
Groups, Rings and Fields, IB/IIA/IIB

THESE NOTES ARE PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THESE NOTES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

0.1 Introduction

These notes are based upon the lecture course given by Dr. Hyland in Lent 1999. Dr. Hyland is in no way connected with these notes, and I give the strong warning that these notes should not be considered replacement for the lecture course.

Comments, corrections etc. to matt.daws@cantab.net.

0.2 Foreword

This is an O-Course from the Cambridge Mathematics Tripos. As such, it is lectured to 1B and 2A students, but examined in part 2 (both A and B, but no essay in B). The course is a first course on abstract algebra, and is the only real work you will do on group theory in the undergrad course, as well as an introduction to rings, fields etc. As such, it is essential for anyone interested in algebra, which in principle includes (but is by no means limited to) anyone doing pure courses in 2B.

The aim of the first section of the course is to introduce key definitions and principles (such as the Sylow theorems). I would say that the proofs are less important than the results and ideas, and you should try to grasp the latter first. You will also find that many proofs are not very hard once the key idea(s) involved have been understood— as such I would advise against just learning proofs by rote, as this should not be necessary.

The second half of the course is more on applications: for example, symmetric polynomials and Galois theory. While these are not as fundamental as the first half of the course, they will crop up in the third year, so are worth learning. Note that Galois theory gets it's own course in 2B, and as one might imagine, the treatment here is cramped, and not very logical. Here the results are paramount, while the proofs are technical and not that illuminating (while in the 2B course they are much easier, as more machinery is built up). If you were to drop one section of the course, I would make it this bit.

—Matt Daws, August 2000

Contents

0.1	Introduction	ii
0.2	Foreword	ii
1	Groups	1
1.1	Groups and subgroups	1
1.1.1	Finite examples	1
1.1.2	Groups of small order	1
1.1.3	Subgroups	1
1.2	Homomorphisms and normal subgroups	2
1.2.1	First Isomorphism Theorem	3
1.2.2	Universal property of the quotient $G \rightarrow G/N$ for $N \triangleleft G$	3
1.2.3	Second isomorphism theorem	3
1.2.4	Third isomorphism theorem	3
1.3	Groups acting on sets	4
1.3.1	Orbits	4
1.3.2	Stabilizers	5
1.3.3	Size of Rotation and Symmetry Groups	5
1.3.4	Terminology	5
1.4	Permutation Groups	6
1.4.1	Observations	6
1.5	Classical Groups Over Finite Fields	6
1.5.1	Classical Groups	7
1.6	Abelian Groups	7
1.7	Class Equation	8
1.7.1	Application to Groups of Order p^n	8
1.8	Sylow's Theorems	9
1.8.1	Typical Applications: Groups of Order 15	9
1.8.2	Typical Applications: No Group of Order 500 is Simple	10
1.8.3	Typical Applications: No Group of Order 600 is Simple	10
2	Rings	11
2.1	Rings and Homomorphisms	11
2.1.1	Quotients	12
2.2	Fields and Integral Domains	12
2.2.1	The Remainder Theorem	13
2.2.2	The Field of Fractions	14
2.3	Principal Ideal Domains	14
2.4	The Gaussian Integers	16
2.4.1	Basic Number Theory	17
2.5	Unique Factorisation	17
2.5.1	Eisenstein's Irreducibility Criterion	18
2.5.2	Appendix on Number Theory	18

3	Invariants	19
3.1	Rings of Invariants	19
3.1.1	Explanation of Main Result	20
3.1.2	Basic Examples	20
3.2	Symmetric Functions	20
3.2.1	Illustration of Proof	21
3.2.2	Invariants For The Alternating Group A_n	21

Chapter 1

Groups

1.1 Groups and subgroups

A group G is a set equipped with an associative binary operation, denoted by '.', where associative means $x.(y.z) = (x.y).z$, an identity $e \equiv e_G$, $e.x = x.e = x$, and inverse, x^{-1} , $x^{-1}.x = x.x^{-1} = e$.

1.1.1 Finite examples

1. S_n group of all permutations of $\{1, 2, \dots, n\}$
 A_n group of all even permutations.
2. C_n cyclic group of order n , $\cong \mathbb{Z}/n\mathbb{Z}$ with addition, \cong rotations of regular n -gon.
 D_{2n} dihedral groups¹ of order n , \cong all symmetries of regular n -gon.
Groups of symmetries of regular figures– e.g. platonic solids.
3. Classical groups over finite fields, e.g. for finite fields $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ (p a prime) we have
 $GL_n(p) \cong GL_n(\mathbb{F}_p)$ group of all invertible $(n \times n)$ matrices with co-efficients in \mathbb{F}_p
 $SL_n(p) \cong SL_n(\mathbb{F}_p)$ group of $n \times n$ matrices with $\det = 1$ over \mathbb{F}_p .
4. The quaternion group, $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$; $ij = k, jk = i, ki = j$, group of order 8.

1.1.2 Groups of small order

1	:	trivial group
$p = 2, 3, 5, 7$:	C_p
4	:	C_4 and $V = C_2 \times C_2$
6	:	$C_6 \cong C_2 \times C_3, S_3$
8	:	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q$

1.1.3 Subgroups

A *subgroup* $H \leq G$ of a group G is a subset closed under the group operations (i.e. composition and inverse, and with identity element) and so itself forms a group.

Given $H \leq G$, we can find the set $G/H = \{gH : g \in G\}$ which partitions G into subsets of equal size.

Theorem 1.1.1. Lagrange's Theorem

The order of a subgroup divides the order of the group: if $H \leq G$ finite then $|G| = |H||G : H|$ where $|G : H|$, the index of H in G , is $|G/H|$. (In particular, the order of an element divides the order of a group).

Proof. See 1A, or

Introduce an equivalence relation \sim on G by $x \sim y$ iff there exists $h \in H$ such that $xh = y$ (i.e. iff $x^{-1}y \in H$, or equivalently $y^{-1}x \in H$). Then an equivalence class is precisely a right coset, gH , for if $x \sim g$ then $gh = x$ for some $h \in H$, so $x \in gH$ or conversely, if $x \in gH$ then $x = gh$ for some $h \in H$ so

¹So authors call this group D_n which can lead to confusion if n is substituted for an action number!

$x \sim g$. It is also apparent that $|gH| = |H|$ for all $g \in G$, for $gh_1 = gh_2$ iff $h_1 = h_2$ and hence we have a natural bijection $gH \rightarrow H, gh \mapsto h$. Hence we have decomposed G into a number of equivalence classes, each of the size of H . So done. \square

Examples 1.1.2. 1. $A_n \leq S_n$
 $V \cong C_2 \times C_2 \leq A_4$ and so $V \leq S_4$
 $V = \{e, (12)(34), (13)(24), (14)(23)\}$

2. $C_n \leq D_{2n}$, also D_{2n} has lots of subgroups C_2 corresponding to reflections.

3. $C_m \leq C_n$ iff $m|n$.

Note that the converse of Lagrange's Theorem is not true. For example, $|A_4| = 12$ but A_4 has no subgroup of order 6. Note, however, that if $p|G|$ and p prime, the G does contain elements of order p (and hence subgroups of order p).

1.2 Homomorphisms and normal subgroups

A *homomorphism* $\theta : G \rightarrow H$ is a map preserving the group structure: $\theta(ab^{-1}) = \theta(a)\theta(b)^{-1}$ suffices.

Examples 1.2.1. 1. If $H \leq G$ then $H \hookrightarrow G$ is a homomorphism (i.e. the inclusion map).

