n, \mathbb{R})$, is the set of functions from $\mathbb{R} \rightarrow \mathbb{R}$ which are linear and invertible. Or we can think of the group as the set of $n \times n$ invertible matrices under matrix multiplication. We can view this group as a subgroup of $\text{Sym}(\mathbb{R}^n)$

- (viii) The subgroup of S_n which are even permutations, so can be written as a product of evenly many transpositions, A_n
- (ix) The subgroup of D_{2n} which are only the rotation symmetries which is denoted by C_n
- (x) The subgroup of $GL(n, \mathbb{R})$ of matrices which have determinant 1 which is $SL(n, \mathbb{R})$
- (xi) The Klein four-group, which is $K_4 = C_2 \times C_2$, the symmetries of the non-square rectangle
- (xii) The quaternions, Q_8 with the elements $\{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication defined with $ij = k, ji = -k, i^2 = j^2 = k^2 = -1$

1.2 Cosets

Definition. Let G be a group and $g \in G$. Let H be a subgroup of G . The *left coset*, written as gH is the set $\{gh : h \in H\}$

Some observations we can make are,

- (i) Since $e \in H$ we have that $g \in gH$. So every element is in some coset
- (ii) The cosets partition, so if $gH \cap g'H \neq \emptyset$ then $gH = g'H$
- (iii) The function, $f : H \rightarrow gH$ defined by $f(h) = gh$ is a bijection, so all cosets are the same size

Theorem. (Lagrange's Theorem) If G is a finite group, then for a subgroup H of G , $|G| = |H||G : H|$, where $|G : H|$ is the number of left cosets of H in G

Proof. Obvious from the observations we've just made.

Definition. Let G be a group, and take some element $g \in G$. We define the *order* of g as the smallest positive integer n , such that $g^n = e$. If no such n exists, we say the order of g is infinite. We denote the order by $\text{ord}(g)$.

Proposition. Let G be a group and $g \in G$. Then $\text{ord}(g)$ divides $|G|$

Proof. Let $g \in G$. Consider the subset, $H = \{e, g, g^2, \dots, g^{n-1}\}$ where n is the order of g . We claim H is a subgroup. $e \in H$ so H is non-empty. Observe that $g^r g^{-s} = g^{r-s} \in H$ so we have that $H \leq G$. Elements are distinct since if $g_i = g_j, i \neq j, 0 \leq i < j < n$ then $gj - i = e$ which contradicts the minimality of n since $0 \leq j - i \leq n$. We have that $|H| = n$, so by Lagrange, $|H|$ divides $|G|$. \square

1.3 Normal subgroups

When does $gH = g'H$? Then $g \in g'H$, so we have that $g'^{-1}g \in H$. The converse also holds.

Lemma. For a group G with $g, g' \in G$ and subgroup H we have that $gH = g'H$ if and only if $g'^{-1}g \in H$

Proof. In Part IA Groups

Let $G/H = \{gH : g \in G\}$ be the set of left cosets. This partitions G . Does G/H have a natural group structure?

We propose the formula that $g_1H \cdot g_2H = (g_1g_2) \cdot H$ for a group law on G/H .

We need to check well definedness of this proposed formula. *Case 1:* Suppose that $g_2H = g'_2H$. Then $g'_2 = g_2h$ for some $h \in H$. $(g_1H) \cdot (g'_2H) = g_1g'_2H$ by the proposed formula. By the previous relation this is $g_1g_2hH = g_1g_2H$.

Case 2: Suppose that $g_1H = g'_1H$ we have that $g'_1 = g_1h$ for some $h \in H$. We need $g_1g_2H = \underbrace{g_1h}_{g'_1}g_2H$. Equivalently we need that $(g_1g_2)^{-1}g_1hg_2 \in H$. Or equivalently still, $g_2^{-1}hg_2 \in H$ for all g_2 and h . This is the definition of normality.

Definition. (Normality) A subgroup $H \leq G$ is *normal* if $\forall g \in G, h \in H$, we have that $ghg^{-1} \in H$

If $H \leq G$ is normal we write that $H \triangleleft G$.

Definition. (Quotient) Let $H \triangleleft G$. The *quotient group* is the set $(G/H, \cdot, e = eH)$ where $\cdot : G/H \times G/H \rightarrow G/H$ by $(g_1H, g_2H) \rightarrow (g_1g_2)H$.

Definition. (Homomorphism) Let G and H be groups. A *homomorphism* is a function $f : G \rightarrow H$ such that for all $g_1, g_2 \in G$ we have that $f(g_1g_2) = f(g_1)f(g_2)$

This is a very constrained condition. For example $f(e_G) = e_H$ always. To see this, observe $e_G = e_G e_G$, so we have that $f(e_G) = f(e_G)f(e_G)$ so $f(e_G) = e_H$ by multiplying by $f(e_G)^{-1}$.

Lemma. If $f : G \rightarrow H$ is a homomorphism. Then $f(g^{-1}) = f(g)^{-1}$

Proof. Calculate $f(gg^{-1})$ in two ways.

In the first way $f(gg^{-1}) = f(e) = e$, in the second way $f(gg^{-1}) = f(g)f(g^{-1})$.

Equating gives that $f(g^{-1}) = f(g)^{-1}$. □

Definition. Let $f : G \rightarrow H$ be a homomorphism. The *kernal* of f is $\ker f = \{g \in G : f(g) = e\}$. The *image* of f is $\text{im } f = \{h \in H : h = f(g) \text{ for some } g \in G\}$.

Proposition. Let $f : G \rightarrow H$ be a homomorphism. Then $\ker f \triangleleft G$ and $\text{im } f \leq H$.

Proof. First let's proof that $\ker f$ is a subgroup by the subgroup test. Observe by the lemma that $e \in \ker f$. If $x, y \in \ker f$, then $f(xy^{-1}) = f(x)f(y)^{-1} = e \implies xy^{-1} \in \ker f$. For normality, let $x \in G$ and $g \in \ker f$. Calculate $f(xgx^{-1}) = f(x)f(g)f(x)^{-1}$. But $f(g) = e$. So we just get the identity. Hence we have that $xgx^{-1} \in \ker f$. So $\ker f \triangleleft G$.

To check that the $\text{im } f \leq H$, take $a, b \in \text{im } f$, say that $a = f(x), b = f(y)$. Then $ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$. But $xy^{-1} \in G$ so $f(xy^{-1}) \in \text{im } f$. Also $e \in \text{im } f$, so we have that $\text{im } f \leq H$. \square

Definition. (Isomorphism) A homomorphism $f : G \rightarrow H$ is an *isomorphism* if it is a bijection. Two groups are called *isomorphic* if there exists an isomorphism between them.

Theorem. (First isomorphism theorem) Let $f : G \rightarrow H$ be a homomorphism. Then $\ker f$ is normal, and the function $\varphi : G/\ker f \rightarrow \text{im } f$, by $\varphi(g\ker f) = f(g)$, is a well-defined, isomorphism of groups.

Proof. Already shown $\ker f \triangleleft G$. Consider whenever φ is well-defined. Suppose that $g\ker f = g'\ker f$. Need to check $\varphi(g\ker f) = \varphi(g'\ker f)$. We know that $gg'^{-1} \in \ker f$, so $f(gg'^{-1}) = e \iff f(g) = f(g')$. To see that φ is a homomorphism: $\varphi(g\ker f g'\ker f) = \varphi(gg'\ker f) = f(gg') = f(g)f(g') = \varphi(g\ker f)\varphi(g'\ker f)$. So φ is a homomorphism.

Finally let's check φ is bijective. First for surjectivity, let $h \in \text{im } f$, then $h = f(g)$ for some $g \in G$. So we have that $h = \varphi(g\ker f)$.

Now for injectivity, $\varphi(g\ker f) = \varphi(g'\ker f) \implies f(g) = f(g') \implies gg'^{-1} \in \ker f$. Hence the cosets are the same by the coset equality criterion, so we have that $g\ker f = g'\ker f$, hence we have injectivity, so φ is an isomorphism.

For an example of this theorem, consider the groups $(\mathbb{C}, +)$ and (\mathbb{C}^*, \times) related by the homomorphism, $\varphi(z) = e^z$. The kernel of \exp is exactly, $2\pi i\mathbb{Z} \leq \mathbb{C}$, so the first isomorphism theorem gives that $\frac{\mathbb{C}}{2\pi i\mathbb{Z}} \cong \mathbb{C}^*$. (Try to visualise this!) \square

Theorem. (Second isomorphism theorem) Let $H \leq G$ and $K \triangleleft G$. Then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G , the set $H \cap K$ is normal in H , and $\frac{HK}{K} \cong \frac{H}{H \cap K}$.

Proof. We take the statements in turn. First we can see that HK is a subgroup. Clearly it contains the identity, and take some $x, y \in HK$, $x = hk, y = h'k'$. We will show that $yx^{-1} \in HK$. Observe that $yx^{-1} = h'k'k^{-1}h^{-1} = h'(h^{-1}h)(k'k^{-1})h^{-1} = (h'h^{-1})h \underbrace{(k'k^{-1})}_{k''} h^{-1}$. But we have

that $hk''h^{-1} \in K$ by the normality of K , hence $yx^{-1} \in HK$. So we have that $HK \leq G$.

Now we prove that $H \cap K \triangleleft H$. Consider the homomorphism, $\varphi : H \rightarrow G/K$, defined as $\varphi(h) = hK$. This is a well defined homomorphism for the same reason that the group structure G/K is well-defined. The kernel of φ , is $\ker \varphi = \{h : hK = K\} = \{h : h \in K\} = H \cap K \triangleleft H$.

Now finally we're left to prove the isomorphism. Now apply the first isomorphism theorem to φ . This tells us that $\frac{H}{\ker \varphi} = \frac{H}{H \cap K} \cong \text{im } \varphi$. The image of the φ is exactly those cosets of K in G that can be represented as hK which is exactly $\frac{HK}{K}$. \square

Theorem. (Correspondence theorem). Consider a group G with $K \triangleleft G$, with the homomorphism $p : G \rightarrow G/K$, by $p(g) = gK$. Then there is a bijection between the subgroups of G which contain K and the subgroups of G/K .

Proof. For some subgroup L , we have $K \triangleleft L \leq G$, and we map L to L/K , so we have that $L/K \leq G/K$. In the reverse direction, for a subgroup $A \leq G/K$, we map it to $\{g \in G : gK \in A\}$. We can think of this as taking $L \rightarrow p(L)$ and $p^{-1}(A) \leftarrow A$.

Now we will state some facts without proof. (Although the proofs are fairly straightforward).

- (i) This is a bijection.
- (ii) This correspondence maps normal subgroups to normal subgroups.

Theorem. (Third isomorphism theorem) Let K, L be normal subgroups of G with $K \leq L \leq G$. Then we have that $\frac{G/K}{L/K} \cong \frac{G}{L}$.

Proof. Define a map $\varphi : G/K \rightarrow G/L$, by $\varphi(gK) = gL$. First we'll show that φ is a well-defined homomorphism, then we'll calculate the image and kernel, and finally apply the first isomorphism theorem. To see well-definedness, if $gK = g'K$, then $g'g^{-1} \in K \subseteq L$, so $g'L = gL$, so φ is well-defined. Obviously a homomorphism.

The kernel of φ is $\ker \varphi = \{gK : gL = L\} = \{gK : g \in L\} = L/K$. φ is clearly surjective, so we conclude by the first isomorphism theorem that $\frac{G/K}{L/K} \cong \frac{G}{L}$. \square

Definition. (Simple groups) A group G is called *simple* if the only normal subgroups are G itself and $\{e\}$.

Proposition. Let G be an abelian group. Then G is simple if and only if $G \cong C_p$, for p prime.

Proof. If $G \cong C_p$, then any $g \in G, g \neq e$ is a generator of G by Lagrange. Conversely if G is simple and abelian, then take some non-identity, $g \in G$, then $\{g^n : n \in \mathbb{Z}\}$ is a subgroup, and because G is abelian, this subgroup is normal. Since $g \neq e$, we must have G is cyclic, generated by g . Now if G is infinitely cyclic, then $G \cong \mathbb{Z}$, which is not simple since $2\mathbb{Z} \triangleleft \mathbb{Z}$, so we can't have this. Therefore $G \cong C_m$ for some $m \in \mathbb{Z}_{>0}$. Say q divides m , then the subgroup of G generated by $g^{\frac{m}{q}}$ is a normal subgroup, so we must have that $q = m$ or $q = 1$ by simplicity, hence we have that m is prime. \square

Theorem. (Composition series) Let G be a finite group. Then there exists subgroups such that, $G = H_1 \triangleright H_2 \triangleright H_3 \triangleright \cdots \triangleright H_n = \{e\}$, such that $\frac{H_i}{H_{i+1}}$ is simple.

Proof. If G is simple then take $H_2 = \{e\}$ and we're done. Otherwise, let H_2 be a proper normal subgroup of maximal order in G . We claim that G/H_2 is simple. To see this, suppose not and consider $\varphi : G \rightarrow G/H_2$. By non-simplicity and correspondence between normal subgroups, we find a proper normal in G/H_2 and therefore a proper normal $K \triangleleft G$. This leads to a contradiction as K contains H_2 non-trivially, so we contradict maximality, so G/H_2 is simple. Now we continue by replacing G with H_2 and iterate the process. Either we get that H_2 simple and we're done again, or we get find a proper normal subgroup $H_3 \triangleleft H_2$ of maximal order. This process must terminate, since G is finite and the order is strictly decreasing in each step. \square

We know from Part IA groups that A_5 is simple. We see a series like this for S_5 , namely, $S_5 \triangleright A_5 \triangleright \{e\}$.

1.4 Groups actions and permutations

Definition. Let X be a set. Let $\text{Sym}(X)$ denote the symmetric group of X and $S_n = \text{Sym}([n])$ where we have that $[n] = \{1, 2, \dots, n\}$.

Reminders from IA Groups:

- (i) We can write any $\sigma \in S_n$ as a product of disjoint cycles.
- (ii) If $\sigma \in S_n$ we can write σ as a product of transpositions. The number of transpositions needed to write σ is well-defined modulo 2. This is called the sign of the transposition, denoted by sgn , where $\text{sgn} : S_n \rightarrow \{\pm 1\}$.
- (iii) sgn is a homomorphism between the groups where $\{\pm 1\}$ is given the unique group structure. When $n \geq 3$, the homomorphism is surjective.

Definition. (Alternating group) The *alternating group* A_n is the kernel of sgn .

A homomorphism $\varphi : G \rightarrow \text{Sym}(X)$ is called a permutation representation of G .

Definition. (Group action) An *action* of G on a set X is a function $\tau : G \times X \rightarrow X$ sending $(g, x) \rightarrow \tau(g, x) \in X$ such that $\tau(e, x) = x, \forall x \in X$, and $\tau(g_1, \tau(g_2, x)) = \tau(g_1 g_2, x), \forall g_1 g_2 \in G, \forall x \in X$.

