

Groups, Rings, and Modules

Notes made by Finley Cooper

23rd August 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 $n \geq 5$	11
1.7	Finite p -groups	12
1.8	Finite abelian groups	13
1.9	Sylow Theorems	13
2	Rings	16
2.1	Definitions and examples	16
2.2	Homomorphisms, ideals, and quotients	18
2.3	Integral domains	21
2.4	Factorisation in integral domains	23

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,

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

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,

- $e \in H$
- If $a, b \in H$ then $a \circ b \in H$
- (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.

- The integers under addition, $(\mathbb{Z}, +)$
- The integers modulo n under addition $(\mathbb{Z}_n, +_n)$
- The rational numbers under addition $(\mathbb{Q}, +)$
- The set of all bijections from $\{1, \dots, n\}$ to itself with the operation given by functional composition, S_n
- The set of all bijections from a set X to itself under functional composition is a group $\text{Sym}(X)$
- The dihedral group, D_{2n} the set of symmetries of the regular n -gon
- 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 $\text{Sym}(\mathbb{R}^n)$

- The subgroup of S_n which are even permutations, so can be written as a product of evenly many transpositions, A_n
- The subgroup of D_{2n} which are only the rotation symmetries which is denoted by C_n
- The subgroup of $GL(n, \mathbb{R})$ of matrices which have determinate 1 which is $SL(n, \mathbb{R})$
- The Klein four-group, which is $K_4 = C_2 \times C_2$, the symmetries of the non-square rectangle
- 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,

- Since $e \in H$ we have that $g \in gH$. So every element is in some coset
- The cosets partition, so if $gH \cap g'H \neq \emptyset$ then $gH = g'H$
- 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 $g^{j-i} = e$ which contradicts the minimality of n since $0 < j-i < n$. 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 prove 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, $\varphi(g\ker f) = \varphi(g'\ker f) \implies f(g) = f(g') \implies g'g^{-1} \in \ker f$. 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 $H \cap K \triangleleft G$. 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 $\ker \varphi = \{h : hK = K\} = \{h : h \in K\} = H \cap K \triangleleft G$.

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).

- This is a bijection.
- 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:

- We can write any $\sigma \in S_n$ as a product of disjoint cycles.
- 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 $\text{sgn} : S_n \rightarrow \{\pm 1\}$.
- 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 symmetric group it. 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 $G \rightarrow (X) \cong S_4$. The kernel $G_X = \ker(\varphi) = \{, \text{ send each vertex to its opposite}\}$. 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 isomorphism 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 isomorphism 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:

- A_n is generated by 3-cycles
- If $H \triangleleft A_n$ that contains a 3-cycle then it contains all the 3-cycles
- 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:

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

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

- (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.
- (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.
- (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.
- (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 $x^m Z(G)$, $m \in \mathbb{Z}$. Since any $g \in G$ lies in some coset of $Z(G)$, we can write $g = x^m z$, 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 applies. 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:

- The set $\text{Syl}_p(G) = \{P \leq G \mid P \text{ is a Sylow } p\text{-subgroup of } G\}$ is non-empty.
- Any $H, H' \in \text{Syl}_p(G)$ are conjugate, namely $H = gH'g^{-1}$, for some $g \in G$.
- 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 5, 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 $|\Omega| = \binom{n}{p^a} \equiv m \not\equiv 0 \pmod{p}$. 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

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

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 it 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 $+$: $R \times R \rightarrow R$, and \circ : $R \times R \rightarrow R$, called addition and multiplication are functions satisfying the following:

- $(R, +, 0_R)$ is an abelian group.
- \circ is associative, so $a \circ (b \circ c) = (a \circ b) \circ c$.
- $1_R \circ a = a \circ 1_R = a$.
- 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 $f(x) + 0x^{n+1}$ 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 $r_1, r_2 \in R$:

- $f(r_1 + r_2) = f(r_1) + f(r_2)$
- $f(0_R) = 0_S$
- $f(r_1 r_2) = f(r_1) f(r_2)$
- $f(1_R) = 1_S$.

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 $(r_1+I)(r_2+I) = r_1r_2+I$.

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 $r'_1r'_2 = (r_1+a_1)(r_2+a_2) = r_1r_2 + r_1a_2 + r_2a_1 + a_1a_2$. By the absorbing property the last three terms are contained in I , so $r_1r_2+I = r'_1r'_2+I$. 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:

$$a_0 + a_1X + \cdots + a_nX^n + (X), \text{ but } \sum_{i=1}^n a_iX^i \in (X)$$

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 $a_0 + a_1X + (X)$ with the following multiplication given by $(a_0 + a_1X)(b_0 + b_1X) = a_0b_0 + (a_1b_0 + a_0b_1)X$.

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 $f = qg + r$ with $\deg(r) < \deg(g)$.

Proof. Let n be the degree of f . So $f = \sum_{i=0}^n a_iX^i$ with $a_i \in K, a_n \neq 0$. Similarly $g = \sum_{i=0}^m b_iX^i$ 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 $r \rightarrow r + J$. 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:

- $R \leq F$ is a subring,
- 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 $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$. 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 $\frac{b}{a} \frac{a}{b} = 1_F$, 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 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:

- $\varphi(ab) \geq \varphi(b)$ for all $a, b \neq 0$.
- 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