Groups, Rings, and Modules

Notes made by Finley Cooper

18th July 2025

Contents

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 $\circ : G \times G \to G$ 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 $\{1, \cdots, n\}$ 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 $\mathrm{Sym}(X)$
- The dihedral group, D_{2n} the set of symmetries of the regular n-gon
- The general linear group over $\mathbb{R}$, $\mathrm{GL}(n, \mathbb{R})$, is the set of functions from $\mathbb{R} \to \mathbb{R}$ which are linear and invertiable. Or we can think of the group as the set of $n \times n$ invertiable matrices under matrix multiplication. We can view this group as a subgroup of $\mathrm{Sym}(\mathbb{R}^n)$

- 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 $\mathrm{GL}(n, \mathbb{R})$ of matrices which have determinate 1 which is $\mathrm{SL}(n, \mathbb{R})$
- 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, $f : H \to gH$ 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 ord(g).

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

Proof. Let $g \in G$. Consider the subset, $H = \{e, g, g^2, \cdots, g^{n-1}\}$ 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 $|G|$. □

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 $g_2H = g_2'H$. Then $g_2' = g_2h$ for some $h \in H$. $(g_1H) \cdot (g_2'H) = g_1g_2'H$ by the proposed formula. By the previous relation this is $g_1g_2hH = g_1g_2H$.

Case 2: Suppose that $g_1H = g_1'H$ 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 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 $\cdot : G/H \times G/H \to G/H$ by $(g_1H, g_2H) \to (g_1g_2)H$.

Definition. (Homomorphism) Let G and H be groups. A *homomorphism* is a function $f : G \to H$ 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 $e_G = e_Ge_G$, 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 $f : G \to H$ 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 $f : G \to H$ be a homomorphism. The *kernal* of f is $\ker f = \{g \in G : f(g) = e\}$. The *image* of f is $\operatorname{im} f = \{h \in H : h = f(g) \text{ for some } g \in G\}$.

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

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 $\operatorname{im} f \leq H$, take $a, b \in \operatorname{im} f$, 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 $f(xy^{-1}) \in \operatorname{im} f$. Also $e \in \operatorname{im} f$, so we have that $\operatorname{im} f \leq H$. $\square$

Definition. (Isomorphism) A homomorphism $f : G \to H$ 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 $f : G \to H$ be a homomorphism. Then $\ker f$ is normal, and the function $\varphi : G/\ker f \to \operatorname{im} f$, by $\varphi(g \ker f) = f(g)$, is a well-defined, isomorphism of groups.

Proof. Already shown $\ker f \lhd G$. 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 $f(g'g^{-1}) = e \iff f(g') = f(g)$. 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 $h \in \operatorname{im} f$, 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 kernal 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 $K \lhd G$. 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 $H \cap K \lhd G$. Consider the homomorphism, $\varphi : H \to G/K$, 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 kernal of φ, is $\ker \varphi = \{h : hK = K\} = \{h : h \in K\} = H \cap K \lhd G$.

Now finally we're left to prove the isomorphism. Now apply the first isomorphism theorem to φ. This tells us that $\frac{H}{\ker \varphi} = \frac{H}{H \cap K} \cong \operatorname{im} \varphi$. The image of the φ is exactly those coests 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 $p : G \to G/K$, 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 $L \to p(L)$ 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 $\varphi : G/K \to G/L$, by $\varphi(gK) = gL$. First we'll show that φ is a well-defined homomorphism, then we'll calculate the image and kernal, and finally apply the first isomophism 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 kernal 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 $\varphi : G \to G/H_2$. 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-trivally, 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. □

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 $\mathrm{Sym}(x)$ denote the symmetric group of X and $S_n = \mathrm{Sym}([n])$ where we have that $[n] = \{1, 2, \ldots, n\}$.

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 $\mathrm{sgn} : S_n \to \{\pm 1\}$.
- 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 kernal of sgn.

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

Definition. (Group action) An *action* of G on a set X is a function $\tau : G \times X \to X$ sending $(g, x) \to \tau(g, x) \in X$ 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 permmutation representations related?
For some homomorphism, $\varphi : G \to \mathrm{Sym}(X)$ we map the homomorphism to $a(\varphi) : G \times X \to X$, where $(g, x) \to \varphi(g)(x)$.