How are actions and permutation representations related?

For some homomorphism, $\varphi : G \rightarrow \text{Sym}(X)$ we map the homomorphism to $a(\varphi) : G \times X \rightarrow X$, where $(g, x) \rightarrow \varphi(g)(x)$.

Proposition. The function a above is a bijection from the set of homomorphism from $G \rightarrow \text{Sym}(X)$ to the set of actions from G on X .

Proof. We'll construct an inverse of a . Given a group action $* : G \times X \rightarrow X$. Define $\varphi(*) : G \rightarrow \text{Sym}(X)$ defined by sending $g \rightarrow \varphi(*) (g)$, where $\varphi(*) (g)(x) = g * x$. We aim to show that $\varphi(*) (g) : X \rightarrow X$ is a permutation. We have an inverse $\varphi(*) (g^{-1})$, and to see that it is a homomorphism $\varphi(*) (g_1) \varphi(*) (g_2)(x) = g_1 * (g_2 * x) = (g_1 g_2) * x = \varphi(*) (g_1 g_2)(x)$. This is true for all x , so the construction is a group homomorphism. \square

Notation: Given a group action G acting on X given by $\varphi : G \rightarrow \text{Sym}(X)$, denote $G^X = \text{im}(\varphi)$, and $G_X = \ker(\varphi)$. By the first isomorphism theorem we have that $G_X \triangleleft G$ and $G/G_X \cong G^X$.

For an example, consider the unit cube. Let G be the its symmetric group. Now let X be the set of (body) diagonals of the cube. Any element of G sends a diagonal to another diagonal, we get an action $G \rightarrow \text{Sym}(X) \cong S_4$. The kernel $G_X = \ker(\varphi) = \{e, \text{ send each vertex to its opposite}\}$. Easy exercise to check that any diagonal can be sent to any other diagonal, so $G^X = \text{im}(\varphi) = \text{Sym}(X)$. So by the first isomorphism theorem, we have that $S_4 \cong G^X \cong G/G_X \implies \frac{|G|}{2} = 4! \implies |G| = 48$.

For the next example let's look at a group acting on itself. Let G act on itself by $G \times G \rightarrow G$, sending $(g, g_1) \rightarrow gg_1$. This gives a homomorphism $G \rightarrow \text{Sym}(G)$ (easy to check that φ is injective since the kernel is trivial). By the first isomorphism theorem we get that every group is isomorphic to a subgroup of a symmetric group (Cayley's theorem).

Now let $H \leq G$ and let $X = G/H$, let G act on X by $g * g_1H = gg_1H$. We get $\varphi: G \rightarrow \text{Sym}(X)$. Consider $G_X = \ker \varphi$. If $g \in G_X$, then $gg_1H = g_1H, \forall g_1 \in G$, so $g_1^{-1}gg_1H = H \implies G_X \subseteq \bigcap_{g_1 \in G} g_1Hg_1^{-1}$. This argument is completely reversible, so if $g \in \bigcap_{g_1 \in G} g_1Hg_1^{-1}$, then for each $g_1 \in G$, we have $g_1^{-1}gg_1 \in H$, so $g \in G_X \implies G_X = \bigcap_{g_1 \in G} g_1Hg_1^{-1}$. Since G_X is a kernel and is a subset of H , we've got a way of making H smaller and making it normal. This is the largest normal subgroup contained in H .

Theorem. Let G be finite and $H \leq G$ of index n . There exists a normal subgroup of G , $K \triangleleft G$, with $K \leq H$, such that G/K is isomorphic to a subgroup of S_n . Thus, $|G/K|$ divides $n!$, and $|G/K| \geq n$.

Proof. Consider G acting on G/H in the previous example. So the kernel of $\varphi: G \rightarrow \text{Sym}(G/H)$ is normal, denote it by K . We've shown it is contained by H . First isomorphism theorem gives that $G/K \cong \text{im}(\varphi) \leq \text{Sym}(X) \cong S_n$. Give that $|G/K|$ divides $n!$ by Lagrange. Since that $K \leq H$, we have that $|G/K| \geq |G/H| \implies |G/K| \geq n$. \square

Corollary. Let G be non-abelian and simple. Let $H \leq G$ be a proper subgroup of index $n > 1$. Then G is isomorphic to a subgroup A_n . Moreover, $n \geq 5$, i.e. no subgroup of index less than 5.

Proof. Action of G on the set $X = G/H$ gives a homomorphism $\varphi: G \rightarrow \text{Sym}(X) \cong S_n$. Since the kernel is normal, since G is simple it is either G or $\{e\}$. Since H is a proper subgroup, for some $g \in G$, $gH \neq H$, so we must have that $\ker \varphi = \{e\}$. So $G \cong \text{im } \varphi \leq S_n$. Now we want to show that $\text{im } \varphi \leq A_n$. To see this observe that $A_n \triangleleft S_n$. Consider $A_n \cap \text{im } \varphi \leq \text{im } \varphi$. By the second isomorphism theorem, $\text{im } \varphi \cap A_n \triangleleft \text{im } \varphi \implies \text{im } \varphi \cap A_n = \{e\}$ or $\text{im } \varphi$ itself. By the rest of the second isomorphism theorem, if $\text{im } \varphi \cap A_n = \{e\} \implies \text{im } \varphi \cong \frac{\text{im } \varphi}{\text{im } \varphi \cap A_n} \cong \frac{\text{im } \varphi A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2$, but G is non-abelian, so $\text{im } \varphi$ is non-abelian, so we have a contradiction. So we have that $\text{im } \varphi \cap A_n = \text{im } \varphi$, so $\text{im } \varphi$ is a subgroup of A_n .

For the next part of the corollary, S_1, S_2 are abelian and S_3, S_4 have no non-abelian simple subgroups, so we must have $n \geq 5$. \square

Definition. (Orbits and stabiliser) Let G act on some set X . Then, the *orbit* of $x \in X$ is $G \cdot x = \text{orb } x = \{gx : g \in G\} \subseteq X$. And the *stabiliser* of $x \in X$ is $G_x = \text{stab}_G(x) = \{g \in G : gx = x\} \leq G$.

Theorem. (Orbit-stabiliser) For a group G acting on a set X . For all $x \in X$, there is a bijection $G \cdot x \rightarrow G/G_x$ given by $g \cdot x \rightarrow gG_x$. In particular, if G is finite, then $|G| = |G \cdot x| |G_x|, \forall x \in X$.

Proof. In the IA Groups course.

1.5 Conjugacy, centralisers, and normalisers

Let G be a group. The conjugation action of G acting on itself by $G \times G \rightarrow G$, is $(g, h) \rightarrow ghg^{-1}$. This is equivalent to a homomorphism $G \rightarrow \text{Sym}(G)$.

Fix $g \in G$. Then the permutation $G \rightarrow G$ given by $h \rightarrow ghg^{-1}$ is also a homomorphism.

Definition. (Automorphism) Let G be a group. A permutation $G \rightarrow G$ that is also a homomorphism is called an *automorphism* of G . The set of all automorphisms of G , $\text{Aut}(G) = \{f : G \rightarrow G : f \text{ is a automorphism}\} \subseteq \text{Sym}(G)$, is a subgroup, called the automorphism group of G .

Definition. (Conjugacy classes and centralisers) Fix $g \in G$. The *conjugacy class* of g is the set $\text{ccl}_G(g) = \{hgh^{-1} : h \in G\}$, i.e it is the orbit under the conjugation action. The *centraliser* of $g \in G$ is $C_G(g) = \{h \in G : hgh^{-1} = g\}$, i.e the stabiliser of g under the action.

Definition. (Centre) The *centre* of G is $Z(G) = \{z \in G : hzh^{-1} = z \forall h \in G\}$, i.e. it is the kernel of the conjugation action and the intersection of the centralisers.

Corollary. Let G be a finite group. Then $|\text{ccl}_G(x)| = |G : C_G(x)| = \frac{|G|}{|C_G(x)|}$.

Proof. Apply orbit-stabiliser to the conjugation action.

Definition. (Normaliser) Let $H \leq G$. The *normaliser* of H in G is $N_G(H) = \{g \in G : gHg^{-1} = H\}$

We can see clearly that $H \subseteq N_G(H)$ so $N_G(H)$ is non-empty and we also have that $N_G(H) \leq G$. In fact we have that $N_G(H)$ is the largest subgroup containing H in which H is normal.

1.6 Simplicity of A_n for $n \geq 5$

Recall from Part IA groups that a conjugacy class in S_n consists of the set of all elements with a fixed cycle type.

Theorem. Let $n \geq 5$. Then A_n is simple.

Proof. We will prove the statement via these three claims:

- (i) A_n is generated by 3-cycles
- (ii) If $H \triangleleft A_n$ that contains a 3-cycle then it contains all the 3-cycles
- (iii) Any non-trivial $H \triangleleft A_n$ contains a 3-cycle.

First we prove the first claim. Let $g \in A_n$, when viewed in S_n it is the product of evenly many transposition. Consider a product of two transpositions:

- (i) $(ab)(ab) = e \in A_n$
- (ii) $(ab)(bc) = (abc) \in A_n$
- (iii) $(ab)(cd) = (acb)(acd) \in A_n$.

In each case we can write all products of transpositions as a product of 3-cycles, hence we can write all elements in A_n as a product of 3-cycles.

Now for the second claim, any two 3-cycles in A_n are conjugate when viewed in S_n . Let δ, δ' be 3-cycles and write $\delta' = \sigma\delta\sigma^{-1}$, where $\sigma \in S_n$. If σ is even, we're done since it's in A_n . If σ is odd, observe since $n \geq 5$, there exists a transposition τ disjoint from δ , now $\delta' = \sigma(\tau\tau^{-1})\delta\sigma^{-1} = (\sigma\tau)\delta(\sigma\tau)^{-1}$. Since $\sigma\tau$ is even, we're done.

Finally for the last claim take some $H \triangleleft A_n$ not trivial. We break into cases

- (i) (a) If H contains an element on the form $\sigma = (12 \cdots r)\tau$ where τ is disjoint from $1, \dots, r$, and $r \geq 4$. Then let $\delta = (123)$. Now consider $\delta\sigma\delta^{-1} \in H$ (by normality). But then $\sigma^{-1}\delta^{-1}\sigma\delta \in H$ as well. As τ misses $1, 2, 3$ and commutes with $(12 \cdots r)$ we expand this: $\sigma^{-1}\delta^{-1}\sigma\delta = (r \cdots 21)(132)(123 \cdots r)(123) = (23r)$ so we find a 3-cycle.
- (ii) (b) Suppose H contains $\sigma = (123)(456)\tau$ (or any relabeling of such). τ is disjoint from $1, \dots, 6$. Take $\delta = (124)$ and calculate the conjugation $\sigma^{-1}\delta^{-1}\sigma\delta = (124236)$ which is a 5-cycle so we're done by the first case.
- (iii) (c) Suppose that H contains σ of the form $\sigma = (123)\tau$ where τ is a product of disjoint transpositions. Note if τ contains anything longer than a transposition, we can just apply case (a) or (b). Then $\sigma^2 = (123)^2$ which is a 3-cycle since the transpositions cancel.
- (iv) (d) Suppose that H contains $\sigma = (12)(34)\tau$, where τ is a product of transpositions. Let $\delta = (123)$, consider $\mu = \sigma^{-1}\delta^{-1}\sigma\delta = (14)(23)$. Let $\nu = (152)\mu(125) = (13)(45)$. But observe that $\mu\nu \in H$, but this is a 5-cycle, so we're done by case (a).

Up to relabeling, we're covered all the cases. Hence any normal subgroup of A_5 must be trivial or A_5 itself, so A_5 is normal. \square

1.7 Finite p -groups

Definition. (Finite p -groups) For p prime, a *finite p -group* is a group of order p^n , $n \in \mathbb{N}$.

Theorem. Let G be a finite p -group. Then $Z(G)$ is non-trivial.

Proof. Consider G acting on itself by conjugation. The centre of G is the union of orbits of size 1. The orbits partition G , so

$$|G| = p^n = |Z(G)| + \sum \text{sizes of conjugacy classes of size } > 1$$

We know that the sizes of the non-trivial conjugacy classes always divide p^n . So all the terms of size larger than one are divisible by p . Hence we have that p divides $|Z(G)|$. So since $p \geq 2$, the centre is non-trivial. \square

Theorem. A group of size p^2 must be abelian.

Proof. Follows from an independently interesting technical result:

Lemma. If G is any group and $\frac{G}{Z(G)}$ is cyclic, then G is abelian.

Proof. Let $xZ(G)$ generate $\frac{G}{Z(G)}$. Every coset of the form $x^mZ(G)$, $m \in Z$. Since any $g \in G$ lies in some coset of $Z(G)$, we can write $g = x^mz$, for some $z \in Z(G)$. Now for some $g' \in G$, $g' = x^n z'$, so $gg' = x^m z x^n z' = x^{n+m} z z' = x^n z' x^m z = g'g$, so the group is abelian.

Our proof of the theorem follows since $Z(G)$ is non-trivial, so it either has size p^2 or p . If it has size p^2 , the group is abelian so we're done. If it has size p , the $G/Z(G)$ also has size p , so it's cyclic, hence it's abelian, so by the lemma we have that G is abelian. \square

Theorem. Let G be a group of size p^n . Then for any $0 \leq k \leq n$, G has a subgroup of size p^k .

Proof. (Inductive proof) The base case $n = 1$ is clear because the group must be cyclic. Now suppose that $n > 1$, if $k = 0$, we take $\{e\}$, so we're done, so assume that $k \geq 1$. Note that $Z(G)$ is non-trivial, let $x \in Z(G)$ with $x \neq e$. The order of x is a power of p . By raising x to some power we can find an element with order p in $Z(G)$. Replacing x with this element we can assume $\text{ord}(x) = p$. The subgroup generated by x is normal of size p because x is central of order p . Now $\frac{G}{\langle x \rangle}$ is a group of order p^{n-1} so inductive hypothesis allies. Let $L \leq \frac{G}{\langle x \rangle}$ of size p^{k-1} . But by the subgroup correspondence result, we can find some $K \leq G$ containing $\langle x \rangle$ such that $\frac{K}{\langle x \rangle} = L$. So K has size p^k , so we're done. \square

1.8 Finite abelian groups

Theorem. (Classification of finite abelian groups) Let G be a finite abelian group. There exists positive integers d_1, \dots, d_r such that:

$$G \cong C_{d_1} \times C_{d_2} \times \dots \times C_{d_r}$$

Moreover, we can choose d_i such that $d_{i+1} \mid d_i$ in which case this is unique.

Proof. To come later...

Abelian groups of order 8 are exactly $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$.