2. The sign map from S_n , $\epsilon : S_n \rightarrow \{\pm 1\}$.

3. The determinant, $\det : GL_n(F) \rightarrow F^\times$ where F is a field (see later) and F^\times is the multiplicative group of non-zero elements of F .

4. Homomorphisms arise from group actions.

Example 1.2.2. The group of all symmetries of a regular tetrahedron is isomorphic to S_4 . (Why? A symmetry is determined by a permutation of the vertices; and all the transpositions occur via reflections, and these generate S_4).

There are three lines joining the mid-points of opposite edges. Call line a then line joining mid-point of (12) to (34); line b that (13) to (24); and line c that (14) to (23).

Any symmetry of the tetrahedron permutes these three lines and we get a homomorphism $\phi : S_4 \rightarrow S_3$. For example, $\phi(23) = (ab)$; $\phi(12)(34) = e$ and so on.

A subgroup $H \leq G$ is *normal* iff $gHg^{-1} = H$ for all $g \in G$. Equivalently, $gH = Hg$ for all $g \in G$ (it suffices to check $gHg^{-1} \leq H$ for all $g \in G$).

Proposition 1.2.3. *If $H \leq G$, then H is normal in G , write $H \triangleleft G$, iff $(aH, bH) \mapsto abH$ is a well-defined map on cosets. In this case, G/H is itself a group, $aH \cdot bH = abH$ and $G \rightarrow G/H$ is a group homomorphism.*

Proof. If $H \triangleleft G$ then $gHg^{-1} = H$ for all $g \in G$. Hence if $a_1H = a_2H$ and $b_1H = b_2H$ (i.e. $a_1 = a_2h_a$ and $b_1 = b_2h_b$ for some $h_a, h_b \in H$), we want $a_1b_1H = a_2b_2H$. However, $a_1b_1H = a_2h_a b_2h_b H = a_2h_a b_2H = a_2h_a H b_2 = a_2H b_2 = a_2b_2H$, so done.

Conversely, if the coset map is well-defined, then $a_1b_1H = a_2b_2H$ for $a_1 = a_2h_a$ and $b_1 = b_2h_b$. So $a_1b_1H = a_2h_a b_2H = a_2b_2H$ hence $b_2^{-1}h_a b_2H = H$. Hence we have that $gHg^{-1} \leq H$ for all $g \in G$, so $H \triangleleft G$. \square

Examples 1.2.4. 1. Any subgroup of index 2 is normal. For if $|G : H| = 2$ then there are two left cosets of H and $gH = G \setminus H$ for $g \notin H$, and two right cosets of H and $Hg = G \setminus H$ for $g \notin H$. So $gH = Hg$ for all $g \in G$. In particular, $A_n \triangleleft S_n$ and $C_n \triangleleft D_{2n}$.

2. The reflection groups C_2 are not normal in D_{2n} (except when $n = 2$).

1.2.1 First Isomorphism Theorem

Suppose $\theta : G \rightarrow H$ is a group homomorphism. Then $\ker \theta \triangleleft G$ and there is a group isomorphism $\bar{\theta} : G/\ker \theta \rightarrow \text{Im } \theta$, so that θ factors as

$$\begin{array}{ccc} G & \longrightarrow & H \\ \downarrow & & \downarrow \\ G/\ker \theta & \xrightarrow{\bar{\theta}} & \text{Im } \theta \end{array}$$

Proof. If $a \in \ker \theta$ then $\theta(gag^{-1}) = \theta(g)\theta(a)\theta(g)^{-1} = \theta(g)\theta(g)^{-1} = e_H$ and so $gag^{-1} \in \ker \theta$. Thus $g \ker \theta g^{-1} \leq \ker \theta$ and $\ker \theta \triangleleft G$.

$$a \ker \theta = b \ker \theta \Leftrightarrow a^{-1}b \in \ker \theta \Leftrightarrow \theta(a^{-1}b) = e_H \Leftrightarrow \theta(a)^{-1}\theta(b) = e_H \Leftrightarrow \theta(a) = \theta(b)$$

This shows that the map $\bar{\theta} : a \ker \theta \mapsto \theta(a)$ is well-defined, and injective, so onto $\text{Im } \theta$ as required. $\bar{\theta}$ is clearly a group (iso)morphism and the factorisation follows as $\theta(a) = \bar{\theta}(a \ker \theta)$. \square

1.2.2 Universal property of the quotient $G \rightarrow G/N$ for $N \triangleleft G$

Given $\theta : G \rightarrow H$. Suppose $\ker \theta \geq N$. Then θ factors uniquely through $\bar{\theta} : G/N \rightarrow H$. For if $aN = bN$ then $a^{-1}bN = N$ and so $a^{-1}b \in N$. This implies $a^{-1}b \in \ker \theta$ so $\theta(a^{-1}b) = e$ so $\theta(a) = \theta(b)$. Thus $\bar{\theta}(aN) = \theta(a)$ is well-defined. It is easy to show that $\bar{\theta}$ is a group homomorphism and θ factors

$$\begin{array}{ccc} G & \xrightarrow{\theta} & H \\ \downarrow & & \uparrow \bar{\theta} \\ G/N & \longrightarrow & \end{array}$$

1.2.3 Second isomorphism theorem

Suppose $H \leq G$ and $K \triangleleft G$. Then $HK \leq G$; also $K \triangleleft HK$ and $H \cap K \triangleleft H$; what is more $H/H \cap K \cong HK/K$.

Proof. Given $h_1k_1, h_2k_2 \in HK$ we have

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = (h_1h_2^{-1})k_3 \in HK \quad \text{for some } k_3 \in K \text{ as } k_1k_2^{-1} \in K \triangleleft G$$

Also $e = e.e \in HK$, so $HK \leq G$.

Consider the homomorphism $H \xrightarrow{\theta} HK/K$, $h \mapsto hK$. θ is surjective as an arbitrary coset $hkK = hK$; also $\ker \theta = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K$. We deduce $H/H \cap K \cong HK/K$ by the first isomorphism theorem. \square

1.2.4 Third isomorphism theorem

Suppose $N \triangleleft G$. Then $H \rightarrow H/N$ is a bijection between the subgroups of H with $N \leq H \leq G$ and the subgroups of G/N . Under this bijection, $H \triangleleft G$ iff $H/N \triangleleft G/N$ and if so, $(G/N)/(H/N) \cong G/H$.

Proof. The inverse to the bijection takes $L \leq G/N$ to $\{g \in G : gN \in L\} \leq G$.

If $H \triangleleft G$ then for $hN \in H/N$ we have $(gN)(hN)(gN)^{-1} = ghg^{-1}N \in H/N$ so $H/N \triangleleft G/N$. Conversely, $H/N \triangleleft G/N$ then for $h \in H$, and $g \in G$, we have $(ghg^{-1})N \in H/N$ so $ghg^{-1} \in H$ ($\because N \leq H$).

Consider that the map $G \rightarrow G/H$ factors thru $G \rightarrow G/N$ via $\phi : G/N \rightarrow G/H$ by the universal property. ϕ is surjective and $\ker \phi = \{gN : gH = H\} = \{hN : h \in H\} = H/N$. Now,

$$(G/N)/(H/N) \cong G/H$$

by the first isomorphism theorem. \square

1.3 Groups acting on sets

Definition 1.3.1. An *action* of a group G on a set X is a map $G \times X \rightarrow X; (g, x) \mapsto g.x$ such that $e.x = x$ and $g.(h.x) = (g.h).x$ (note that this is a left action; right actions can be defined in the obvious way).

Examples 1.3.2. 1. S_X the group of all permutations of X acts on X ($S_n = S_{\{1,2,\dots,n\}}$).