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

Proof. We'll construct an inverse of a. Given a group action $* : G \times X \to X$. Define $\varphi(*) : G \to \mathrm{Sym}(X)$ defined by sending $g \to \varphi(*)(g)$, where $\varphi(*)(g)(x) = g * x$. We aim to show that $\varphi(*)(g) : X \to X$ 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. □

Notation: Given a group action G acting on X given by $\varphi : G \to \mathrm{Sym}(X)$, denote

$G^X = \mathrm{im}(\varphi)$, and $G_X = \ker(\varphi)$. By the first isomorphism theorem we have that $G_X \lhd G$ 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 $G \to (X) \cong S_4$. The kernal $G_X = \ker(\varphi) = \{,\ \text{send each vertex to its opposite}\}$. Easy exercise to check that any diagonal can be sent to any other diagonal, so $G^X = \mathrm{im}(\varphi) = \mathrm{Sym}(X)$. 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 $G \times G \to G$, sending $(g, g_1) \to gg_1$. This gives a homomorphism $G \to \mathrm{Sym}(G)$ (easy to check that φ is injective since the kernal is trival). 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 $\varphi G \to \mathrm{Sym}(X)$. Consider $G_X = \ker\varphi$. If $g \in G_X$, then $gg_1H = g_1H, \forall g_1 \in G$, so ${g_1}^{-1}gg_1H = H \implies G_X \subseteq \bigcap_{g_1 \in G} g_1H{g_1}^{-1}$. This argument is completely reversible, so if $g \in \bigcap_{g_1} g_1Hg_1^{-1}$, then for each $g_1 \in G$, we have $\mathrm{g}_1^{-1}gg_1 \in H, so\ \mathrm{g}\!\in G_X \implies G_X = \bigcap_{g_1 \in G} g_1H{g_1}^{-1}$. Since G_X is a kernal 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, $K \lhd G$, 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 kernal of $\varphi : G \to \mathrm{Sym}(G/H)$ is normal, denote it by K. We've shown it is contained by H. First isomorphism theorem gives that $G/K \cong \mathrm{im}(\varphi) \leq Sym(X) \cong S_n$. Give that $|G/K|$ divides $n!$ by Lagrange. Since that $K \leq H$, we have that $|G/K| \geq |G/H| \implies |G/K| \geq n$. □

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 $\varphi : G \to \mathrm{Sym}(X) \cong S_n$. Since the kernal 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 $G \cong \mathrm{im}\,\varphi \leq S_n$. Now we want to show that $\mathrm{im}\,\varphi \leq A_n$. To see this observe that $A_n \lhd S_n$. Consider $A_n \cap \mathrm{im}\,\varphi \leq \mathrm{im}\,\varphi$. By the second isomorphism theorem, $\mathrm{im}\,\varphi \cap A_n \lhd \mathrm{im}\,\varphi \implies \mathrm{im}\,\varphi \cap A_n = \{e\}$ or $\mathrm{im}\,\varphi$ itself. By the rest of the second isomorphism theorem, if $\mathrm{im}\,\varphi \cap A_n = \{e\} \implies \mathrm{im}\,\varphi \cong \frac{\mathrm{im}\,\varphi}{\mathrm{im}\,\varphi \cap A_n} \cong \frac{\mathrm{im}\,\varphi A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2$, but G is non-abelian, so $\mathrm{im}\,\varphi$ is non-abelian, so we have a contradiction. So we have that $\mathrm{im}\,\varphi \cap A_n = \mathrm{im}\,\varphi$, so $\mathrm{im}\,\varphi$ 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 $n \geq 5$. □

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

Theorem. (Orbit-stabiliser) For a group G acting on a set X. For all $x \in X$, there is a bijection $G \cdot x \to G/G_x$ given by $g \cdot x \to gG_x$. 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 $G \times G \to G$, is $(g, h) \to ghg^{-1}$. This is equivilent to a homomorphism $G \to \operatorname{Sym}(G)$.