Lemma. (Chinese remainder theorem) If n and m are coprime, then $C_n \times C_m \cong C_{nm}$

Proof. Consider $C_n \times C_m$. Suffices to produce an element of order nm . Let $g \in C_n$ and $h \in C_m$ be generators of order n and m respectively. Consider (g, h) . Say its order is $k \implies (g, h)^k = (e, e)$. So n, m both divide k , and since n, m are coprime we have that nm divides k and by Lagrange we have that k divides nm , so we're done. \square

1.9 Sylow Theorems

Definition. (Sylow p -subgroup) Let G be a finite group of order $p^a m$, where $p \nmid m$, p is a prime. Then a *Sylow p -subgroup* of G is a subgroup of size p^a .

Theorem. (Sylow theorems) For a finite group G of order $p^a m$, where $p \nmid m$, p is prime:

- (i) The set $\text{Syl}_p(G) = \{P \leq G \mid P \text{ is a Sylow } p\text{-subgroup of } G\}$ is non-empty.
- (ii) Any $H, H' \in \text{Syl}_p(G)$ are conjugate, namely $H = gH'g^{-1}$, for some $g \in G$.
- (iii) If $n_p = |\text{Syl}_p(G)|$ then $n_p \equiv 1 \pmod{p}$ and n_p divides $|G|$, so $n_p \mid m$

Before we prove the statement, let's see why this theorem is useful.

Lemma. If $\text{Syl}_p(G) = \{P\}$, then P is normal in G .

Proof. For any $g \in G$, the subgroup gPg^{-1} is isomorphic (as a group) to P . So gPg^{-1} is in $\text{Syl}_p(G) \implies gPg^{-1} = P$, which proves the claim. \square

Corollary. Let G be a non-abelian simple group, and $p \mid |G|$, p prime. Then $|G|$ divides $\frac{n_p!}{2}$ and $n_p \geq 5$.

Let G act by conjugation on $\text{Syl}_p(G)$ which gives a homomorphism $\varphi : G \rightarrow \text{Sym}(\text{Syl}_p(G)) \cong S_{n_p}$. By simplicity, $\ker \varphi = G$ or $\{e\}$. If $\ker \varphi = G$, then $gPg^{-1} = P$ for all $g \in G$ and all $P \in \text{Syl}_p(G)$. So P is normal. Thus P is either $\{e\}$ or G . Well P is Sylow- p so it can't be $\{e\}$, so $P = G$. So G would be a p -group. But from earlier, the centre of G is non-trivial proper since G is non-abelian, but the centre is always normal, so this contradicts simplicity, hence $\ker \varphi = \{e\}$. So we have that φ is an injective homomorphism $G \rightarrow S_{n_p}$, so by the first isomorphism theorem, $G \cong \text{im } \varphi$. We'll show that φ lands in A_{n_p} . Consider the composition $G \rightarrow S_{n_p} \rightarrow \{\pm 1\}$. If this composition is surjective, then $\ker(\text{sgn} \circ \varphi)$ is index 2, but G simple so not possible. So $\text{im } \varphi \subseteq \ker(\text{sgn}) = A_{n_p}$, so we're done by Lagrange. For the final statement we show all non-abelian subgroups of A_2, A_3, A_4 are not simple which finishes the statement which is just grunt work, and I pinky promise it's true, so we're done. \square

Let's see a sample application. Let have G has size 11×12 . If G is simple then there are exactly 12 Sylow 11-subgroups. Consider the number n_{11} . We know from the Sylow theorems that $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 12$. So $n_{11} = 12$ since G is simple. Similarly $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 44$. So either $n_3 = 4$ or 22 . The corollary says that G divides $\frac{n_3!}{2}$, so n_3 can't be 4, so $n_3 = 22$. But this is a lot of elements. And 2 Sylow 11-subgroups intersect only at the identity which leads to too many elements, so none of this even works, which seems confusing, but actually just means that G can't exist, hence all groups of order 132 are non-simple.

Finally we now prove the Sylow theorems.

Proof. Let G be a group of order $n = p^a m$, with $p \nmid m$, p prime. Define the set $\Omega = \{X \subseteq G : |X| = p^a\}$. Let G act on Ω by multiplying all elements of Ω on the left by $g \in G$ (we can see this obeys the axioms of the group action after some quick inspection). We have $|\Omega| = \binom{n}{p^a} \equiv m \pmod{p}$. The proof of this can be seen by expanding out the binomial coefficient, but we'll assume it here. Suppose we have some $U \in \Omega$, then let $H \leq G$ stabilise U . Then $|H| \mid |U|$. We can prove this by seeing that $hU = U$ for all $h \in H$. In other words for each $u \in U$ the coset Hu is

contained in U . Every $u \in U$ lies in some coset of H , so the cosets partition U , so $|H| \mid |U|$. We know that $|\Omega| \not\equiv 0 \pmod{p}$. Since orbits partition, we know that

$$|\Omega| = |O_1| + |O_2| + \cdots + |O_r|, \text{ } O_i \text{ are the orbits}$$

So there exists an orbit Θ whose size is prime to p . Let $T \in \Theta$. By orbit-stabiliser, $|G| = |\Theta| |\text{stab}(T)|$. So $p^a m = |\Theta| |\text{stab}(T)|$. By our previous lemma, $|\text{stab}(T)| \mid p^a$, so we're done because there are no factors of p in Θ , so we've prove the first part of the theorem.

Now for the second part, we actually show something stronger, that is, if $Q \leq G$ is a subgroup of size p^b , where $0 \leq b \leq a$, then there exists $g \in G$ and $P \in \text{Syl}_p(G)$, such that $gQg^{-1} \leq P$. To prove this, let Q act on G/P by left coset multiplication. Note that the size of G/P does not divide by p . Orbits have size dividing p^b , so each orbit has size 1 or a power of p . But $p \nmid |G/P|$, so there exists a size 1 orbit. In other words, there exists some coset gP such that $\forall q \in Q, qgP = gP$, so rearranging gives that $gQg^{-1} \leq P$. So our second statement follows taking $b = a$.

For the final theorem, we need to show that $n_p \mid |G|$, and $n_p \equiv 1 \pmod{p}$. For the first statement, consider G acting on $\text{Syl}_p(G)$ by conjugation. By the second theorem, we know that there is one orbit of size n_p , so the statement follows instantly from orbit-stabiliser. For the second statement, let $P \in \text{Syl}_p(G)$. Consider P acting on $\text{Syl}_p(G)$ by conjugation. By orbit-stabiliser, all the orbits have size 1 or p . Since $\{P\}$ is a size 1 orbit, to prove the statement suffices to show that $\{P\}$ is the only size 1 orbit. Say $\{Q\}$ is another size 1 orbit. So $\forall h \in P$, we have $hQh^{-1} = Q$. This means that $N_G(Q)$ contains P . Now observe if p^a is the largest power of p dividing $|G|$, we know that it's the largest power of p dividing $|N_G(Q)|$. But Q is normal in $N_G(Q)$ by definition, and $Q, P \in \text{Syl}_p(N_G(Q)) \implies P = Q$, since normality \iff uniqueness for Sylow subgroups. So we've prove all the Sylow theorems and we're done. \square

2 Rings

2.1 Definitions and examples

Definition. (Rings) A *ring* is a quintuple $(R, +, \circ, 0_R, 1_R)$, where R is a set with $0_R, 1_R \in R$, and $+, \circ : R \times R \rightarrow R$, called addition and multiplication are functions satisfying the following:

- (i) $(R, +, 0_R)$ is an abelian group.
- (ii) \circ is associative, so $a \circ (b \circ c) = (a \circ b) \circ c$.
- (iii) $1_R \circ a = a \circ 1_R = a$.
- (iv) We have distributivity, so $r_1 \circ (r_2 + r_3) = (r_1 \circ r_2) + (r_1 \circ r_3)$ and $(r_1 + r_2) \circ r_3 = (r_1 \circ r_3) + (r_2 \circ r_3)$.

Usually we just say "Let R be a ring..." with everything implicit. The symbol $(-r)$ denotes the additive inverse of r .

In IB Groups, Rings and Modules, rings will always be commutative, so $r_1 \circ r_2 = r_2 \circ r_1$ for all $r_1, r_2 \in R$.

Definition. (Subring) A *subring* of a ring R , is a subset $S \subseteq R$, such that $0_R, 1_R \in S$, S is closed under both multiplication and addition of the ring, and $(S, +, \circ, 0_R, 1_R)$ is a ring.

We notate this as $S \leq R$.

For examples we have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ which are all rings under usual multiplication and addition. Along a similar line, we also have the Gaussian integers, $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ with multiplication and addition induced by \mathbb{C} .

Another example is $\mathbb{Z}/n\mathbb{Z}$ which forms a ring under addition and multiplication modulo n . In $\mathbb{Z}/6$ we have $2, 3 \in \mathbb{Z}/6$ such that $2 \circ 3 = 0 \pmod{6}$ which is perfectly allowed.

Definition. (Units) An element $u \in R$, is called a *unit* if there exists some $v \in R$, such that $uv = 1_R \in R$.

This notion does *not* interact well with subrings, as we can take a unit in a subring without taking its inverse, making it no longer a unit. For example 2 is a unit \mathbb{Q} , but not in \mathbb{Z} .

Discussion. Does 0_R behave like it should? We would like $0 \circ R = 0_R$ for all $r \in R$. In R we have that $0_R + 0_R = 0_R$, now multiplying by $r \in R$, so $r \circ 0_R + r \circ 0_R = r \circ 0_R$, hence cancelling a $r \circ 0_R$ on both sides gives that $r \circ 0_R = 0_R$.

In particular this implies that if $1_R = 0_R$ then for any $r \in R$, $r = r \circ 1_R = r \circ 0_R = 0_R$ so for all $r \in R$, $r = 0_R$, so R must be the zero ring, $\{0_R\}$.

Definition. (Polynomial) Let R be a ring. Then a *polynomial* in x with coefficients in R in an expression:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

and x^i are formal symbols. We will identify $f(x)$ with $f(x) + 0 \circ x^{n+1}$ as the same. The largest i such that $a_i \neq 0$ is called the degree of the polynomial. A polynomial $f(x)$ is monic of degree n if $a_n = 1$ and it is of degree n .

Definition. (Polynomial ring) The *polynomial ring* $R[X]$ is given by:

$$R[X] = \{f(X) : f \text{ is a polynomial in } X \text{ with coefficients in } R\}$$

$+, \circ$ are the usual operations, $0_{R[X]} = 0_R$ and $1_{R[X]} = 1_R$.

Definition. (Ring of formal power series) The *ring of formal power series* is a ring in X with coefficients in R is:

$$R[[X]] = \left\{ \sum_{n=0}^{\infty} r_n X^n : r_n \in R, \forall n \geq 0, n \in \mathbb{Z} \right\}$$

with the standard $+, \circ$ of R .

For an example consider $(1 - x) \in R[X]$. Is it a unit? No! If $g(x)(1 - x) = 1$, then if $g(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, then $(1 - x)g(x) = a_0 + (a_1 - a_0)x + \cdots + (a_n - a_{n-1})x^n - a_nx^{n+1}$ which cannot be 1 since the highest power term has a non-zero coefficient.

However $(1 - x)$ is a unit in $R[[X]]$! $(1 - x)(1 + x + x^2 + \cdots) = 1 \in R[[X]]$.

Definition. (Laurent polynomials) If R is a ring then a *Laurent polynomial* with coefficients in R is:

$$R[X, X^{-1}] = \left\{ \sum_{i \in \mathbb{Z}} a_i X^i : a_i \in R, \forall i \in \mathbb{Z} \right\}$$

Where a_i is non-zero for at most finitely many i and with standard multiplication and addition.

If R is a ring, and X is a set the set of R -valued functions, namely, $\{f : X \rightarrow R\}$ is a ring with "pointwise" addition and multiplication as given by the ring R . (So $(f + g)(x) = f(x) + g(x)$)

2.2 Homomorphisms, ideals, and quotients

Definition. (Ring homomorphism) Let R and S be rings. A function $f : R \rightarrow S$ is a *ring homomorphism* if for all $r_1, r_2 \in R$:

- (i) $f(r_1 + r_2) = f(r_1) + f(r_2)$
- (ii) $f(0_R) = 0_S$
- (iii) $f(r_1 r_2) = f(r_1) f(r_2)$
- (iv) $f(1_R) = 1_S$.

These first two conditions are the conditions for f to be a group homomorphism with the addition operation. Note that the second condition is not required and it follows from the first condition.

But non-symmetrically the fourth condition is not implied by the third condition.

Definition. (Isomorphism) An *isomorphism* $f : R \rightarrow S$ is a bijective ring homomorphism. The inverse function is also a ring homomorphism.

Definition. (Kernal) The *kernal* of a ring homomorphism $f : R \rightarrow S$ is the set $\ker f = \{r \in R : f(r) = 0_S\}$.

Definition. (Image) The *image* of a ring homomorphism $f : R \rightarrow S$ is $\text{im } f = \{s \in S : s = f(r) \text{ for some } r \in R\}$.

Lemma. A homomorphism $f : R \rightarrow S$ is injective if and only if $\ker f = \{0\}$.

Proof. Follows from the corresponding fact about groups. □

Definition. (Ideal) A subset $I \subseteq R$ is an *ideal*, written as $I \triangleleft R$, if I is a subgroup and if $a \in I$ and $b \in R$, then $ab \in I$.

Keep in mind that an ideal is usually not a subring, since if $1_R \in I$ then $I = R$.

Lemma. If $f : R \rightarrow S$ is a ring homomorphism then $\ker f \triangleleft R$.

Proof. Since f is also a group homomorphism, then $\ker f$ is a subgroup. If $a \in \ker f$ and $b \in R$ then $f(ab) = f(a)f(b) = 0f(b) = 0$, so $ab \in \ker f$. □

Now we'll look at some examples.

If \mathbb{Z} is the ring of integers then $n\mathbb{Z}$ are ideals for all $n \in \mathbb{N} \cup \{0\}$. In fact, every ideal of \mathbb{Z} has this form. To see this $I \neq \{0\}$ is an ideal. Let $n \in \mathbb{Z}$ be the smallest positive element of I . We claim that $I = n\mathbb{Z}$. Let $m \in I$. We claim that it's divisible by n . Apply the Euclidean algorithm so $m = qn + r$ where $0 \leq r < n$. But $qn \in I$ by the absorbing property so $r \in I$ since I is a subgroup which contradicts minimality unless $r = 0$. □

Definition. Let $A \subseteq R$. The ideal generated by A is

$$(A) = \left\{ \sum_{a \in A} r_a a, \quad r_a \in R, \quad \text{all but finitely many } r_a \text{ are } 0 \right\}$$

Definition. (Principle) An ideal $I \triangleleft R$ is *principle* if there exists $r \in R$ such that $(r) = I$.

For another example let $\mathbb{R}[X]$ be the polynomial ring in one variable over \mathbb{R} . The subset $\{f \in \mathbb{R}[X] : \text{constant term is } 0\}$, is an ideal. It is actually principle, generated by (X) .