2. The symmetry group of (geometric/algebraic) structures acts on “components”. $\text{Symm}(\text{triangle})$ acts on 3-element set of “edge diagonals”. $\text{Symm}(\text{cube})$ acts on 8 vertices and on 4 diagonals; acts on 12 edges and so on 6 edge diagonals; acts on 6 faces and so on 3 face-diagonals; acts on 2 inscribed tetrahedrons.

3. $GL_n(\mathbb{F}_p)$ and $SL_n(\mathbb{F}_p)$ act on \mathbb{F}_p^n .

4. *Cayley multiplication actions:* G acts on G by multiplication $(g, x) \mapsto gx$. Similarly G acts on G/H by multiplication; $(g, xH) \mapsto gxH$.

5. *Conjugacy actions:* G acts on G by conjugation: $(g, x) \mapsto gxg^{-1}$. Similarly G acts on subsets/subgroups by conjugation: $(g, A) \mapsto gAg^{-1}$.

Theorem 1.3.3. Suppose G acts on X . Then there is an induced homomorphism $\phi : G \rightarrow S_X$ defined by $\phi(g)(x) = g.x$. Conversely, given $\phi : G \rightarrow S_X$, $g.x = \phi(g)(x)$ defines an action.

Proof. (\Rightarrow) $\phi(g^{-1}).\phi(g)(x) = g^{-1}.g.x = x$ similarly $\phi(g).\phi(g^{-1})(x) = x$ so $\phi(g)$ is a bijection (permutation of X) with inverse $\phi(g^{-1})$. So $(\phi(g))^{-1} = \phi(g^{-1})$. For $g, h \in G$, $\phi(gh^{-1})(x) = (gh^{-1})(x) = g(h^{-1}x) = \phi(g)(\phi(h^{-1})(x)) = \phi(g) \circ \phi(h^{-1})(x)$ by above. So $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1}$, so ϕ is a homomorphism.

(\Leftarrow) $e.x = \phi(e)(x) = e_{S_X}(x) = x$, $g.(h.x) = \phi(g).\phi(h)(x) = \phi(gh)(x) = (gh).x$ so this is an action. \square

Examples 1.3.4. 1. Have $\phi : S_4 \rightarrow S_3$.

2. There are homomorphisms $\text{Symm}(\text{Cube}) \rightarrow S_8, S_4, S_{12}, S_6, S_3, S_2$.

A typical application of this is: If $H \leq G$ then G acts on G/H , non-trivially, and so there is a non-trivial $G \rightarrow S_{G/H}$.

Hence we have the token conclusion: There is no simple group of order 80. Sylow’s theorem (coming up later) implies there exists subgroup $H \leq G$ of order 16. So there exists a non-trivial homomorphism $G \rightarrow S_5$, but $80 \nmid 120$, so not injective. So has a non-trivial kernel, hence a non-trivial normal subgroup, so G cannot be simple (by definition).

Definition 1.3.5. An action $G \times X \rightarrow X$ is *faithful* iff $g.x = h.x$ for all $x \in X$ implies $g = h$. Equivalently, iff $(g.x = x \ \forall x \in X \Rightarrow g = e)$, iff $\ker(G \xrightarrow{\phi} S_X) = 1$. In this case, we can regard G as a group of permutations of X .

Example 1.3.6. The Cayley action of G on G : $(g, x) \mapsto gx$, as $gx = hx \ \forall x \in G \Rightarrow ge = he \Rightarrow g = h$.

Theorem 1.3.7. *Cayley*

Any group is isomorphic to a permutation group. $G \cong$ subgroup of S_G .

The conjugacy action of G on G , $(g, x) \mapsto gxg^{-1}$ gives $\phi : G \rightarrow S_G$ where $\ker \phi = \{g : gxg^{-1} = x \ \forall x \in G\} = \{g : gx = xg \ \forall x \in G\}$ The *centre* $Z = Z(G) = \{g \in G : gx = xg \ \forall x \in G\}$ is the group of elements commuting with all elements of G . $Z(G) \triangleleft G$. The conjugacy action is faithful iff $Z(G) = \{e\}$.

1.3.1 Orbits

Proposition 1.3.8. Let G act on X . Then $x \sim y$ iff $\exists g$ such that $g.x = y$ is an equivalence relation on X .

Proof. $e.x = x \Rightarrow x \sim x$

$g.x = g.y \Rightarrow g^{-1}y = g^{-1}gx = x$ so $x \sim y \Rightarrow y \sim x$

$g.x = y, h.y = z \Rightarrow h.(g.x) = (h.g).x = z$ so $x \sim y, y \sim z \Rightarrow x \sim z$. \square

Definition 1.3.9. The *orbits* of the action are the equivalence classes under \sim . In particular, the *orbit* of $x \in X$, $\text{orb}(x) = O_x = \{g.x : g \in G\}$ (we could write G_x , but this is confusing).

If O_i are the distinct orbits, they partition X and so

$$|X| = \sum |O_i|$$

Definition 1.3.10. An action $G \times X \rightarrow X$ is *transitive* iff there is just one orbit iff $\forall x, y \in X, \exists g \in G$ such that $g.x = y$.

Example 1.3.11. The multiplication action of G on G/H for any $H \leq G$. Here $\text{orb}(H) = \{gh : g \in G\} = G/H$.

The *orbits* for conjugacy actions are *conjugacy classes*. The conjugacy class of $x \in G$ is $\{x\}$ iff $gxg^{-1} = x \forall x \in G$ iff $gx = xg \forall g$ iff $x \in Z(G)$. The conjugacy class of $H \leq G$ is $\{H\}$ iff $gHg^{-1} = H \forall g$ iff $H \triangleleft G$.

1.3.2 Stabilizers

Proposition 1.3.12. Let G act on X . For $x \in X, G_x = \{g \in G : gx = x\} \leq G$.

Proof. $e.x = x$ so $e \in G_x$.

If $g, h \in G_x$ then $(gh).x = g.(h.x) = g.x = x$ so $gh \in G_x$.

If $g \in G_x$ then $g.x = x \Rightarrow x = g^{-1}.x$ so $g^{-1} \in G_x$. □

Definition 1.3.13. Let G act on X . For each $x \in X$, the *stabilizer* of x is $\text{stab}_G(x) = G_x = \{g \in G : gx = x\} \leq G$.

Aside: $\ker \phi = \bigcap_{x \in X} G_x$.

Proposition 1.3.14. $\text{stab}(gx) = g \text{stab}(x) g^{-1}$, so the stabilizers of elements in the same orbit are conjugate.

Proof. $\text{stab}(gx) = \{h : hgx = gx\} = \{h : g^{-1}hgx = x\} = \{h : g^{-1}hg \in \text{stab}(x)\} = g \text{stab}(x) g^{-1}$. □

Theorem 1.3.15. Let G act on X with $x \in X$. Then there is a bijection, $O_x \rightarrow G/G_x, g.x \mapsto gG_x$. So in particular, we have $|G| = |O_x|.|G_x|$. (In fact, $O_x \rightarrow G/G_x$ is a map of sets with a G -action).

Proof. $gx = hx \Leftrightarrow g^{-1}hx = x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow gG_x = hG_x$. This shows that $gx \mapsto gG_x$ is well-defined, and is injective. Clearly it is surjective, so we have a bijection. Then as $|G| = |G : H|.|H|$ in general, and $|O_x| = |G : G_x|$ we are done. □

1.3.3 Size of Rotation and Symmetry Groups

Solid	Rotation group $G, x = \text{vertex}$	Symmetry group G
Tetrahedron	$ G_x = 3, O_x = 4, G = 12$	$ G_x = 6, O_x = 4, G = 24$
Cube	$ G_x = 3, O_x = 8, G = 24$	$ G_x = 6, O_x = 8, G = 48$
“Diamond” ²	$ G_x = 4, O_x = 6, G = 24$	$ G_x = 8, O_x = 6, G = 48$
Icosahedron	$ G_x = 5, O_x = 12, G = 60$	$ G_x = 10, O_x = 12, G = 120$

1.3.4 Terminology

A *simple* group is a group G whose only normal subgroups are 1 and G itself.