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

Definition. (Automorphism) Let G be a group. A permutation $G \to G$ that is also a homomorphism is called an *automorphism* of G. The set of all automorphisms of G, $\operatorname{Aut}(G) = \{f : G \to G : f \text{ is a automorphism}\} \subseteq \operatorname{Sym}(G)$, 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 $\operatorname{ccl}_G(g) = \{hgh^{-1} : h \in G\}$, 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 kernal of the conjugation action and the intersection of the centralisers.

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

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-trival $H \triangleleft A_n$ 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 trival. We break into cases

- (a) If H contains an element on the form $\sigma = (12\cdots r)\tau$ where τ is disjoint from $1, \ldots, r$, 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 $1, \cdots, 6$. 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 tranposition, 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-trival.

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. □

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 $x^m Z(G), m \in Z$. 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 $gg' = x^m z x^n z' = x^{n+m} zz' = x^n z' x^m z = g'g$, 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. □

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

1.8 Finite abelian groups

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

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

Moreover, we can 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. □

1.9 Sylow Theorem

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 $\mathrm{Syl}_p(G) = \{P \leq G \mid P \text{ is a Sylow p-subgroup of } G\}$ is non-empty.
- Any $H, H' \in \mathrm{Syl}_p(G)$ are conjugate, namely $H = gH'g^{-1}$, for some $g \in G$.
- If $n_p = |\mathrm{Syl}_p(G)|$ then $n_p \equiv 1 \mod p$ *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 $\mathrm{Syl}_p(G) = \{P\}$, 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 $\mathrm{Syl}_p(G) \implies gPg^{-1} = P$, which proves the claim. □

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 $\mathrm{Syl}_p(G)$ which gives a homomorphism $\varphi : G \to \mathrm{Sym}(\mathrm{Syl}_p(G)) \cong S_{n_p}$. By simplicity, $\ker\varphi = G$ or $\{e\}$. If $\ker\varphi = G$, then $gPg^{-1} = P$ for all $g \in G$ and all $P \in \mathrm{Syl}_p(G)$. 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 $G \to S_{n_p}$, so by the first isomorphism theorem, $G \cong \operatorname{im}\varphi$. We'll show that φ lands in A_{n_p}. Consider the composition $G \to S_{n_p} \to \{\pm 1\}$. If this composition is surjective, then $\ker(\mathrm{sgn} \circ \varphi)$ is index 5, but G simple so not possible. So $\operatorname{im}\varphi \subseteq \ker(\mathrm{sgn}) = A_{n_p}$, 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 $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$. So $n_{11} = 12$ since G is simple. Similarly $n_3 \equiv 1 \mod 3$ 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 interset 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 $|\Omega| = \binom{n}{p^a} \equiv m \neq 0 \mod p$. The proof of this can be seen by expanding out the binomial coeffient, 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 $|\Omega| \neq 0 \mod p$. 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, $|G| = |\Theta||\mathrm{stab}(T)|$. So $p^a m = |\Theta||\mathrm{stab}(T)|$. By our previous lemma, $|\operatorname{stab} T| \mid p^a$, 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 $P \in \mathrm{Syl}_p(G)$, 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 $gQQ^{-1} \leq P$. So our second statement follows taking $b = a$.

For the final theorem, we need to show that $n_p \mid |G|$, and $n_p \equiv 1 \mod p$. For the first statement, consider G acting on $\mathrm{Syl}_p(G)$ 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 $P \in \mathrm{Syl}_p(G)$. Consider P acting on $\mathrm{Syl}_p(G)$ by conjugation. By orbit-stabiliser, all the orbits have size 1 or p. Since $\{P\}$ is a size 1 orbit, to prove the statement is 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 $Q, P \in \mathrm{Syl}_p(N_G(Q)) \implies P = Q$, 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 $+ : R \times R \to R$, and $\circ : R \times R \to R$, 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 by 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 multipliction 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 $2 \circ 3 = 0 \mod 6$ 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 it's 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 coefficents 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:

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

$+, \circ$ 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 coefficents in R is:

$$R[[X]] = \sum_{n=0}^{\infty} r_i X^i$$

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 coefficent.

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