Definition. (Quotient) Let $I \triangleleft R$ be an ideal. Then the *quotient ring* R/I is the set of cosets $r + I$ with $0_R/I = 0_R + I$ and $1_R/I = 1_R + I$, and operations $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ and $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.

Proposition. The quotient ring is a ring. The function $f : R \rightarrow R/I$ sending r to $r + I$ is a ring homomorphism.

Proof. Obviously an abelian group. Multiplication is well-defined. To see this 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 absorbing property the last three terms are contained in I , so $r_1 r_2 + I = r'_1 r'_2 + I$. The rest is straightforward. \square

For another example, we have $n\mathbb{Z} \triangleleft \mathbb{Z}$. The quotient $\mathbb{Z}/n\mathbb{Z}$ is the usual ring of integers modulo n . Take $(X) \triangleleft \mathbb{C}[X]$. The elements of $\mathbb{C}[X]/(X)$ are represented by:

$$a_0 + a_1 X + \cdots + a_n X^n + (X), \text{ but } \sum_{i=1}^n a_i X^i \in (X)$$

so each coset is represented equivalently by $a_0 + (X)$, so we have that $\mathbb{C}[X]/(X) \cong \mathbb{C}$.

Similarly $(X^2) \triangleleft \mathbb{C}[X]$, the ring $\mathbb{C}[X]/(X^2)$ consists of elements represented by linear polynomials $a_0 + a_1 X + (X)$ with the following multiplication given by $(a_0 + a_1 X)(b_0 + b_1 X) = a_0 b_0 + (a_1 b_0 + a_0 b_1)X$.

This ring is quite weird. For example if we take $X \in \mathbb{C}[X]/(X^2)$. Then $0 \neq X$ but $X^2 = 0$. We say that X is nilpotent.

Proposition. (Euclidean algorithm for polynomials in X) Let K be a field and $f, g \in K[X]$. Then there exists polynomials $r, q \in K[X]$ such that $f = gq + r$ with $\deg(r) < \deg(g)$.

Proof. Let n be the degree of f . So $f = \sum_{i=0}^n a_i X^i$ with $a_i \in K, a_n \neq 0$. Similarly $g = \sum_{i=0}^m b_i X^i$ with $b_i \in K$ and $b_m \neq 0$.

If $n < m$ set $q = 0$ and $r = f$ so we're finished.

If instead $n \geq m$, proceed by induction on the degree. Let $f_1 = f - a_n b_m^{-1} X^{n-m} g$. Observe that $\deg(f_1) < n$. If $n = m$ then $\deg(f_1) < n = m$. So write $f = (a_n b_m^{-1} X^{n-m})g + f_1$, so we're done. Otherwise if $n > m$, then because $\deg(f_1) < n$, by induction we can write $f_1 = gq_1 + r_1$ where $\deg(r_1) < \deg(g) = m$. Then $f = (a_n b_m^{-1} X^{n-m} g + q_1 g + r_1) = (a_n b_m^{-1} X^{n-m} + q_1)g + r_1$ \square

Corollary. If K is a field then $K[X]$ every ideal is principal.

Proof. Identical to the case of \mathbb{Z} using the proposition.

This proof fails for $\mathbb{Z}[X]$ (since \mathbb{Z} is not a field) and for $K[X, Y]$.

Theorem. (First isomorphism theorem) Let $\varphi : R \rightarrow S$ be a ring homomorphism. Then the function $f : R/\ker \varphi \rightarrow \text{im } \varphi \leq S$ sending $r + \ker \varphi \rightarrow \varphi(r)$ is well-defined and an isomorphism of rings.

Proof. Well-definedness, bijective, additive homomorphism property all follow from the group statement. We check multiplicativity. $f((f + \ker \varphi)(t + \ker \varphi)) = f(rt + \ker \varphi) = \varphi(rt) = \varphi(r)\varphi(t) = f(r + \ker \varphi)(f + t + \ker \varphi)$ since φ is a ring homomorphism. \square

For an example consider the homomorphism $\varphi : \mathbb{R}[X] \rightarrow \mathbb{C}$ sending $f(X)$ to $f(i)$. Clearly this is a surjective ring homomorphism since $a + bX \rightarrow a + bi$ under φ . The kernel is exactly real polynomials $f(X)$ such that $f(i) = 0$ i.e i is a root. But since f has real coefficients that means that $(X + i)(X - i) \mid f(X)$ i.e. $(X^2 + 1) \mid f(X)$. So in fact $\ker \varphi = (X^2 + 1)$, the ideal generated by $X^2 + 1$. Now applying the first isomorphism theorem $\frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}$.

Theorem. (Second isomorphism theorem) Let $R \leq S$ and $J \triangleleft S$. Then $J \cap R \triangleleft R$ and $\frac{R+J}{J} = \{r + J : r \in R\} \leq \frac{S}{J}$. Furthermore,

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

Proof. Define a function $\varphi : R \rightarrow S/J$ by $r \mapsto r + J$. The kernel is $\{r : r + J = 0\} = \{r \in J\} = R \cap J$. The image $\text{im } \varphi = \{r + J : r \in R\} = \frac{R+J}{J}$, so apply the first isomorphism theorem to conclude. \square

Again similar to groups we have a correspondence result.

Theorem. (Correspondence theorem) If $I \triangleleft R$ is an ideal there is a bijection between subrings of R/I and subrings of R which contain I . This is given by sending $L \leq R/I \rightarrow \{r \in R : r + I \in L\}$ and conversely $I \triangleleft S \leq R \rightarrow S/I \leq R/I$

Proof. Same as from groups.

Similar for ideals there is a bijection between ideals in R/I and ideals in R that contain I .

Theorem. (Third isomorphism theorem) Let $I \triangleleft R$ and $J \triangleleft R$ with $I \subseteq J$. Then $\frac{J}{I} \triangleleft \frac{R}{I}$ and we have that,

$$\frac{R/I}{J/I} \cong R/J.$$

Proof. Define a function $\varphi : R/I \rightarrow R/J$ sending $r + I$ to $r + J$. Well-definedness follows from the same argument as from groups. Easy verification to see it is a ring homomorphism. The kernel is $\ker \varphi = \{r + I : r + J = J\}$, i.e. that $\ker \varphi = J/I$. So apply the first isomorphism theorem to get the result. \square

Claim. Let R be any ring. There is a unique ring homomorphism

$$i : \mathbb{Z} \rightarrow R$$

The kernel of i , $\ker i$ is an ideal $n\mathbb{Z} \triangleleft \mathbb{Z}$. The number $|n|$ is called the characteristic of R . The rings $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{C}[X]$ all have characteristic 0. $\mathbb{Z}/k\mathbb{Z}$ has characteristic k .

2.3 Integral domains

In the ring $\mathbb{Z}/6$ we have that $2 \cdot 3 = 0$. In an integral domain this will not happen.

Definition. (Integral domain) A nonzero ring R is an integral domain if $\forall a, b \in R$, if $ab = 0$ then $a = 0$ or $b = 0$.

An element that violates this is called a zero divisor, i.e. a zero divisor is a non-zero element $a \in R$ such that $\exists b \in R, b \neq 0$ where $ab = 0$.

All fields are integral domains, since if $ab = 0, b \neq 0$ then $a(bb^{-1}) = 0b^{-1} = 0$ so $a = 0$.

Any subring of an integral domain is an integral domain. To list a set of examples we have $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}, \mathbb{C}, \mathbb{R}[X], \mathbb{Z}[X]$, etc. For a set of non-examples we have $\mathbb{Z}/6, \mathbb{Z}/pq, \mathbb{C}[X]/(X^2)$ etc.

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

Proof. Let $a \in R$ be non-zero. Consider the function $\mu_a : R \rightarrow R$ sending $r \rightarrow ar$. It's easy to verify that μ_a is an (additive) group homomorphism for all a non-zero. Since R is an integral domain, $\ker \mu_a$ is trivial so the map is injective. So since R is finite, μ_a is also surjective. In particular $1 = ab$ for some $b \in R$ hence this is an inverse of a , so R is a field. \square

Definition. Let R be an integral domain. A *text of fractions* for R is a field F such that:

- (i) $R \leq F$ is a subring,
- (ii) every $x \in F$ can be written as ab^{-1} , where $a, b \in R$, where b^{-1} is the multiplicative inverse to b in F .

\mathbb{Q} is a field of fractions for \mathbb{Z} .

Theorem. Every integral domain has a field of fractions.

Proof. Define a set $S = \{(a, b) \in R \times R : b \neq 0\}$. Place an equivalence relation \sim , defined as $(a, b) \sim (c, d) \iff ad = bc$ on S . We can check this is an equivalence relation, the only non-trivial axiom to check is transitivity. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. So we have that $ad = bc$ and $cf = de$. We wish to deduce that $af = be$. Multiple the first equality by f and the second by b . So we get that $adf = bcf$ and $bcf = bed$. Rearranging we get $d(af - be) = 0$ since d is non-zero and R is an integral domain we know that $af = be$. So \sim is an equivalence relation. Now define $F = \frac{S}{\sim}$ with notation $\frac{a}{b} = [(a, b)]_{\sim}$. Now we turn F into a ring. Take the operations to be $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Some elementary operations show that these operations are well-defined and makes F into a ring. To see that F is a field, if $\frac{a}{b} \neq 0_F$ i.e. $\frac{a}{b} \neq \frac{0}{1} \implies a \cdot 1 \neq b \cdot 0 = 0$, so $a \neq 0$. now $\frac{b}{a} \in F$ and $\frac{b}{a} \cdot \frac{a}{b} = 1_F$, so F is a field.

We now construct an injective homomorphism $R \rightarrow F$ by $r \rightarrow \frac{r}{1}$. Straightforward to check that this is a ring homomorphism. The kernel is $\{r \in R : \frac{r}{1} = 0 \text{ in } F\} = (0)$. By the first isomorphism theorem R is isomorphic to the image of $R \rightarrow F$, in other words $R \leq F$. Finally since $\frac{a}{b} \in F$ is $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} \implies \frac{a}{1} \left(\frac{1}{b}\right)^{-1} = ab^{-1}$ \square

Sometimes we write $\text{FF}(R)$ for a field of fractions of R .

Proposition. Let R be a ring. Then R is a field if and only if the only ideals in R are (0) and R .

Proof. If R is a field and $I \triangleleft R$ is non-zero then I contains a unit u . Since $1 = uv$ we have that $1 \in I$. But for any $r \in R$, we have $1 \cdot r = r \in I$, so $I = R$.

Conversely suppose that (0) and R are the only ideals of R . Take $r \in R$ non-zero. We know that $(r) = R$ since r is non-zero. Since $1 \in (r)$ we know that $r \cdot b = 1$ for some $b \in R$ so r is a unit hence R is a field.

Definition. (Maximal ideal) An ideal $I \triangleleft R$ is called *maximal* if it is not R itself and if for any $J \triangleleft R$ with $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

Proposition. An ideal $I \triangleleft R$ is maximal if and only if R/I is a field.

Proof. R/I is a field if and only if the ideals are R/I and (0) . Now apply the ideal correspondence theorem. \square

Definition. (Prime ideal) An ideal $I \triangleleft R$ is *prime* if whenever $ab \in I$ either a or b lies in I .

An ideal $n\mathbb{Z} \triangleleft \mathbb{Z}$ is a prime ideal if and only if n is a prime number (or zero). We can see this since if $n = p$ is prime, and $ab \in p\mathbb{Z}$ then ab is a multiple of p so either a or b must be a multiple of p hence in $p\mathbb{Z}$. Conversely if n is not prime and wlog positive (zero case is trivial) we know that $n = m_1 m_2$, $1 < m_1, m_2 < n$. Then $m_1, m_2 \notin n\mathbb{Z}$ but $m_1 m_2 \in n\mathbb{Z}$ so the ideal is not a prime ideal.

Interestingly $p\mathbb{Z} \triangleleft \mathbb{Z}$ for p non-zero prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field so $p\mathbb{Z}$ is maximal.

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

Proof. If $I \triangleleft R$ is prime, then let $(a+I)$ and $(b+I) \in R/I$. Suppose $(a+I) \cdot (b+I) = (ab+I) = 0+I$ (recall $0+I$ is the zero element in R/I). This means that $ab \in I$ but I is prime so a or $b \in I$, so $a+I$ or $b+I$ is 0 .

Conversely if R/I is an integral domain, consider $ab \in I$. Then $ab+I = 0$. So either $a+I$ or $b+I$ is zero so a or b lies in I . So I is a prime ideal. \square

Corollary. If R is a prime and $I \triangleleft R$ is maximal, then I is prime.

Proof. Since $I \triangleleft R$ is maximal then R/I is a field. Hence R/I is an integral domain so I is prime by the proposition. \square

Every nonzero ring R has a maximal ideal and therefore a prime ideal (proof is very set theoretic, equivalent to the axiom of choice through Zorn's lemma)

2.4 Factorisation in integral domains

From now on we let R be a general integral domain

Definition. (Division) Let $a, b \in R$ we say that a *divides* b , written as $a \mid b$ if there exists some $c \in R$ such that $b = ac$. Equivalently we have that $(b) \subseteq (a)$.

Definition. (Associates) We say that a and b in R are *associates* if $a = bc$ for $c \in R$ a unit. Equivalent to $(a) = (b)$ and also equivalent to that $a \mid b$ and $b \mid a$.

In \mathbb{Z} for example, we want to factorise up to units, i.e $6 = 2 \times 3 = (-2) \times (-3)$. But as 2 and -2 are associates we declare some amount of uniqueness.

Definition. (Irreducible) An element $a \in R$ is called *irreducible* if $a \neq 0$, a is not a unit, and if $a = xy$ then either x or y is a unit.

In the special case of \mathbb{Z} irreducible and prime are the same thing. But this is NOT always the case.

Definition. (Prime element) We say that an element $p \in R$ is *prime* if $p \neq 0$, not a unit and if $p \mid xy$, then either $p \mid x$ or $p \mid y$.

Proposition. Let $r \in R$. Then $r \neq 0$ is prime if and only if (r) is a prime ideal.

Proof. Suppose that (r) is a prime ideal. Then it is proper by definition, so r is not a unit. Suppose that $r \mid xy$, so $xy \in (r)$ so by primality either x or y lies in (r) so $r \mid x$ or $r \mid y$. Conversely let $r \in R$ be a prime. Suppose $xy \in (r)$ then $r \mid xy$ so $r \mid x$ or $r \mid y$ so $x \in (r)$ or $y \in (r)$ \square

Again irreducible and prime are not the same thing. However...

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

Proof. Let $r \in R$ be a prime and suppose can write r as $r = xy$. Since $r = 1_R r$ we have that $r \mid xy$ so either $r \mid x$ or $r \mid y$. Assume by symmetry that $r \mid x$. This means that $x = rz$ for $z \in R$. So $r = xy = rzy$. So since we're in an integral domain and $r \neq 0$ we have that $zy = 1$ hence y is a unit \square

Now let's look at an example.