The stabilizers in the conjugacy action of G on G are *centralisers*:

$$G_G(x) = \{g \in G : gx = xg\}$$

More generally, if $X \subseteq G$ then $G_G(X) = \{g \in G : gx = xg \forall x \in X\}$ is the centraliser of X .

The stabilisers of subgroups under the conjugacy action are *normalisers*:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Note $H \triangleleft N_G(H)$ and $N_G(H)$ is the largest subgroup of G in which H is normal.

Remark 1.3.16. “All symmetries”

For example, for a tetrahedron put the centre of mass at 0 and then consider the elements of $GL_3(\mathbb{R})$ which permute the vertices. The group $\cong S_4$, 12 rotations, 6 reflections and 6 others.

But the cube and icosahedron have a central order 2 element $x \mapsto -x$ so $\text{symm}(\text{cube}) = \text{rot}(\text{cube}) \times C_2$.

1.4 Permutation Groups

Theorem 1.4.1. *There exists a map $\epsilon : S_n \rightarrow \{\pm 1\}$ with $\ker \epsilon = A_n$, the even permutations.*

Proof. See 1A, Algebra and Geometry. □

Theorem 1.4.2. *Two permutations are conjugate in S_n iff they have the cycle type. Given*

$$\alpha = (a_1 \dots a_k)(a'_1 \dots a'_{k'}), \beta = (b_1 \dots b_k)(b'_1 \dots b'_{k'})$$

then there exists $\delta : a_i \rightarrow b_i$ and $\delta\alpha\delta^{-1} = \beta$.

1.4.1 Observations

Suppose $H \leq S_n$. Then either $H \leq A_n$ and $H \cap A_n = H$ or $H \cap A_n \triangleleft H$ of index 2. (For if H has an odd permutation, τ say, then any $\sigma \in H$ is either even and so in $H \cap A_n$, or is odd so $\tau^{-1}\sigma$ is even and so $\sigma \in \tau(H \cap A_n)$.)

Suppose S_n acts on a set X . Take $x \in X$ and consider $\text{orb}_{S_n}(x)$, $\text{orb}_{A_n}(x)$.

Either $\text{stab}_{S_n}(x) \leq A_n$, so that $\text{stab}_{A_n}(x) = \text{stab}_{S_n}(x) \cap A_n = \text{stab}_{S_n}(x)$ so that $|\text{orb}_{A_n}(x)| = |A_n : \text{stab}_{A_n}(x)| = \frac{1}{2}|S_n : \text{stab}_{S_n}(x)| = \frac{1}{2}|\text{orb}_{S_n}(x)|$

Or $\text{stab}_{A_n}(x) = \text{stab}_{S_n}(x) \cap A_n \triangleleft \text{stab}_{S_n}(x)$ of index 2, so that $|\text{orb}_{A_n}(x)| = |A_n : \text{stab}_{A_n}(x)| = |S_n : \text{stab}_{S_n}(x)| = |\text{orb}_{S_n}(x)|$.

Deduce that if $\text{stab}_{S_n}(x) \leq A_n$ the orbit splits when we restrict to A_n . If $\text{stab}_{S_n}(x) \not\leq A_n$ then the orbit is the same for A_n as for S_n .

Theorem 1.4.3. *A_5 is simple.*

Proof. We consider the conjugacy classes of elements of A_n

Cycle type	Size for S_n	Size for A_n
e	1	1
(123)	20	20
$(12)(34)$	15	15
(12345)	24	12, 12

$$|C_{S_5}(123)| = 120/20 = 6, \text{ so } C_{S_5}(123) = \langle (123), (45) \rangle = \langle (123)(45) \rangle \not\leq A_5$$

$$|C_{S_5}(12345)| = 120/24 = 5, \text{ so } C_{S_5}(12345) = \langle (12345) \rangle \leq A_5$$

So we use the above observations to arrive at the table displayed above. So they are 1,20,15,12,12. But a normal subgroup is a union of conjugacy classes and must contain e . No sum of 1 and some of 20, 14, 12, 12 divides 60, except 60. Hence done. □

The symmetry group of the icosahedron:

- | | | |
|--------------|---------------|---|
| | 1 | identity element |
| 1. There are | 6×4 | elements of order 5 (rotations about 6 diagonals) |
| | 15 | rotations about 15 edge diagonals (order 2) |
| | 16×2 | order 3: rotations about 10 face diagonals |
- giving a total of 60. There are no more as a rotation must have an axis of symmetry.
2. The group acts faithfully on the 5 “co-ordinate axes”, so there is an injection into S_5 . So it is $\triangleleft S_5$ and by checking conjugacy classes must be A_5 .

1.5 Classical Groups Over Finite Fields

We know the fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime. There are finite fields \mathbb{F}_q for $q = p^n$.

1.5.1 Classical Groups

- $GL_n(\mathbb{F}) = (n \times n)$ invertible matrices over \mathbb{F} acts on \mathbb{F}^n . Called the *general linear group*.
- $PGL_n(\mathbb{F}) = GL_n(\mathbb{F})/Z$, *projective general linear group* acts on $\mathbb{P}^{n-1}(\mathbb{F})$, $Z = \lambda\{I\}$.³
- $SL_n(\mathbb{F}) = (n \times n)$ matrices with $\det = 1$, *special linear group*.
- $PSL_n(\mathbb{F}) = SL_n(\mathbb{F})/Z$ where now $Z = \{\lambda I : \lambda^n = 1\}$.

Note: I rather suspect this little section is rather off the syllabus!

Theorem 1.5.1. $PSL_n(\mathbb{F})$ is simple (non-abelian) except in the case $n = 2$ and $\mathbb{F} = \mathbb{F}_2$ or \mathbb{F}_3 .

For \mathbb{F}_2 , all the same $PSL_2(\mathbb{F}_2)$ has 6 elements, acts on $0, 1, \infty$ faithfully⁴. So $\cong S_3$.

$PSL_2(\mathbb{F}_3)$ has 12 elements in it, acts on $0, -1, \infty, +1$ faithfully, so $\cong A_4$.

$SL_2(\mathbb{F}_3)$ has 24 elements, acts on an octagon, $\not\cong S_4$. It has $Z = (\pm I)$, has A_4 as a *quotient*.

1.6 Abelian Groups

A group G is *abelian* iff $gh = hg \forall g, h \in G$ iff $Z(G) = G$.

As a matter of convention, we use additive notation for abelian groups. Group operations are now $0, +, -$. For a^k we write $ka, k \in \mathbb{Z}$. Like vector spaces, but with co-efficients in \mathbb{Z} (note this is called a module). Also write $A \oplus B$ for $A + B = \{(a, b) : a \in A, b \in B\}$. An abelian group A is *finitely generated* iff there exists $a_1, \dots, a_k \in A$ such that for any $a \in A$ we can write $a = \lambda_1 a_1 + \dots + \lambda_k a_k$ for $\lambda_i \in \mathbb{Z}$. Note that \mathbb{Q} is not finitely generated.

Claim 1.6.1. Any finitely generated abelian group A can be written

$$A \cong \mathbb{Z}^k \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

where $d_1 | d_2 | \dots$

In particular, a finite abelian group can be written

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

with $d_1 | d_2 | \dots | d_m$, essentially unique.