Let $R = \mathbb{Z}[\sqrt{-5}] \leq \mathbb{C}$, i.e. elements of the form $a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$. Observe that R is an integral domain since it is a subring of a field. Let's discuss the units. We define a "norm", $N : R \rightarrow \mathbb{Z}_{\geq 0}$ sending $a + b\sqrt{-5} \rightarrow a^2 + 5b^2$. This is a function and importantly it is multiplicative, so $N(ab) = N(a)N(b)$. Notice that all units have norm 1, since if $1 = uv$, then $N(1) = N(u)N(v) = 1$, so we must have that $N(u) = N(v) = 1$. This implies the units are ± 1 .

Claim. $2 \in R$ is an irreducible element

Proof. If $2 = ab$ then $N(2) = 4 = N(a)N(b)$. But no element in R has norm of 2. Therefore either a or b has norm 1, which means either a or b is a unit. \square

A similar calculation shows that $3, 1 \pm \sqrt{-5}$ are all also irreducible. But are they prime?

Observe that $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3$

Claim. 2 does not divide $1 \pm \sqrt{-5}$

Proof. If it did then $N(2) \mid N(1 \pm \sqrt{-5})$ but $N(2) = 4$ and $N(1 \pm \sqrt{-5}) = 6$ but $4 \nmid 6$ so 2 is no longer a prime in $\mathbb{Z}[\sqrt{-5}]$.

In this same example, we see unique factorisation of 6 no longer holds.

Definition. An integral domain R is called a *Euclidean domain* if there exists a Euclidean function $\varphi : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that:

- (i) $\varphi(ab) \geq \varphi(b)$ for all $a, b \neq 0$.
- (ii) If $a, b \in R$ with $b \neq 0$, then there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

This definition is just saying we can run the Euclidean algorithm (or some equivalent form of it) on the ring.

We've already seen \mathbb{Z} is an integral domain where $\varphi(x) = |x|$. Also seen, that if we take K a field, then $K[X]$ is a Euclidean domain with a Euclidean function given by the degree of the polynomial.

Now take $R = \mathbb{Z}[i] \leq \mathbb{C}$ (Gaussian integers). This is a Euclidean domain with Euclidean function $\varphi(z) = |z|^2$

Claim. φ is a Euclidean function of R

Proof. The first requirement is obvious. For the second requirement, consider $a, b \in \mathbb{Z}[i]$, with $b \neq 0$. Consider the ratio $\frac{a}{b} \in \mathbb{C}$. There is a point $q \in \mathbb{Z}[i]$ that has distance at most 1 from $\frac{a}{b}$. So we have that $|\frac{a}{b} - q| < 1$. Then write $\frac{a}{b} = q + c$ where $|c| < 1$. Then we have that $a = bq + bc$, now set $r = bc$. We know that $r = a - bq \in R$. And finally $\varphi(r) = \varphi(b)\varphi(c) < \varphi(b)$ \square

Definition. (Principal ideal domain) A ring R is a *principle ideal domain* (PID) if it is an integral domain, and every ideal is a principal ideal, i.e for all $I \triangleleft R$, there is some a such that $I = (a)$.

Proposition. Every Euclidean domain is a principal ideal domain.

Proof. Identical to the case of \mathbb{Z} just with a general Euclidean function φ instead of $|x|$.

$\mathbb{Z}, \mathbb{R}[X], \mathbb{C}[X], \mathbb{Z}[i]$ are all examples of PIDs.

For a non-example we have $R = \mathbb{Z}[X]$ and let $I = (2, X)$. Suppose that I is principal, so $I = (f)$, hence $2 \in (f)$. So we have that $2 = fg$ for some $g \in R$. Hence we have that f is of degree zero,

so $f \in \{\pm 1, \pm 2\}$. But we can't have $f = \pm 1$ since ± 1 are units in $\mathbb{Z}[X]$ (since $(2, X) \neq R$). But now since $X \in (f)$ we must have that $\pm 2 \mid X$ which is false, hence $(2, X)$ is not a principal ideal.

Similarly $\mathbb{C}[X, Y]$, $K[X_1, \dots, X_n]$, $n \geq 2$ are not PIDs

Definition. (Unique factorisation domain) An integral domain R is a *unique factorisation domain* (UFD) if:

- (i) Every non-unit in R can be written as a product of irreducibles.
- (ii) If $p_1 \dots p_n = q_1 \dots q_m$, where p_i, q_i are irreducible, then $n = m$ and up to reordering p_i are q_i are associates.

Now we aim to show that $\text{PID} \implies \text{UFD}$.

Lemma. In a PID, any irreducible element is also prime.

Proof. Let R be a PID and $p \in R$ irreducible. Suppose $p \mid ab$ and $p \nmid a$ then we need to show that $p \mid b$. Let's consider the ideal (p, a) . This is principal so $(p, a) = (d)$ for some $d \in R$. So we must have that $d \mid p$ and $d \mid a$. So we have that $p = q_1 d$ so since p is irreducible we know that either d or q_1 is a unit. If q_1 is a unit, then $d = q_1^{-1} p$ and this divides a so we have that $a = q_1^{-1} p x$ which is a contradiction since $p \nmid a$. So we have that d is a unit, so $1_R \in (p, a)$ so we can write $1_R = rp + sa$ for some $r, s \in R$, so $b = rpb + sab$. But now we can see that ab is divisible by p so b is divisible by p . \square

Lemma. (PIDs are Noetherian) Let R be a PID. If $I_1 \subseteq I_2 \subseteq \dots$ ideals in R then for some $N \in \mathbb{Z}_{>0}$, we have for all $n \geq N$, $I_n = I_{n+1}$.

Proof. Consider $I = \bigcup_i I_i$. This is an ideal and $I \triangleleft R$ so $I = (a)$ for some $a \in R$. But $a \in I_N$ for some N , so the result follows. \square

Theorem. Let R be a principal ideal domain. Then R is a unique factorisation domain.

Proof. First we show that any $r \in R$ is a product of irreducibles. If r is irreducible, we're done. If not, we can write $r = r_1 s_1$ where either r_1 or s_1 are units. If both are products of irreducibles, then we're done. We can therefore assume by relabeling that r_1 is not a product of irreducibles. So we can write $r_1 = r_2 s_2$ with r_2, s_2 not units. Again without loss of generality we suppose that r_2 cannot be factored as a product of irreducibles. We continue in this way. So we can write that $(r) \subseteq (r_1) \subseteq (r_2) \subseteq \dots$. But by our lemma this chain stabilises so there is some n such that $(r_n) = (r_{n+1}) = \dots$, so we have that s_{n+1} is a unit which is a contradiction so r must be a product of irreducibles.

For uniqueness let $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ with p_i, q_i irreducibles. So in particular we have that $p_1 \mid q_1 \dots q_m$. Since p_1 is irreducible it is prime by our lemma so p_1 divides some q_i . We reorder and suppose that $p_1 \mid q_1$. So $q_1 = p_1 a$ for some a . But since q_1 is irreducible, a must be a unit so p_1 and q_1 are associates. Since R is a principal ideal domain, it is an integral domain so we can cancel p_1 to get that $p_2 p_3 \dots p_n = (aq_2) q_3 \dots q_m$. Now we can rename aq_2 as q_2 and continue as above show that p_i, q_i are associates for all i . This also shows that $n = m$ as if we had a leftover product, suppose $p_{k_1} \dots p_n = 1$ which is a contradiction since they are irreducible so a product of them cannot be a unit as that would imply that each p_i was a unit for $k+1 \leq i \leq n$. \square

Claim. Let R be a unique factorisation domain. Then every irreducible in R is prime.

If $p \in R$ is irreducible and $ab \in (p)$. Write $ab = pc$. Now compare unique factorisation so $(q_1 \dots q_r)(s_1 \dots s_k) = p(t_1 \dots t_\ell)$. So p is an associate of some q_i or s_j . So done because either a or b is p times some element so lies in (p) .

Definition. (Greatest common divisor) Let R be an integral domain and $a_1, \dots, a_n \in R$. We say that $d \in R$ is a *greatest common divisor* (GCD) of a_1, \dots, a_n if:

- (i) $d \mid a_i$ for all i .
- (ii) If $d' \mid a_i$ for all i then $d' \mid d$.

Definition. (Least common multiple) Let R be an integral domain and $a_1, \dots, a_n \in R$. We say that $m \in R$ is a *least common multiple* (LCM) of a_1, \dots, a_n if:

- (i) $a_i \mid m$ for all i .
- (ii) If $a_i \mid m'$ for all i then $m \mid m'$.

Theorem. Let R be a unique factorisation domain. Then gcd's and lcm's exist and are unique up to associates.

Proof. Let $a_1, \dots, a_n \in R$. Let p_1, \dots, p_n be list of all irreducible factors of the a_i and no two are associates of each other. So we can write

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

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

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

and set

$$d = \prod_{i=1}^m p_i^{m_i}.$$

So clearly, for all i we have that $d \mid a_i$. Suppose we have some $d' \mid a_i, \forall i$, can set write d' as

$$d' = v \prod_{j=1}^n p_j^{t_j},$$

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

Now uniqueness up to associates follows from the fact that any two greatest common divisors must divide each other by definition, hence they must be associates. The argument for least common multiples is similar. \square

We've created a lot of 'special' types of rings, so to make this section clearer use the following class inclusion.

rings \supset integral domains \supset unique factorisation domains \supset principal ideal domains \supset Euclidean domains \supset fields

It should be very obvious why fields are Euclidean domains.

2.5 Factorisation in polynomial rings

Recall that, for F a field, $F[X]$ is a Euclidean domain. Hence it is also a principal ideal domain and therefore a unique factorisation domain. This gives a few consequences.

- (i) If $I \triangleleft F[X]$, then $I = (f)$ for some $f \in F[X]$.
- (ii) If $f \in F[X]$, then f is irreducible if and only if f is prime.
- (iii) If f is irreducible suppose $(f) \subseteq J \subseteq F[X]$. Then $J = (g)$ for some $g \in F[X]$. Since $(f) \subseteq (g)$ we must have that $f = gh$. But since f is irreducible, either g or h is a unit. If h is a unit, then $(f) = (g)$ and if g is a unit, then $J = F[X]$ so (f) is a maximal ideal.
- (iv) $J \triangleleft F[X]$ is a non-zero prime ideal if and only if it is a maximal ideal. We've seen that maximal ideals implies prime ideals, so conversely suppose (f) is a prime ideal, non-zero. Hence f is prime and therefore irreducible so be the previous point (f) is maximal.
- (v) Finally we have that $f \in F[X]$ is irreducible if and only if $F[X]/(f)$ is a field.

We have that $X^2 + 1$ is irreducible in $\mathbb{R}[X]$. Hence we have that $\frac{\mathbb{R}[X]}{X^2+1} \cong \mathbb{C}$.

Definition. (Content) Let R be a unique factorisation domain and let $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. We define the *content* as

$$c(f) = \gcd(a_0, \dots, a_n) \in R.$$

Since the gcd is only defined up to a unit, so is the content.

Definition. (Primitive polynomials) A polynomial is called *primitive* if $c(g)$ is a unit.

Now we want to introduce Gauss' Lemma which provides an equivalency for reducibility using the field of fractions of a unique factorisation domain. But before that we require some preparation.

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

Proof. Let

$$\begin{aligned} f &= a_0 + a_1X + \dots + a_nX^n \\ g &= b_0 + b_1X + \dots + b_mX^m \end{aligned}$$

be primitive, with $a_n, b_m \neq 0$. Suppose for contradiction, $c(fg)$ is not a unit. Since R is a UFD, we can find irreducible $p \in R$ which divides $c(fg)$. By assumption, $c(g)$ and $c(f)$ are units, so $p \nmid c(g)$, $p \nmid c(f)$. Let k be minimal such that $p \nmid a_k$ and let ℓ be minimal such that $p \nmid b_\ell$. Consider the coefficient of $X^{k+\ell}$ in fg , given by

$$\sum_{i+j=k+\ell} a_i b_j.$$

Since $p \mid c(fg)$ we have that

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

However $p \mid a_{k+\ell}b_0 + \dots a_{k+1}b_{\ell-1}$ and $p \mid a_{k-1}b_{\ell+1} + \dots a_0b_{\ell+k}$, therefore $p \mid a_k b_\ell$ so either $p \mid a_k$ or $p \mid b_\ell$ which in either case is a contradiction, so $c(fg)$ is a unit. \square

Corollary. Let R be a unique factorisation domain. Then for $f, g \in R[X]$, $c(fg)$ is an associate of $c(f)c(g)$.

Proof. Write $f = c(f)f_1$ and $g = c(g)g_1$ so we have that f_1, g_1 are primitive. Then

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

so therefore $c(fg) = c(f)c(g)c(f_1g_1)$ and $c(f_1g_1)$ is a unit so they are associates.

Finally we can now prove Gauss' lemma.

Lemma. (Gauss' lemma) Let R be a unique factorisation domain with F its field of fractions. Let $f \in R[X]$ be primitive. Then f is reducible in $R[X]$ if and only if f is reducible in $F[X]$.

Proof. First for the forwards direction, let $f = gh$ be a product in $R[X]$ with g, h not units. Since f is primitive so are g and h . So both have non-zero degree hence they are not units. So f is reducible in $F[X]$.

For the other direct let $f = gh$ in $F[X]$ with g and h not units. So we can clear denominators so we pick $a, b \in R$ such that $ag, bh \in R[X]$. then we have that $abf = (ag)(bh)$.

Let

$$\begin{aligned} ag &= c(ag)g_1, \\ bh &= c(bh)h_1, \end{aligned}$$

where g_1 and h_1 are primitive. So $ab = uc(abf) = uc((ag)(bh)) = u'c(ag)c(bh)$. But $abf = c(ag)(bh)g_1h_1 = u^{-1}abg_1h_1$, since we're in a integral domain we can cancel ab to get $f = u^{-1}g_1h_1 \in R[X]$. So f is reducible in $R[X]$. \square

Now for an example. Consider $f = X^3 + X + 1 \in \mathbb{Z}[X]$. We can see that $c(f) = 1$ so f is primitive. Suppose for contradiction that f is reducible in $\mathbb{Q}[X]$. So by Gauss' lemma, f is reducible in $\mathbb{Z}[X]$, so $X^3 + X + 1 = gh$ where $g, h \in \mathbb{Z}[X]$ not units. Hence $\deg(g), \deg(h) \geq 1$. Since $\deg(f) = 3 = \deg(g) + \deg(h)$, suppose that $\deg(g) = 1$ and $\deg(h) = 2$. Hence let $g = b_0 + b_1X$ and let $h = c_0 + c_1X + c_2X^2$. Multiplying out and equating coefficients we get that $b_0c_0 = 1$ and $c_2b_1 = 1$. Hence b_0, b_1 must be ± 1 , so we must have that g is either $1 \pm X$ or $-1 \pm X$. Hence ± 1 is a root of g which is a contradiction since f does not have a root of ± 1 . So f is not reducible in $\mathbb{Q}[X]$, hence it has no root in \mathbb{Q} and we have that $\mathbb{Q}[X]/(X^3 + X + 1)$ is a field.

Proposition. Let R be a unique factorisation domain and F its field of fractions. Let $g \in R[X]$ be primitive. Then a polynomial $f \in R[X]$ is divisible by g in $R[X]$ if and only if it is divisible by g in $F[X]$. Or in other words if $J = (g) \triangleleft R[X]$ and $I = (g) \triangleleft F[X]$ then $J = I \cap R[X]$.

Proof. We'll prove the second formulation. Certainly we have that $J \subseteq I \cap R[X]$. So let $f \in I \cap R[X]$. So we can write

$$f = gh \quad \text{with } h \in F[X]$$

Now we clear denominators by choosing $b \in R$ such that $bh \in R[X]$. We know by multiplying by b so that $bf = g(bh)$. We let $(bh) = c(bh)h_1$ where h_1 is primitive and $h_1 \in R[X]$. So $bf = c(bh)gh_1$, but g and h_1 are both primitive, so gh_1 is also primitive. So $c(bh) = c(bf)u$ where u is a unit. Since bf is a product in $R[X]$

$$c(bf) = c(b)c(f) = b \cdot c(f)$$

This gives that $bf = ub \cdot c(f)gh_1$ so cancelling b gives that f is divisible by g . \square

Theorem. If R is a unique factorisation domain, then $R[X]$ is also a unique factorisation domain.

Proof. First we prove that factorisations exist. Let $f \in R[X]$. We can write $f = c(f)f_1$ where f_1 is primitive. Since F is a UFD, factorise $c(f)$ as $p_1 \dots p_n$ for $p_i \in R$ irreducible. Now we deal with f_1 . If f_1 is not irreducible then write $f_1 = f_2f_3$ where f_2, f_3 are not units. Since f_1 is primitive neither f_2 nor f_3 can be constant. So $\deg(f_2), \deg(f_3) > 0$ and also $\deg(f_1) = \deg(f_2) + \deg(f_3)$ using the fact that we're working in an integral domain (*think!*). Induct on the degree, if f_2 and f_3 are irreducible, we're done otherwise repeat the same steps until the process terminates, which will happen in finitely many steps since the degree is strictly decreasing. Putting this together we can write $f = p_1 \dots p_n q_1 \dots q_m$ all irreducibles.

Now for uniqueness. First we deal with the p 's. The content has a unique factorisation $c(f) = p_1 \dots p_n$. So cancelling the content suffices to show uniqueness of factorisation for $f_1 = q_1 \dots q_m$. Suppose $f_1 = q_1 \dots q_m = r_1 \dots r_\ell$ are two factorisations in $R[X]$. Viewing this in $F[X]$, where F is the fraction field of R , since $F[X]$ is a Euclidean domain, we know that $\ell = m$ and up to reordering q_i and r_i are associates in $F[X]$. So $q_i \mid r_i$ and $r_i \mid q_i$ in $F[X]$. But from the previous proposition we get the same statement in $R[X]$ \square

This gives us that rings such as $\mathbb{Z}[X]$ and $\mathbb{C}[X, Y]$ are not principal ideal domains, but they are unique factorisation domains.

Theorem. (Eisenstein's criterion) Let R be a unique factorisation domain and

$$f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \in R[X]$$

is primitive, with $a_n \neq 0$. Let $p \in R$ be irreducible such that

- (i) $p \nmid a_n$.
- (ii) $p \mid a_i$ for $0 \leq i \leq n-1$.
- (iii) $p^2 \nmid a_0$.

Then f is irreducible in $R[X]$.

Proof. Suppose we have $f = gh$, with $g = r_0 + r_1X + \dots + r_kX^k$ and $h = s_0 + s_1X + \dots + s_\ell X^\ell$ and $r_k, s_\ell \neq 0$. We know that and since $p \nmid a_n$ it does not divide r_k nor s_ℓ . Similarly $r_0s_0 = a_0$ and $p^2 \nmid a_0$ so p divides exactly one of r_0 and s_0 . Let assume $p \mid r_0$ so $p \nmid s_0$. Let j be the index such that

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

Consider a_j . We know $a_j = r_0s_j + r_1s_{j-1} + \dots + r_{j-1}s_1 + r_js_0$. We know that $p \mid r_0s_j + \dots + r_{j-1}s_1$, also $p \nmid r_j$ and $p \nmid s_0$, because p is prime, $p \nmid a_j$. So we must have that $j = n$. We also have that

$j \leq k \leq n$, so $j = k = n$. Hence $\deg g = n$ and $\deg h = 0$. Since f is primitive we must have that h is a unit, so this is not a proper factorisation. Hence f is irreducible in $R[X]$. \square

For an example consider the polynomial $X^n - p \in \mathbb{Z}[X]$ with p prime. Apply Eisenstein's criterion with $p \in \mathbb{Z}$ and observe all the conditions hold. This is certainly primitive, since this is monic. So $X^n - p$ is irreducible in $\mathbb{Z}[X]$, hence it is also irreducible in the fraction field polynomial, namely $\mathbb{Q}[X]$. In particular $X^n - p$ has no rational roots, so $\sqrt[n]{p}$ is irrational.

Next, consider $f = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X]$ for p prime. See that we can write f as

$$f = \frac{X^p - 1}{X - 1}.$$

So perchance we should write $Y = X - 1$. Then we get a new polynomial

$$\hat{f}(Y) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1}Y^{p-2} + \dots + \binom{p}{p-1}.$$

So now we can apply Eisenstein's criterion so \hat{f} . So \hat{f} is irreducible in $\mathbb{Z}[X]$. If we had a factorisation $f(X) = g(X)h(X) \implies \hat{f}(Y) = g(Y+1)h(Y+1)$, but we know that \hat{f} cannot be factorised, so f is irreducible.

2.6 Gaussian integers

This is the ring $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \leq \mathbb{C}$ and we have the usual norm $N(a + ib) = a^2 + b^2$ which helpfully is a Euclidean function. This implies that $\mathbb{Z}[i]$ is a Euclidean domain, hence it is a principal ideal domain and therefore a unique factorisation domain. So irreducible and prime are the same in the Gaussian integers. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$ which are exactly the norm 1 elements.

We make the following observations.

- (i) We have $2 = (1 + i)(1 - i)$ so 2 is not a prime.
- (ii) Similarly $5 = (1 + 2i)(1 - 2i)$ so also not a prime.
- (iii) We claim that 3 is a prime in $\mathbb{Z}[i]$. The norm of 3 is 9 so if $3 = uv$ then either $N(u)$ or $N(v)$ is 1 (so one is a unit) or $N(u) = N(v) = 3$. But if $u = a + bi$ then we'd need $a^2 + b^2 = 3$ which has no solutions for $a, b \in \mathbb{Z}$. So one of u or v is a unit, hence 3 is prime.

So what are the primes in $\mathbb{Z}[i]$?

Proposition. A prime number $p \in \mathbb{Z}$ remains prime when viewed 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 in $\mathbb{Z}[i]$ we can write $p = (a + bi)(a - bi)$ so p is not irreducible and hence not prime.

Conversely suppose $p = uv$ is a product of non-units in $\mathbb{Z}[i]$ then $p^2 = N(u)N(v)$. Since u and v are non-units then $N(u) = N(v) = p$. Write $u = a + bi$. Then we have that $a^2 + b^2 = p$. \square

Now we want to classify all of the primes in $\mathbb{Z}[i]$. But before that we need a lemma.

Lemma. Let p be a prime number. Then the group \mathbb{F}_p^\times of non-zero elements $\pmod p$ under multiplication is a cyclic group. So $\mathbb{F}_p^\times \cong C_{p-1}$.

Proof. Certainly \mathbb{F}_p^\times is finite abelian. By the classification of finite abelian groups, if \mathbb{F}_p^\times is not cyclic then it contains $C_m \times C_m$ as a subgroup for some $m > 1$. This means there are at least m^2 elements $x \in \mathbb{F}_p^\times$ satisfying $x^m - 1 = 0$. But a polynomial with coefficients in \mathbb{F}_p has number of solutions bounded above by the degree, which is a contradiction. \square

Now let's prove the theorem.

Theorem. (Classification of primes in $\mathbb{Z}[i]$) The primes in $\mathbb{Z}[i]$ up to associates are exactly
 (i) The primes $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod 4$.
 (ii) Gaussian integers $z \in \mathbb{Z}[i]$ with $N(z) = p$ where p is a prime that is either 2 or 1 $\pmod 4$.

Proof. Firstly we prove the two types of Gaussian integers are prime. If $p \in \mathbb{Z}$ is 3 $\pmod 4$ then $p \neq a^2 + b^2$ for $a, b \in \mathbb{Z} \setminus \{0\}$ (by arithmetic) so by our proposition these are primes in $\mathbb{Z}[i]$. Now for $z \in \mathbb{Z}[i]$ if $N(z) = p$, with p prime congruent to 2 or 1 $\pmod 4$, we'll show that z is irreducible. Write $z = uv$ in $\mathbb{Z}[i]$, then $p = N(z) = N(u)N(v)$ in $\mathbb{Z}_{\geq 0}$. So either $N(u)$ or $N(v)$ is 1 so u or v is a unit, so z is irreducible hence prime.

Now we show all primes in $\mathbb{Z}[i]$ are of this form. Let $z \in \mathbb{Z}[i]$ be prime. Observe that $N(z) = z\bar{z}$ is a factorisation of $N(z)$ viewed inside $\mathbb{Z}[i]$ into irreducibles. Let p be a prime number that divides $N(z)$ in $\mathbb{Z}_{\geq 0}$. Suppose $p \equiv 3 \pmod 4$ so p is prime in $\mathbb{Z}[i]$. So $p = z\bar{z}$ hence $p \mid z$ or $p \mid \bar{z}$ therefore because z is conjugate to \bar{z} so $p \mid z$ and $p \mid \bar{z}$. But then $p = z$ up to associates. Now assume that $p \equiv 2$ or 1 $\pmod 4$. The $p \equiv 2 \pmod 4$ case can be worked out by hand, so assume $p = 4k + 1$ for $k \in \mathbb{Z}$. By the lemma we know that $\mathbb{F}_p^\times \cong C_{4k}$. There is a unique order 2 element here (which is -1). If $a \in \mathbb{F}_p^\times$ is order 4, then we have $a^2 \equiv -1 \pmod p$. So p divides $(a + i)(a - i)$ but not $a + i$ or $a - i$ individually. So p is not irreducible in $\mathbb{Z}[i]$. So now we can write $p = z_1 z_2$ non-units. Taking the norm we get that $N(p) = p^2 = N(z_1)N(z_2)$. Because these are non-units, we must have that $N(z_1) = N(z_2) = p$. So $\bar{z}_1 = z_2$. Finally we have that $p = z_1 \bar{z}_1 \mid N(z) = z\bar{z}$ all of z, \bar{z} are irreducible so z, z_1 or z, \bar{z}_1 are associates. Hence $N(z) = p$. \square

Corollary. An non-negative integer n can be written as a sum of two squares if and only if when we write n as a product of distinct primes,

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

$p_i \equiv 3 \pmod 4$ implies that n_i is even.

Proof. If $n = x^2 + y^2$ we have that $n = N(z)$ where $z = x + iy \in \mathbb{Z}[i]$. Factorise z into primes, $z = \alpha_1 \cdots \alpha_q$. Either α_i is a prime number in \mathbb{Z} that is 3 $\pmod 4$ or it has norm p where p is 2 or 1 $\pmod 4$. Taking norms we get that $n = x^2 + y^2 = N(z) = N(\prod \alpha_i) = \prod N(\alpha_i)$. Each factor is this product is either p^2 or $p \equiv 3 \pmod 4$ or p with $p = 2$ or $p \equiv 1 \pmod 4$. For the converse let $n = p_1^{n_1} \cdots p_k^{n_k}$ satisfying hypothesis given. Now we know that $p_i = N(\alpha_i)$ if $p_i \equiv 3 \pmod 4$, $p_i^{n_i} = N(p_i)^{\frac{n_i}{2}}$ otherwise $p_i = 2$ or $p_i = 1 \pmod 4$ so $p_i = N(\alpha_i)$ for some α_i so $p_i^{n_i} = N(\alpha_i^{n_i})$ so write n as $N(z)$ in this way. \square

2.7 Algebraic integers

Definition. (Algebraic integer) A complex number $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial in $\mathbb{Z}[X]$.

For a piece of notation we write $\mathbb{Z}[\alpha] \leq \mathbb{C}$ for an algebraic integer α , as the smallest subring containing α so

$$\mathbb{Z}[\alpha] = \bigcap_{\substack{R \leq \mathbb{C} \\ \alpha \in R}} R.$$

Or equivalently $\mathbb{Z}[\alpha]$ is the image of $e_\alpha : \mathbb{Z}[X] \rightarrow \mathbb{C}$ given by $g \rightarrow g(\alpha)$

Proposition. Let $\alpha \in \mathbb{C}$ be an algebraic integer. The ideal $I = \ker(e_\alpha) \triangleleft \mathbb{Z}[X]$ is principal, and $I = (f_\alpha)$ with f_α monic and irreducible.

Recall that $\mathbb{Z}[X]$ is not a principal ideal domain, so this proposition is not trivial.

From our proposition we can use the following definition.

Definition. (Minimal polynomial) The *minimal polynomial* of an algebraic integer α is the irreducible monic f_α such that $(f_\alpha) = \ker(e_\alpha)$.

Now for the proof of the proposition

Proof. By definition $I = \ker e_\alpha$ is non-zero. Take $f_\alpha \in I$ of minimal degree. We can assume f_α is primitive (since monic). Now we aim to show that $I = (f_\alpha)$. Let $h \in I$. In $\mathbb{Q}[X]$ we have the Euclidean algorithm so we can write $h = f_\alpha q + r$ with $r = 0$ or $\deg r < \deg f_\alpha$. Now clearing denominators so for some $a \in \mathbb{Z}$ we get that $ah = f_\alpha(aq) + (ar)$. Now plugging in α we get that

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

Since that $f_\alpha, h \in I$ we get that $f_\alpha(\alpha) = h(\alpha) = 0$, so we have that $ar(\alpha) = 0$. So $(ar) \in I$. But since we have that $f_\alpha \in I$ has minimal degree, and $\deg(r) = \deg(ar)$ we must have that $r = 0$. So we know that $ah = f_\alpha \cdot (aq)$. This almost what we want, we just need to factorise h instead of ah . Taking the contents we know that $c(f_\alpha)$ is a unit so $c(ah) = c(aq)$, so $a \mid c(aq)$. Therefore $aq = a\bar{q}$ for $\bar{q} \in \mathbb{Z}[X]$. So this means that $q = \bar{q} \in \mathbb{Z}[X]$. So we know that $h = f_\alpha q \in (f_\alpha)$. Hence $I = (f_\alpha)$.