Equivalently, any finite abelian group can be written as the \oplus of cyclic groups of prime power order. The Chinese Remainder Theorem implies if $d = p_1^{r_1} \dots p_k^{r_k}$ then

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_k^{r_k}\mathbb{Z}$$

Example 1.6.2. The abelian groups of order 36 are:

- $\mathbb{Z}/36\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$
- $\mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$
- $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
- $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

Theorem 1.6.3. \mathbb{Z}^n is the free abelian group on n generators e_1, \dots, e_n . (Note that e_i is the i th standard basis vector, $(0, \dots, 0, 1, 0, \dots, 0)$ where the 1 is in the i th place).

³ \mathbb{P}^{n-1} is n -dimensional *projective space*, i.e. \mathbb{F}^n / \sim where \sim is the equivalence relation $x \sim y$ iff $x = \lambda y$ for some non-zero $\lambda \in \mathbb{F}$. Z thus represents the matrix analogue of this, i.e. $Z = \{\lambda I : \lambda \neq 0\}$ where I is the identity matrix.

⁴Whoaaaa! Where does ∞ come from? Well, you need to know a little about projective space. I recommend you look it up (slightly unfair to have it in this course at all), but briefly, we have $\mathbb{P}^2 = \{(x : y) : x, y \in \mathbb{F}\}$ where we treat $(x : y) = (x' : y')$ iff there is some non-zero λ such that $x = \lambda x'$ and $y = \lambda y'$. Hence if $x \neq 0$ then $(x : y) = (1 : yx^{-1})$ and if $x = 0$ then $(0 : y) = (0 : 1)$ for all y . So $\mathbb{P}^2 = \{(1 : y) : y \in \mathbb{F}\} \cup \{(0 : 1)\}$. The point $(0 : 1)$ is in this case referred to as the "point at infinity" or simply ∞ . For higher dimensions, you get the "line at infinity", the "plane at infinity" etc.

Suppose $M \leq Z^n$. Then:

1. $M \cong \mathbb{Z}^m$ for some $m \leq n$.
2. There is a basis f_1, \dots, f_n for \mathbb{Z}^n such that $d_1 f_1, \dots, d_m f_m$ form a basis for M with $d_1 | d_2 | \dots | d_m$.
3. $\mathbb{Z}^n / M \cong \mathbb{Z} / d_1 \mathbb{Z} \oplus \dots \oplus \mathbb{Z} / d_m \mathbb{Z} \oplus \mathbb{Z}^{n-m}$

If A is finitely generated there is a surjection $\mathbb{Z}^n \xrightarrow{\phi} A$ and A is \cong to $\mathbb{Z}^n / \ker \phi$. So we read off the results.

Proof. Sketch

Suppose M is generated by a_1, \dots, a_k . Consider the matrix $A = (a_1 | a_2 | \dots | a_k)$. Then do Gaussian Elimination over \mathbb{Z} .

Row operations are equivalent to writing in terms of new basis for \mathbb{Z}^n .

Column operations are equivalent to a new set of generators for M .

Euclid implies we can transform A into

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

where d_1 divides all entries in A_2 . Take $d_1 = \gcd(a_{ij})$. Then repeat. □

1.7 Class Equation

Recall that if G acts on X and O_i are the distinct orbits then $|X| = \sum |O_i|$ where $|\text{orb}(x_i)| = |G : G_{x_i}|$.

Consider the conjugacy action of G on G . The number of conjugacy classes is the *class number* h . If O_1, \dots, O_h are the distinct orbits and we set

$$n_i = |O_i| = |G : G_{x_i}|$$

$x_i \in O_i$, then we have the class equation: $|G| = n_1 + \dots + n_h$.

Traditionally, we let $O_1 = \{e\}$. The number of i with $n_i = 1$ is $|Z(G)|$ (note $n_1 = 1$).

1.7.1 Application to Groups of Order p^n

Proposition 1.7.1. *If $|G| = p^n, n \geq 1$ then $Z(G) \neq 1$*

Proof. For otherwise the class equation is $p^n = |G| = 1 + n_2 + \dots + n_h$ and $p | n_2, \dots, n_h$ (for $n_i = |O_i| = |G : G_{x_i}| \mid |G| = p^n$). Contradiction. □

Lemma 1.7.2. *If G is such that $G/Z(G)$ is cyclic, then G is abelian (and so $G = Z(G)$).*

Proof. If $G/Z(G)$ is cyclic, take a generator of Z . Any element of G is of the form $a^k z, z \in Z$. Take two such: $a^k z, a^l y$ then $(a^k z)(a^l y) = a^k a^l z y = a^l a^k y z = (a^l y)(a^k z)$. So G is abelian. □

Proposition 1.7.3. *If $|G| = p^2$ then G is abelian.*

Proof. $Z(G) \neq 1$ by (1.7.1). If $|Z(G)| = p$ then $|G/Z| = p$ so G/Z is non-trivial cyclic, implies by lemma that $Z(G) = G$, contradiction. So $|Z(G)| = p^2$, hence $G = Z(G)$. □

Proposition 1.7.4. *If $|G| = p^n$ then there is a sequence $1 = Z_0 \leq Z_1 \leq \dots \leq Z_n = G$ where each $Z_i \triangleleft G$ and $Z_{i+1}/Z_i = Z(G/Z_i)$.*

Proof. Define $Z_1 = Z(G)$ and inductively determine Z_{i+1} by $Z_{i+1}/Z_i = Z(G/Z_i)$. Using the fact that a normal subgroup of G/N for $N \leq H \triangleleft G$. The 1st proposition says the G_i increase. □

Proposition 1.7.5. *Application to Cauchy's Theorem*

If p prime and $p \mid |G|$ then G has an element of order p .

Proof. Induction on $|G|$. Initial case $|G| = p$ is easy. Induction step:

Either $Z(G) \neq 1$. Take an element $a \in Z$ with prime order, q say. If $q = p$ then done. Else, $q \neq p$ then $p \mid |G/\langle a \rangle|$. So by induction hypothesis, there is $b \langle a \rangle$ of order p in $G/\langle a \rangle$. Then $b^p \in \langle a \rangle$, so b has order p or pq in which latter case, b^q had order p .

Or $Z(G) = 1$. Claim there is a $g \neq e$ with $p \mid |C(g)|$. For otherwise the class equation is $p \mid |G| = 1 + |G : C(g_2)| + \dots + |G : C(g_k)|$ contradiction. Take such a $g, C(g) < G$ so by induction hypothesis there exists an element a of order p in $C(g)$. □

1.8 Sylow's Theorems

Definition 1.8.1. Suppose p is prime and $|G| = p^m s$ with $\gcd(p, s) = 1$. Then a subgroup $H \leq G$ with $|H| = p^m$ is a *Sylow p -subgroup* of G .

Theorem 1.8.2. Suppose $|G| = p^m s$ with $\gcd(p, s) = 1$. Then:

1. Sylow p -subgroups exist.
2. Any two Sylow p -subgroups are conjugate.
3. The number n_p of such Sylow p -subgroups is $\equiv 1 \pmod{p}$.

Remark 1.8.3. By (2), if P is a Sylow p -subgroup then $n_p = |\text{org}(P)| = |G : N_G(P)|s$ as $P \leq N_G(P)$.

So we have: $n_p | s$ and $n_p \equiv 1 \pmod{p}$.

Examples 1.8.4. 1. $S_3 (\cong D_6)$ has: one Sylow 3-subgroup (rotations); and two Sylow 2-subgroups (reflections).

2. A_4 has: four Sylow 3-subgroups; and one Sylow 2-subgroup.

Proof. (Wielamelt)

Consider $\mathcal{W} = \{A \subseteq G : |A| = p^m\}$ with the multiplicative action by G , $(g, A) \mapsto gA$.

For $A \in \mathcal{W}$, let $H = \text{stab}(A)$. Observe that $HA = A$ so A is a union of right cosets of the subgroup H , and hence $|H| \mid |A| = p^m$.

If $|H| \neq p^m$ then $|\text{orb}(A)| = |G : H|$ is divisible by p .

If $|H| = p^m$ then $|\text{orb}(A)| = |G : H| = s$; moreover $A = Ha$ for $a \in A$ and so $\text{orb}(A) = \text{orb}(a^{-1}Ha) =$ set of left cosets of $a^{-1}Ha$, and so contains a unique Sylow p -subgroup (namely $a^{-1}Ha$); conversely if $\text{orb}(A)$ contains a Sylow p -subgroup, P say, then $\text{stab}(P) = P$ (because clearly $P \leq \text{stab}(P)$ and $|\text{stab}(P)| \mid p^m$) and so $|H| = |\text{stab}(P)| = |P| = p^m$.

We deduce that

$$|\mathcal{W}| = \sum_{O_i \text{ orbits with } p \mid |O_i|} |O_i| + n_p s$$

and so $\binom{p^m s}{p^m} \equiv n_p s \pmod{p}$. We can immediately state that this is “clearly” not $\equiv 0 \pmod{p}$ and so Sylow p -subgroups must exist (as $n_p \neq 0$).

Alternatively, $(x + y)^p = x^p + px^{p-1}y + \dots + y^p \equiv x^p + y^p \pmod{p}$, so $(x + y)^{p^m} \equiv x^{p^m} + y^{p^m} \pmod{p}$, so $(x + y)^{p^m s} \equiv (x^{p^m} + y^{p^m})^s \equiv x^{p^m s} + s x^{p^m(s-1)} y^{p^m} + \dots \pmod{p}$ and hence $\binom{p^m s}{p^m} \equiv s \pmod{p}$. So $n_p \equiv 1 \pmod{p}$.

Finally, to prove section (2): Suppose P, Q are two Sylow p -subgroups. Consider $\mathcal{P} =$ orbit of P under the conjugacy action of G , i.e. $\{gPg^{-1} : g \in G\}$. Now consider the action of Q on \mathcal{P} . The orders of the Q -orbits divide $|Q| = p^m$. But $|\mathcal{P}| = |G : N_G(P)| \mid s$. So there must exist a Q -orbit with just one element. That is, we can find $P' = gPg^{-1}$ such that the Q -orbit of P' is $\{P'\}$.

Thus $Q \leq N_G(P')$ and $P' \triangleleft N_G(P')$. So $P'Q \leq N_G(P')$ and

$$|P'Q| = \frac{|P'| |Q|}{|P' \cap Q|} = \frac{p^m \cdot p^m}{|P' \cap Q|}$$

a power of p . However $|P'Q| \mid p^m s$, so $|P' \cap Q| = p^m$ and so $P' = Q$. Hence done. \square

1.8.1 Typical Applications: Groups of Order 15

Let G be a group of order 15. Then $n_3 \equiv 1 \pmod{3}$ and $n_3 | 5$, so $n_3 = 1$; and $n_5 \equiv 1 \pmod{5}$ and $n_5 | 3$, so $n_5 = 1$.

Hence $C_3, C_5 \triangleleft G$.

However, $C_3 \cap C_5 = 1$ and so $G = C_3 C_5 \cong C_3 \times C_5 \cong C_{15}$.

Note that if all the Sylow p -subgroups (i.e. for all p) are normal then G is the direct product of these groups. For example, order 45: $n_3 = 1$ and $n_5 = 1$ so either $C_9 \times C_5 = C_{45}$ or $C_3 \times C_3 \times C_5 = C_{15} \times C_3$.

1.8.2 Typical Applications: No Group of Order 500 is Simple

$500 = 2^2 \times 5^3$ so as above, $n_5 = 1$ so there is a normal Sylow 5-subgroup.

1.8.3 Typical Applications: No Group of Order 600 is Simple

$600 = 2^3 \times 3 \times 5^2$. As above, $n_5 = 1$ or 6. If $n_5 = 1$ then done.

If $n_5 = 6$, then G acts on the six Sylow 5-subgroups, so there exists $\phi : G \rightarrow S_6$ (non-trivial). However, $600 \nmid 720$, so $\ker \phi \neq 1$ and so there is a normal subgroup in G .

Chapter 2

Rings

2.1 Rings and Homomorphisms

Definition 2.1.1. A *ring* R is a set equipped with:

1. the structure of an abelian group $(0, a + b, -a)$;
2. the structure of a (commutative) monoid (group without inverses) under multiplication;
3. the distribution laws: $0.a = 0 = a.0$, $a.(b + c) = a.b + a.c$.

Examples 2.1.2. 1. The ring \mathbb{Z} of integers.

2. The ring $\mathbb{Z}/n\mathbb{Z}$.
3. A field is a ring k such that $k \setminus \{0\}$ is a multiplicative group, so \mathbb{Q} , \mathbb{R} and \mathbb{C} are fields and so rings.
4. If R and S are rings, then so is $R \oplus S = \{(r, s) : r \in R, s \in S\}$ under pointwise operations.
The Chinese Remainder Theorem states that if $\gcd(m, n) = 1$ then $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
5. If R is a ring then so is $R[X] = \{\sum_{i=0}^n a_i X^i : a_i \in R\}$ the ring of polynomials in X under the usual operations $+$, \times .
6. There is a ring 0 , zero ring which is $\{0\}$. Here $0 = 1$, but if $0 \neq 1$ then $a = a.1 = a.0 = 0$ for all $a \in R$, and so R must be the zero ring.
7. In this case “ring” = “commutative ring”¹. Typical non-commutative rings are

- $M_n(R)$ the ring of $n \times n$ matrices over R .
- $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in R\}$ the quaternions. This is a skew field, or a division ring.

Definition 2.1.3. A *homomorphism* $\theta : R \rightarrow S$ of rings is a map $\theta : R \rightarrow S$ preserving the ring structure: $\theta(0) = 0$, $\theta(a + b) = \theta(a) + \theta(b)$, $\theta(-a) = -\theta(a)$, $\theta(1) = 1$, $\theta(ab) = \theta(a)\theta(b)$. Not all of these are needed, for example $\theta(0) = \theta(a - a) = \theta(a) + \theta(-a) = \theta(a) - \theta(a) = 0$.

Example 2.1.4.

For any ring R there is a unique homomorphism $\theta : \mathbb{Z} \rightarrow R$. For we must have $\theta(0) = 0$ and $\theta(1) = 1$ and $\theta(n) = 1 + \dots + 1$ (n repetitions) and $\theta(-n) = -\theta(n)$, $n > 0$. A tedious check is needed that this is a ring homomorphism, but this basically boils down to $(1 + \dots + 1)(1 + \dots + 1) = (1 + \dots + 1)$ where we have n, m, nm lots of 1s respectively. We write n for $\theta(n)$ in any ring R .

1. $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z} \rightarrow \mathbb{Q}$.
2. For any $a \in R$ there is a homomorphism, $\text{ev}_a : R[X] \rightarrow R$ “evaluate at a ” where $\text{ev}_a(f(X)) = f(a)$.
3. There is a unique homomorphism from any R to 0 .

¹In fact, we mean “commutative ring with identity”, for we have assumed that the ring has a multiplicative identity, 1, which in general it may not do.