Now we're left to show that f_α is irreducible. We know that

$$\frac{\mathbb{Z}[X]}{(f_\alpha)} \cong \text{im}(e_\alpha) \leq \mathbb{C}.$$

But since \mathbb{C} is an integral domain all of its subrings are integral domains, so $\mathbb{Z}[X]/(f_\alpha)$ is an integral domain, so (f_α) is prime hence f_α is prime, so it's irreducible. \square

We have plenty of examples of algebraic integers.

- (i) $\alpha = i$ is an algebraic integer with $f_\alpha = X^2 + 1$.
- (ii) $\alpha = \frac{1}{2}(1 + \sqrt{-3})$ is an algebraic integer with $f_\alpha = X^2 - X + 1$.

- (iii) The monic polynomial $X^5 - X + d$ with $d \in \mathbb{Z}_{\geq 1}$ has exactly one real root which is an algebraic integer.

Theorem. The real root of $X^5 - X + d$ cannot be written using integers and the operations $\times, +, -, \sqrt[n]{}, \nabla$.

Proof. II Galois Theory

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

Proof. Let f_α be the minimal polynomial of α irreducible. So by Gauss' lemma we have that the polynomial is also irreducible in $\mathbb{Q}[X]$. But $(X - \alpha)$ divides it in $\mathbb{Q}[X]$ so $f_\alpha = (X - \alpha)$ hence $\alpha \in \mathbb{Z}$.

It should be noted that the set of algebraic integers form a ring, but this is not obvious and will be proved later.

2.8 Hilbert's basis theorem

Definition. (Noetherian ring). A ring is *Noetherian* if for any chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

then there is some N such that $I_N = I_{N+1} = \cdots$. This is known as the *ascending chain condition* (ACC).

Definition. (Finitely generated ideal) An ideal $I \triangleleft R$ is finitely generated if it can be written as $I = (r_1, \dots, r_n)$ for some $r_1, \dots, r_n \in R$.

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

Proof. Suppose all ideals are finitely generated. Given the chain $I_1 \subseteq I_2 \subseteq \cdots$ Consider

$$I = \bigcap_{j=1}^{\infty} I_j.$$

I is an ideal (Example Sheet 2) so we know that I is finitely generated, so $I = (r_1, \dots, r_n)$ with $r_i \in I_{k_i}$. So let

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

Then we have that $r_1, \dots, r_n \in I_K$, so $I_K = I = I_{K+1} = \cdots$ so R is Noetherian.

For the converse if I is not finitely generated, pick $r_1 \in I$ such that $I \neq (r_1)$. Pick $r_2 \in I \setminus (r_1)$ such that $(r_1, r_2) \neq I$, and so on to get $(r_1) \subseteq (r_1, r_2) \subseteq \cdots$ strictly increasing so R is not Noetherian. \square

Theorem. (Hilbert's basis theorem) Let R be a Noetherian ring. Then $R[X]$ is also Noetherian.

Proof. Let $J \triangleleft R[X]$ be an ideal. Let $f_1 \in J$ have minimal degree. If $J \neq (f_1)$ pick $f_2 \in J \setminus (f_1)$ of minimal degree, and so on. If $J = (f_1, \dots, f_k)$ then we're done so suppose for contradiction we don't get this. Let a_i be the leading coefficient of f_i . The chain $(a_1) \subseteq (a_1, a_2) \subseteq \dots$ stabilises by ACC for R . So for some m we have that $(a_1, a_2, \dots, a_m) = (a_1, a_2, \dots)$. Now we let

$$a_{m+1} = \sum_{i=1}^m a_i b_i$$

and consider the polynomial

$$g = \sum_{i=1}^m b_i f_i X^{\deg f_{m+1} - \deg f_i}.$$

This has the same degree and leading coefficient as f_{m+1} . Then $f_{m+1} - g$ has smaller degree and lies in J , but not in (f_1, \dots, f_m) . This contradicts minimality of $\deg f_{m+1}$. So the process must terminate, hence $R[X]$ is Noetherian. \square

We also have that $R[[X]]$ is Noetherian

Corollary. $\mathbb{Z}[X_1, X_2, \dots, X_n]$ is Noetherian, and for F a field $F[X_1, X_2, \dots, X_n]$ is Noetherian.

Proof. Let $J \triangleleft \frac{R}{I}$ and let $J' \triangleleft R$ be the corresponding ideal in R . If J' is generated by r_1, \dots, r_m then J is generated by $(r_1 + I), \dots, (r_m + I)$. \square

In fact all finitely-generated rings is a quotient of some $\mathbb{Z}[X_1, \dots, X_n]$ giving the final corollary of this section.

Corollary. All finitely-generated rings are Noetherian.

Proof. Obvious \square

3 Modules

3.1 Definitions and examples

An example of a module is a vector space over a field K . (Recall a vector space is an abelian group V with a 'scaling', $K \times V \rightarrow V$.)

Another example is that if A is any abelian group, we can think of $\mathbb{Z} \times A \rightarrow A$ sending $(n, a) \rightarrow \underbrace{a + a + \dots + a}_{n \text{ times}}$

Definition. (R -module) Let R be a commutative ring. Then a quadruple $(M, +, 0_M, \circ)$ is an R -module if

- (i) $(M, +, 0_M)$ is an abelian group.
- (ii) $\circ : R \times M \rightarrow M$ satisfies

- (a) $(r_1 + r_2) \circ m = r_1 m + r_2 m$;
 - (b) $r \circ (m_1 + m_2) = (r \circ m_1) + (r \circ m_2)$;
 - (c) $r_1 \circ (r_2 \circ m) = (r_1 \circ r_2) \circ m$; and
 - (d) $1_R \circ M = m$.
- for all $m_1, m_2, m \in M$ and $r_1, r_2, r \in R$.

If $R = K$ is a field, then an R -module is a K -vector space. Any abelian group is naturally a \mathbb{Z} -module.

For any R the self product $R^m = \underbrace{R \times \cdots \times R}_{m \text{ times}}$ is an R -module via $R \times R^m \rightarrow R^m$ given by $(r, r_1, \dots, r_m) \rightarrow (rr_1, \dots, rr_m)$.

If $I \triangleleft R$ then I is an R -module via multiplication.

Similarly the group R/I is also an R -module via $R \times R/I \rightarrow R/I$ given by $(r, s + I) \rightarrow (rs + I)$.

Let V be a K -vector space and let $\alpha \in \text{End}(V)$ so α is a linear map. We can give V the structure of a module over $K[X]$ by

$$\begin{aligned} K[X] \times V &\rightarrow V \\ (f, v) &\rightarrow f(\alpha)(v) \end{aligned}$$

giving a $K[X]$ -module.

Another important example. Let $\varphi : R \rightarrow S$ be a ring homomorphism and let M be an S -module. We can turn M into an R -module via:

$$\begin{aligned} R \times M &\rightarrow M \\ (r, m) &\rightarrow \varphi(r)m. \end{aligned}$$

In particular this turns S into an R -module.

Definition. (Submodule) Let M be an R -module. A subgroup $N \subseteq M$ is an R -submodule if for every $n \in N$ and $r \in R$, we have $rn \in N$. We write $N \leq M$.

For a non-example \mathbb{R}^n is an \mathbb{R} -vector space hence it is an \mathbb{R} -module. But \mathbb{Q}^n is not a \mathbb{R} -submodule because it's not closed under the scaling operation.

If $R = K$ then a K -submodule of V is just a K -vector subspace.

Definition. (Quotient module) Let $N \leq M$ be an R -module. The *quotient module* is the group M/N equipped with

$$\begin{aligned} R \times M/N &\rightarrow M/N \\ (r, m + N) &\rightarrow (rm + N). \end{aligned}$$

It can be seen that this is well defined and itself an R -module.

Definition. Let M, N be R -modules. An R -module homomorphism is group homomorphism $\varphi : M \rightarrow N$ such that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$

Definition. (Isomorphism) An *isomorphism* of R -modules is a bijective homomorphism. We say that the modules are *isomorphic*.

Again we have the isomorphism theorems and a correspondence theorem for modules.

Theorem. (First isomorphism theorem) Let $\varphi : M \rightarrow N$ be a homomorphism of R -modules. Then

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

is a submodule of M . The image

$$\operatorname{im} \varphi = \{\varphi(m) : m \in M\}$$

is a submodule of N . Furthermore there is an isomorphism

$$M / \ker \varphi \cong \operatorname{im} \varphi$$

Proof. Immediate from the first isomorphism theorem of groups. \square

Theorem. (Second isomorphism theorem) Let $L, K \leq M$ be R -submodules. Then

$$K + L = \{k + \ell : k \in K, \ell \in L\}$$

is an R -submodule of M . Moreover

$$\frac{K + L}{K} \cong \frac{L}{L \cap K}$$

is an isomorphism of R -modules.

Proof. Immediate from the second isomorphism theorem of groups. \square

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

$$M/L \cong \frac{M/N}{L/N}$$

is an isomorphism of R -modules.

Proof. Immediate from the third isomorphism theorem of groups. \square

Theorem. (Correspondence theorem) We have the correspondence

$$\{\text{Submodules of } M/N\} \leftrightarrow \{\text{Submodules of } M \text{ which contain } N\}.$$

Proof. Same as the correspondence theorem for groups. \square

Definition. (Annihilator) Let M be an R -module. For $m \in M$ its *annihilator* is

$$\text{Ann}(m) = \{r \in R : rm = 0\}.$$

For any set $S \subseteq M$ we define

$$\text{Ann}(S) = \{r \in R : rm = 0 \text{ for all } m \in S\} = \bigcap_{s \in S} \text{Ann}(s).$$

We observe that the annihilator of $S \subseteq M$ is an ideal in R .

Definition. (Submodule generated by an element) Let M be a R -module and $m \in M$. The submodule generated by m is

$$Rm = \{rm \in M : r \in R\}.$$

Proposition. For $m \in M$ there is an isomorphism $R/\text{Ann}(m) \cong Rm$.

Proof. Consider the function $R \rightarrow M$ sending $r \rightarrow rm$. This is clearly a R -module homomorphism, so the result follows from the first isomorphism theorem. \square

Definition. (Finite generation) An R -module M is finitely generated if there exists elements m_1, \dots, m_k such that

$$M = Rm_1 + Rm_2 + \cdots + Rm_k = \{r_1m_1 + \cdots + r_km_k : r_i \in R\}.$$

Lemma. An R -module M is finitely generated if and only if there is a surjective R -module homomorphism from $R^k \rightarrow M$.

Proof. If $M = Rm_1 + \cdots + Rm_k$ then consider

$$\begin{aligned} R^k &\rightarrow M \\ (r_1, \dots, r_k) &\rightarrow \sum r_i m_i, \end{aligned}$$

clearly surjective homomorphism. Conversely if $\varphi : R^k \rightarrow M$ is given, let $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ with a 1 in the i th position and $m_i = \varphi(e_i)$ and now we can check that m_i generates M by surjectivity. \square

Corollary. If M is finitely generated R -module and $N \leq M$ then M/N is finitely generated.

Proof. Using the previous lemma we can compose surjection $R^k \rightarrow M$ and surjection $M \rightarrow M/N$ hence we have a surjection $R^k \rightarrow M/N$. \square

However a submodule of a finitely-generated module need not be finitely-generated. For example let $R = \mathbb{C}[X_1, X_2, \dots]$. And consider the module $M = R$ so the submodule I generated by (X_1, X_2, \dots) is not finitely-generated but M is finitely-generated (by 1).

3.2 Direct sums and free modules

Now we'll slug through some definitions.

Definition. (Direct sum) Let M_1, \dots, M_k be R -modules. The *direct sum* is the abelian group $M_1 \times \dots \times M_k$ with scaling

$$\begin{aligned} R \times M_1 \times \dots \times M_k &\rightarrow M_1 \times \dots \times M_k \\ (r, m_1, \dots, m_k) &\rightarrow (rm_1, \dots, rm_k) \end{aligned}$$

We notate this as $M_1 \oplus \dots \oplus M_k$.

Definition. (Linear independence) Let $m_1, \dots, m_k \in M$. Then $\{m_1, \dots, m_k\}$ is *R-linearly independent* if

$$\sum r_i m_i = 0 \implies r_i = 0 \text{ for all } i$$

Definition. (Free generation) A subset $S \subseteq M$ *freely generates* M if

- (i) S generates M
- (ii) Any set function $f : S \rightarrow N$ with N an R -module extends to an R -module homomorphism $\varphi_f : M \rightarrow N$ with the condition $\varphi_f(s) = f(s) \quad \forall s \in S$.

Definition. (Free module and basis) A module M is *free* if it is freely generated by some subset $S \subseteq M$, and S is called a *basis*.

Now let's look at an example. Consider the \mathbb{Z} -module $\mathbb{Z}/2$. Suppose $\mathbb{Z}/2$ was generated by some $S \subseteq \mathbb{Z}/2$. This can only happen with $S = \{1\}$. Then this implies that there is a homomorphism $\varphi : \mathbb{Z}/2 \rightarrow \mathbb{Z}$ sending 1 to 1. But it does not send 0 to $1 + 1$ since $\varphi(0) = 0$. So $\mathbb{Z}/2$ is not free.

Proposition. Let $S = \{m_1, \dots, m_k\} \subseteq M$. Then the following three statements are equivalent

- (i) S generates M freely.
- (ii) S generates M and S is linearly independent.
- (iii) Every $m \in M$ is uniquely expressible as $m = r_1 m_1 + \dots + r_k m_k$.

Proof. The fact that (ii) \iff (iii) follows from IB Linear Algebra.

For the first statement, suppose that S generates M freely. If S is not linearly independent we can write

$$0 = r_1 m_1 + r_2 m_2 + \dots + r_k m_k$$

and we can assume with reordering that $r_1 \neq 0$. Consider the set function $f : S \rightarrow R$ sending $m_1 \rightarrow 1$ and $m_i \rightarrow 0$ for all $i > 1$. Now compute $0 = \varphi(0) = \varphi(\sum r_i m_i) = r_1$ which is

contradiction. For the converse assume (iii). Since every m is uniquely $m = \sum_{i=1}^k r_i m_i$. Given any set function $f : S \rightarrow N$ we define $\varphi_f : M \rightarrow N$ by

$$\varphi_f(r_1 m_1 + \cdots r_k m_k) = r_1 \varphi_f(m_1) + \cdots + r_k \varphi_f(m_k).$$

We have well-definedness by uniqueness and is clearly an R -module homomorphism. So S generates M . \square

Now take $\{2, 3\} \subseteq \mathbb{Z}$. This set generates \mathbb{Z} by Bezout's, but

$$0 = 3 \cdot 2 + (-2) \cdot 3$$

so the set does not generate \mathbb{Z} freely. But what differs from linear algebra vector spaces, is that neither 2 or 3 generate \mathbb{Z} so no it's not like a linearly independent list of elements in a vector space where we can chuck elements out to get a basis.