4. A subring $S \leq R$ is a subset closed under the ring operations, and so a ring itself. (i.e. $0, 1 \in S$, $a, b \in S \implies a + b \in S, ab \in S$). Then the inclusion $S \hookrightarrow R$ is a ring homomorphism.
5. Also, if $\theta : R \rightarrow S$ is a homomorphism then $\text{Im } \theta \leq S$ is a subring of S . For example, we can regard $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ as a sequence (or tower) of subrings.

Warning: The map $R \rightarrow R \oplus S; r \mapsto (r, 0)$ is not (usually) a ring homomorphism, so R is not naturally a subring of $R \oplus S$.

Definition 2.1.5. An *ideal* I in ring R is a subset which is:

1. An additive subgroup;
2. Closed under multiplication by elements of R , i.e. if $a \in I, r \in R$ then $ra \in I$.

We write $I \triangleleft R$.

Examples 2.1.6. 1. An ideal is not usually a subring, for if $1 \in I$ then $r.1 = r \in I$ for all $r \in R$, so $I = R$. So an ideal $I \subset R$ with $1 \notin I$ is called *proper*.

2. If $a \in R$ then $\langle a \rangle = (a) = \{ra : r \in R\} \triangleleft R$, the *principle ideal* generated by a .
3. If $a_1, \dots, a_k \in R$ then $\langle a_1, \dots, a_k \rangle \triangleleft R$.

4. Ideals in \mathbb{Z} . If $I \triangleleft \mathbb{Z}$ then, either, $I = \{0\}$
or, we can take $a > 0$ least in I ; then for any $b \in I$, we write $b = qa + r$ where $0 \leq r < a$. Now, $r = b - qa \in I$ and so $r = 0$ (else $r < a$, contradiction), thus $a|b$ for all $b \in I$, and $I = \langle a \rangle$.

Recall the h.c.f. of m, n . Take $\langle m, n \rangle \triangleleft R = \mathbb{Z}$, it is of form $\langle h \rangle$. Then h is hcf(m, n) and h is of form $\lambda m + \mu n$ for $\lambda, \mu \in \mathbb{Z}$.

Proposition 2.1.7. Suppose $\theta : R \rightarrow S$ is a ring homomorphism. Then $\ker \theta = \{a \in R : \theta(a) = 0\} \triangleleft R$.

Proof. $\theta(0) = 0$ so $0 \in \ker \theta$. If $a, b \in \ker \theta$ then $\theta(a + b) = \theta(a) + \theta(b) = 0 + 0 = 0$ so $a + b \in \ker \theta$. If $a \in \ker \theta, r \in R$ then $\theta(ra) = \theta(r)\theta(a) = \theta(r).0 = 0$ so $ra \in \ker \theta$. \square

2.1.1 Quotients

If $I \triangleleft R$ then $R/I = \{a + I : a \in R\}$ the set of additive cosets, and this is certainly an abelian group. Also, $((a + I), (b + I)) \mapsto ab + I$ gives a well-defined multiplication on R/I . For is $a - a' \in I$ and $b - b' \in I$ then

$$ab - a'b' = a(b - b') + (a - a')b' \in I$$

and so it follows that R/I has the structure of a ring and the quotient $R \rightarrow R/I$ is a ring homomorphism.

Theorem 2.1.8. If $\theta : R \rightarrow S$ is a ring homomorphism then $\ker \theta \triangleleft R$, $\text{Im } \theta \leq S$ and there is a $\bar{\theta} : R/\ker \theta \rightarrow \text{Im } \theta$ so that θ factors as

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ R/\ker \theta & \xrightarrow{\bar{\theta}} & \text{Im } \theta \end{array}$$

Definition 2.1.9. Let R be a ring. Take $\theta : \mathbb{Z} \rightarrow R$ the unique homomorphism, and let $\ker \theta = (n)$. Then n is the *characteristic* of the ring R .

2.2 Fields and Integral Domains

We say that a divides b in R iff $ac = b$ for some $c \in R$. Write $a|b$. Equivalently, $a|b$ iff $b \in (a)$ iff $(b) \subseteq (a)$.

A *unit* in a ring R is an element $u \in R$ which divides 1, i.e. such that $\exists v \in R$ with $uv = 1$ (such a v is unique, for if $uv = 1$ and $uv' = 1$ then $v' = v'.1 = v'.uv = 1.v = v$). We write u^{-1} for v such that $uv = 1$.

Notation: (non-standard) $R^\times = \{u \in R : u \text{ a unit}\}$. Note that this is a group.

Definition 2.2.1. A *field* is a ring k such that $k^\times = k \setminus \{0\}$, or alternatively, k is a field iff $0 \neq 1$ and for all $a \in k$, $a \neq 0$ implies $\exists b \in k$ such that $ab = 1$.

Definition 2.2.2. An *integral domain* is a ring R such that $0 \neq 1$ and if $ab = 0$ in R then either $a = 0$ or $b = 0$.

We can an integral domain “has no zero divisors”.

Remark 2.2.3. In an integral domain $a.c = b.c$ implies $a = b$ (with $c \neq 0$), for if $a.c = b.c$ then $(a-b).c = 0$ so $a - b = 0$ implies $a = b$.

Examples 2.2.4. 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

2. Any field is an integral domain. For if $ab = 0$, $a \neq 0$ in a field k , then $b = a^{-1}.0 = 0$.

3. \mathbb{Z} is an integral domain, not a field.

4. $\mathbb{Z}/m\mathbb{Z}$ the ring of integers mod m is an integral domain, just when either $m = 0$ or m is prime.

If $m = 1$ then $\mathbb{Z}/m\mathbb{Z}$ is 0 and $0 = 1$ in $\mathbb{Z}/m\mathbb{Z}$. If $m = ab$ properly composite then $a.b = 0$ in $\mathbb{Z}/m\mathbb{Z}$ but $a, b \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$.

On the otherhand, if m is prime then $\mathbb{Z}/m\mathbb{Z}$ is a field (for every non-zero element is prime to m and so has an inverse mod m).

Aside: Any finite integral domain is a field. For if R is such and $a \in R$, $a \neq 0$, then the map $a(\cdot) : R \rightarrow R; x \mapsto ax$ is injective ($a.x = a.y \implies x = y$) thus as R is finite it is surjective. So there is $x \in R$ such that $ax = 1$ so $a \neq 0$ has an inverse.

5. If R is an integral domain then so is $R[X]$. For if $0 \neq f(X) = a_n X^n + \dots + a_0$, $a_n \neq 0$ and $0 \neq g(X) = b_m X^m + \dots + b_0$, $b_m \neq 0$ then $f(X)g(X) = a_n b_m X^{n+m} + \dots + a_0 b_0$, $a_n b_m \neq 0$ so $f(X)g(X) \neq 0$.

2.2.1 The Remainder Theorem

Proposition 2.2.5. If $f(X) \in R[X]$ has a root a (i.e. $f(a) = 0$ in R) then $(X - a)|f(X)$ (i.e. $f(X) = (X - a)g(X)$ for $g(X) \in R[X]$).

Proof. If $f(a) = 0$, $f(X) = a_n X^n + \dots + a_0$ then $f(X) = f(X) - f(a) = a_n(X^n - a^n) + \dots + a_1(X - a) = (X - a)[a_n(X^{n-1} + \dots + a^{n-1} + \dots + a_1)]$ \square

Proposition 2.2.6. If R is an integral domain, then a polynomial of degree n in $R[X]$ has at most n roots.