Definition. (Relations) Let M be finitely-generated with generators given by $\theta : R^k \rightarrow M$. Then $\ker \theta$ is called the *module of relations* of M with respect to θ .

Definition. (Finitely presented module) We say that a module is *finitely-presented* if $\ker \theta$ is finitely generated.

And for someone completely different.

Proposition. (Invariance of dimension/rank) Let R be a non-zero ring. Then if $R^n \cong R^m$ then $n = m$.

Proof. We will prove the statement by reducing to R to a field where we know the result follows.

If $I \triangleleft R$ is an ideal and M is an R -module, consider $IM = \{r \cdot m : r \in I, m \in M\} \leq M$. So we can consider M/IM as an R -module. If $r \in I$ then its action on M/IM is

$$r(m + IM) = rm + IM = 0 + IM = IM.$$

So we can make M/IM into an R/I -module by

$$(r + I) \cdot (m + IM) = r \cdot m + IM.$$

Now let $I \triangleleft R$ be a maximal ideal So we have an isomorphism $(R/I)^n \cong (R/I)^m$ of R/I -modules. Since R/I is a field we have $n = m$ by the invariance of dimension for vector spaces. \square

3.3 Matrices over Euclidean domains

For the rest of the course we'll fix a Euclidean domain R along with a Euclidean function $\varphi : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$. We know that for $a, b \in R$ we can find $x, y \in R$ such that $ax + by = \gcd(a, b)$.

Definition. (Elementary row operations) Let A be an $m \times n$ matrix with entries in R .

The *elementary row operations* are the following

(ER1) Add $c \in R$ times row i to row j

(ER2) Swap row i and row j

(ER3) Multiply the i th row by a *unit* $c \in R$.

A similarly we can do column operations in the same way.

How 'nice' can we make A ?

Definition. (Equivalent matrices) Two matrices A, B over R are equivalent if A can be obtained from B by a sequence of row and column operations. In particular

$$B = QAT^{-1}$$

for Q, T invertible.

Notice that the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ over \mathbb{Z} cannot be reduced any further.

Theorem. (Smith normal form) Any $m \times n$ matrix over R is equivalent to one of the form

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

with

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

These d_i are the *invariant factors* of A

Proof. If $A = 0$ we're done so assume that $A \neq 0$. Let A_{ij} be some non-zero entry. By row and column operations we can move this to the $(1, 1)$ position, so we can assume that $A_{11} \neq 0$. Now we have two basic moves.

(i) If A_{1j} is not divisible by A_{11} so we can write $A_{1j} = A_{11}q + r$ with $\varphi(r) < \varphi(A_{11})$. By column operations we can make the (i, j) -entry equal to r . Now swap the $(1, j)$ -entry with the $(1, 1)$ -entry. The result of this is that φ of the $(1, 1)$ entry has got smaller.

(ii) Similar move for A_{j1} . Using row operations instead of column operations.

The consequence of (i) and (ii) is that after finitely many operations the $(1, 1)$ entry divides everything in row 1 and column 1. By more operations we get the matrix of the form

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

for a $(m-1) \times (n-1)$ matrix C . Replace A with this matrix. Now suppose that A_{ij} in C is *not* divisible by d . Then

$$A_{ij} = dq + r, \quad \varphi(r) < \varphi(d).$$

Now we add column 1 to column j and subtract q times row 1 from row i . This gives r in the new (i, j) -entry. Swap again to make r the $(1, 1)$ -entry. Now we can repeat (i) and (ii) to get a matrix of the form

$$\begin{pmatrix} d' & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C' & \\ 0 & & & \end{pmatrix}$$

Where $d' = r$. By applying this finitely many times we get a matrix

$$\begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C' & \\ 0 & & & \end{pmatrix}$$

where d divides every entry in C .

Now recurse with C replacing A from the start of the proof. Then the output matrix is as claimed. \square

Remark. However we haven't shown the invariant factors are well-defined.

Recall for a matrix A a $k \times k$ minor is the determinant of a $k \times k$ submatrix.

Definition. (Fitting ideals) For A a matrix over R , the k th *fitting ideal* is the ideal

$$\text{Fit}_k(A) \triangleleft R$$

generated by the $k \times k$ minors of A .

Proposition. If A and B are equivalent matrices then

$$\text{Fit}_k(A) = \text{Fit}_k(B), \quad \forall k.$$

Proof. We'll check that $\text{Fit}_k(A)$ is unchanged by row and column operations. Since $\text{Fit}_k(A) = \text{Fit}_k(A^T)$ it suffices to check row operations. Consider C a $k \times k$ -submatrix of A . Consider adding c times row i to row j .

- (i) If both rows lie inside C then the minor is unchanged by properties of the determinant.
- (ii) If the j th row is outside C then C is unchanged obviously.
- (iii) Suppose the j th row in C and the i th row is not. If row i is $[f_1, \dots, f_k]$ then the new row i is $[C_{j1} + cf_1, \dots, C_{jk} + cf_k]$. Now computing the determinant of this new submatrix along this row. So

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

where D is obtained from C by replacing row j with $[f_1, \dots, f_k]$ But D is a $k \times k$ submatrix of A so we're done since ideals are closed under addition and multiplication.

The remaining operations are straightforward to check. We conclude that $\text{Fit}_k(A) \subseteq \text{Fit}_k(B)$ and since all row operations are invertible we have that $\text{Fit}_k(A) = \text{Fit}_k(B)$ \square

Corollary. If A has Smith normal form then

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

Proof. Trivial □

Proposition. Let R be a principal ideal domain. Any submodule of R^m can be generated by m or fewer elements.

Proof. We will induct on m since the $m = 1$ case is the definition of a PID. Let $N \leq R^m$. Consider $I = \{r \in R : (r, r_2, \dots, r_m) \in N \text{ for some } r_2, \dots, r_m \in R\}$. Certainly this is an ideal so $I \triangleleft R$. Since R is a PID we have that I is generated by a single element (a) . Choose $n = (a, a_2, \dots, a_m) \in N$. for $(r_1, \dots, r_m) \in N$ we know that $a \mid r_1$. So $(r_1, \dots, r_m) - rn = (0, r_2 - ra_2, \dots, r_m - ra_m)$. So everything in N is a multiple of n plus something in $N \cap (\{0\} \times R^{m-1}) \leq R^{m-1}$. Now induct. □

Theorem. Let R be a Euclidean domain. $N \leq R^m$. There exists a basis v_1, \dots, v_m for R^m such that N is generated by $d_1 v_1, \dots, d_r v_r$ for some $0 \leq r \leq m$, $d_i \in R$ such that $d_i \mid d_{i+1}$.

Proof. By the previous proposition we have that N is generated by x_1, \dots, x_n with $n \leq m$. Viewing this as a matrix with x_i as the i th column. Putting this into Smith normal form we note that row operations change the basis for R^m and column operations for N . The matrix has the form

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

So in this new basis N is generated by $\{d_i v_i\}_{i=1}^r$. □

Theorem. If R is a Euclidean domain, then any submodule of R^m is free.

Proof. In the proof of the previous theorem we have a generating set $d_1 v_1, \dots, d_r v_r$. Any linear dependence between $\{d_i v_i\}$ gives a linear dependence between the v_i 's themselves, but $\{v_i\}$ is a basis so it's linear independent. □

Theorem. Let R be a Euclidean domain. Let M be a finitely generated R -module. Then

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

where $d_i \neq 0$ and $d_i \mid d_{i+1}$.

Remark. If $R = \mathbb{Z}$ and M is finite we recover the classification of finite abelian groups. We get a generalisation of this statement to finitely generated abelian groups which may be possibly infinite.

Proof. Write $\gamma : R^m \rightarrow M$ a generating surjection. We know $\ker \gamma \leq R^m$ and

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

Pick a basis v_1, \dots, v_m for R^m such that $\ker \gamma$ is generated by $d_1 v_1, \dots, d_r v_r$ for $0 \leq r \leq m$ with $d_i \mid d_{i+1}$. This means that

$$M \cong \frac{R^m}{\langle (d_1, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, \dots, d_r, 0, \dots, 0) \rangle} \cong \frac{R}{(d_1)} \oplus \dots \oplus \frac{R}{(d_r)} \oplus R \oplus \dots \oplus R$$

hence we're done. \square

Suppose that G is abelian generated by $a, b, c \in G$ with the following relations

$$\begin{aligned} 2a + 3b + c &= 0 \\ a + 2b &= 0 \\ 5a + 6b + 7c &= 0 \end{aligned}$$

We have a surjection of abelian groups

$$\begin{aligned} \mathbb{Z}^3 &\rightarrow G \\ e_1 &\rightarrow a \\ e_2 &\rightarrow b \\ e_3 &\rightarrow c. \end{aligned}$$

The associated matrix is

$$\begin{pmatrix} 2 & 1 & 5 \\ 3 & 2 & 6 \\ 1 & 0 & 7 \end{pmatrix},$$

and the homomorphism $\mathbb{Z}^3 \rightarrow \mathbb{Z}^3$ has $G \cong \mathbb{Z}^3 / \text{im}(a)$. We need to find the " d_i 's" from the theorem. To do this calculate $\text{Fit}_k(A)$. This comes out to

$$\text{Fit}_1(A) = \text{Fit}_2(A) = (1), \quad \text{Fit}_3(A) = (3).$$

So $G \cong \mathbb{Z}/3$

Proposition. (Chinese remainder theorem) For R a Euclidean domain with $a, b \in R$ such that $\gcd(a, b) = 1$. Then

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

Proof. Consider $\varphi : R/(a) \oplus R/(b) \rightarrow R/(ab)$, given by $(r_1 + (a), r_2 + (b)) \rightarrow (br_1 + ar_2 + (ab))$. To show well-definedness, say $(r_1 + (a), r_2 + (b)) = (r'_1 + (a), r'_2 + (b))$. So $r_1 = r'_1 + za$ and

$r_2 = r'_2 + wr_2 = r'_2 + wb$. So by computation we get that $br_1 + ar_2 + (ab) = br'_1 + bza + ar'_2 + awb = br'_1 + ar'_2 + (ab)$. Hence φ is well-defined.

By the Euclidean algorithm we can write $1 = ax + by$. Observe that

$$\varphi(y + (a), x + (b)) = 1 + (ab)$$

and since $R/(ab)$ is generated by $1_{R/(ab)}$ and φ is an R -module homomorphism, the map is surjective.

Finally for injectivity we calculate $\ker \varphi$. If $br_1 + ar_2 \in (ab)$ then write

$$br_1 + ar_2 = abx$$

for some $x \in R$. We know that $a \mid ar_2$ and $a \mid ab \implies a \mid br_1$. $a \mid b$ are coprime so $a \mid r_1$. Symmetrically we have $b \mid r_2$. So $r_1 \equiv 0 \pmod{a}$ and $r_2 \equiv 0 \pmod{b}$ so $\ker \varphi = \{(0, 0)\}$. \square

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

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

where each N_i is either R or $R/(p^n)$ for some prime p .

Proof. We may write $M \cong \frac{R}{(d_1)} \oplus \cdots \oplus \frac{R}{(d_r)} \oplus R \oplus \cdots \oplus R$. For each d_i write as a product of prime powers and apply the previous proposition. \square

3.4 Modules over \mathbb{F} and forms of matrices

Let V be a vector space over \mathbb{F} and $\alpha \in \text{End}(V)$ so $\alpha : V \rightarrow V$ linear. We can make V into an $\mathbb{F}[X]$ -module where

$$\begin{aligned} \mathbb{F}[X] \times V &\rightarrow V \\ (f(X), v) &\rightarrow f(\alpha)v. \end{aligned}$$

For notation we'll write V_α for this module.

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

If we have a generating set for V as an \mathbb{F} -module then they also generate V_α since $\mathbb{F} \leq \mathbb{F}[X]$. \square

For an example suppose that $V_\alpha \cong \mathbb{F}[X]/(X^r)$. As a vector space over \mathbb{F} , V_α is spanned by $1, X, X^2, \dots, X^{r-1}$ which is a basis. As a matrix α i.e. multiplication by X is given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Similarly if we have $V_\alpha \cong \mathbb{F}[X]/(X - \lambda)^r$, for $\lambda \in \mathbb{F}$, then write $\beta : V \rightarrow V$ as $\alpha - \lambda \cdot \text{id}$. Now by the previous example β can be written in some basis as the matrix in the previous example. So α can be written in some basis as

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

Now for another example, let $p(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r$. Suppose that V_α is an $\mathbb{F}[X]$ module and $V_\alpha \cong \mathbb{F}[X]/(p(X))$. As a vector space over \mathbb{F} we have $\dim \mathbb{F}[X]/(p(X)) = r$ (in particular both V_α and this as vector spaces over \mathbb{F} are isomorphic to \mathbb{F}^r). There is a basis for $\mathbb{F}[X]/(p(X))$ given by $\{1, X, X^2, \dots, X^{r-1}\}$. The matrix α in this basis is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{r-1} \end{pmatrix}.$$

This is sometimes called the companion matrix for $p(X)$.

Theorem. (Rational canonical form) Let V be a finite dimensional vector space over \mathbb{F} and let $\alpha \in \text{End}(V)$ giving an $\mathbb{F}[X]$ -module V_α . Then

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

with $f_1 \mid f_2 \mid \cdots \mid f_s$ and there exists a basis for V where α has block diagonal matrix

$$\begin{pmatrix} c(f_1) & & \\ & \ddots & \\ & & c(f_s) \end{pmatrix}$$

where $c(f_i)$ is the companion matrix for f_i .

Proof. Apply classification of modules over $\mathbb{F}[X]$ and the previous example. \square

Remark. In this rational canonical form, the minimal polynomial of α is f_s and the characteristic polynomial is $\prod_i f_i$. This is because $f(\alpha)$ acts by 0 on all direct summands. No smaller degree polynomial than α acts by 0 on $\mathbb{F}[X]/(f_s)$.

Lemma. The primes in $\mathbb{C}[X]$ are exactly $(X - \alpha)$ for $\alpha \in \mathbb{C}$.

Proof. Any constant is either a unit or 0 so not prime. Any quadratic or above has a root so not irreducible. Clearly $(X - \alpha)$ are always prime since $\mathbb{C}[X]/(X - \alpha) \cong \mathbb{C}$ which is a field. \square

Now for the final theorem! (woah)

Theorem. (Jordan canonical form) Let V be a vector space over \mathbb{C} and let $\alpha \in \text{End}(V)$. Then

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

and there is a basis where α is given by the matrix

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

where $J_a(\lambda)$ is the $a \times a$ matrix given by

$$\begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & \lambda \end{pmatrix}$$

which is the Jordan canonical form.

Proof. Apply the prime decomposition theorem using the lemma above to V_α

□