Proof. By induction on $n = \deg f$. Either f has no roots (so done), or we use the above to write $f(X) = (X - a)g(X)$ where $\deg g = n - 1$. Suppose b is so other root of f ; then $0 = f(b) = (b - a)g(b)$, but $b - a \neq 0$ so $g(b) = 0$, i.e. b is a root of g . By induction hypothesis, g has $\leq n - 1$ roots, so f has $\leq n$ roots. \square

Theorem 2.2.7. Any finite subgroup of the multiplication group of a field or integral domain is cyclic.

Proof. Suppose G is such a group, $|G| = n$.

- Let m be the least common multiple of the orders $o(g)$ for $g \in G$. So $g^m = 1$ for all $g \in G$, so $X^m - 1$ has $\geq n$ roots in the field k , so $m \geq n$. By Lagrange, $m|n$, so $m = n$.
- If an abelian group has m = lowest common multiple of the order of its elements, then there is an element of order m .
- So there is an element $g \in G$ of order $m = n$ and so G is cyclic. \square

Remark 2.2.8. We can prove the 2nd point as follows: Suppose $m = p_1^{r_1} \dots p_k^{r_k}$. Then there exist elements g_i of order $p_i^{r_i} s_i$ and so there exist elements $h_i = g_i^{s_i}$ of order $p_i^{r_i}$. So $h_1 \dots h_k$ has order m .

Application 2.2.9. $\text{Aut}(C_p) \cong C_{p-1}$ when p is prime.

Proof. If $C_p = \langle g \rangle$ then g^i , $1 \leq i \leq p - 1$ are generators. $\theta \in \text{Aut}(C_p)$ is determined by $\theta(g) = g^k$ say, and all such occur. So $\text{Aut}(C_p) = \{\theta_k(g) = g^k : 1 \leq k \leq p - 1\}$. Now, $\theta_k(\theta_l(g)) = \theta_k(g^l) = (\theta_k(g))^l = (g^k)^l = g^{kl} = \theta_{kl}(g)$.

So $\text{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ a finite multiplicative subgroup of a field, so cyclic. \square

2.2.2 The Field of Fractions

Let R be an integral domain. Consider $\{(a, b) \in R^2 : b \neq 0\}$, and let F be the set of equivalence classes under

$$(a, b) \sim (a', b') \iff ab' = a'b$$

(Note that \sim is transitive as if $ab' = a'b$ and $a'b'' = a''b'$ then $(ab'')b' = (ab')b'' = (a'b)b'' = ba'b'' = ba''b' = (a''b)b'$ and so cancelling b' we get $ab'' = a''b$.)

On $F = \{(a, b) : b \neq 0\}$ we have the operations

- $0_F = [(0, 1)]$, $1_F = [(1, 1)]$
- $[(a, b)] +_F [(c, d)] = [(ad + bc, bd)]$
- $-_F [(a, b)] = [(-a, b)]$
- $[(a, b)] \cdot_F [(c, d)] = [(ac, bd)]$

Then a tedious check shows that F is a field and $R \rightarrow F; a \mapsto [(a, 1)]$ is an injective ring homomorphism. (c.f. Getting \mathbb{Q} from \mathbb{Z}). Special case is from $k[X]$ we get $k(X)$ the field of rational functions.

Definition 2.2.10. An ideal $M \triangleleft R$ is *maximal* iff $M \neq R$ and if $M \subset I \triangleleft R$ then either $M = I$ or $I = R$.

Definition 2.2.11. An ideal $P \triangleleft R$ is *prime* iff $P \neq R$ and if $ab \in P$ then $a \in P$ or $b \in P$.

Theorem 2.2.12. $M \triangleleft R$ is maximal iff R/M is a field.

$P \triangleleft R$ is prime iff R/P is an integral domain.

Remark 2.2.13. If $I \triangleleft R$, $a \in R$ set $\langle a, I \rangle = \{xa + b : x \in R, b \in I\} \triangleleft R$. This is then the least ideal containing both I and a . If $a \notin I$ then $\langle a, I \rangle \supset I$.

Independent proof that maximal implies prime. If $M \triangleleft R$ is maximal then $1 \notin M$. Also suppose $ab \in M$ but $a \notin M$. Then $\langle a, M \rangle \supset M$, and so $\langle a, M \rangle = R$. So we can write $1 = xa + m$ with $x \in R, m \in M$, and so $b = xab + mb \in M$. \square

Proof of first proposition. Suppose M is maximal. $1 \notin M$ and so $M \neq 1 + M$ (i.e. $0 \neq 1 \in R/M$). Take $a + M \neq M$ in R/M . Then $a \notin M$ and so $\langle a, M \rangle \supset M$ and so $\langle a, M \rangle = R$. So we can write $1 = \bar{a}a + m$, $\bar{a} \in R, m \in M$. But then $(\bar{a} + M)(a + M) = 1 + M$ and $(a + M)$ has a multiplicative inverse in R/M .

Conversely, suppose R/M is a field. Then $1 + M \neq M$ and so $1 \notin M$ so $M \neq R$. Suppose $M \subseteq I \triangleleft R$ and $I \neq M$. Take $a \in I \setminus M$ and $a + M \neq M$; so we have $(\bar{a} + M)(a + M) = 1 + M$ for some $\bar{a} \in R$, and $\bar{a}a + m = 1$ for some $m \in M$. But then $1 = \bar{a}a + m \in R$ and so $I = R$. \square

Proof of second proposition. R/P is an integral domain iff $(1 + P \neq P + (a + P)(b + P) = P$ implies $a + P = P$ or $b + P = P)$ iff $(1 \notin P$ and $(ab \in P$ implies $a \in P$ or $b \in P)$. \square

2.3 Principal Ideal Domains

Definition 2.3.1. An *Euclidean domain* R is an integral domain R equipped with $d : R \setminus \{0\} \rightarrow \mathbb{N}$ such that if $a \in R, b \neq 0 \in R$ then we can write $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

Examples 2.3.2. 1. \mathbb{Z} with $d(n) = |n|$.

2. $k[X]$ with $d(f) = \deg f$.

Proposition 2.3.3. If R is an Euclidean domain then every ideal in R is principal (i.e. generated by one element).

Proof. Take $I \triangleleft R$, either $I = \{0\} = (0)$ or we can take $a \in I$ with $d(a)$ least. Now suppose $b \in I$. Then we can write $b = qa + r$ with $r = 0$ or $d(r) < d(a)$. However, $r = b - qa \in I$, so $r = 0$ by choice of a . Thus $a|b$, and so $I = (a)$. \square

Definition 2.3.4. A *principal ideal domain* (PID) is an integral domain R in which every ideal is principal.

Example 2.3.5. $k[X]$, where k is a field.

Definition 2.3.6. An element $a \neq 0$ in a ring R is said to be *irreducible* iff a is not a unit and if $a = bc$ then either b or c is a unit.

The idea is that “modulo units” you cannot factorize a .

Definition 2.3.7. An element a in a ring R , with $a \neq 0$, is *prime* iff whenever $a|bc$ then either $a|b$ or $a|c$. Note that this means a is prime iff $a \neq 0$ and $\langle a \rangle$ is a prime ideal.

It is more natural to allow 0 to be prime; just when R is an integral domain.

Proposition 2.3.8. *If R is an integral domain, then a prime implies a is irreducible.*

Proof. Suppose that a is prime, and $a = bc$. Then $a|bc$ so wlog we can assume $a|b$; so $b = ar$ for some $r \in R$; then $a = arc$ and as R is an integral domain we can cancel a to give $1 = rc$, so c is a unit. \square

Examples 2.3.9. 1. In $\mathbb{Z}/4\mathbb{Z}$, 0 is zero, 1 and 3 are units and 2 is both prime and irreducible.

2. Consider the ring $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}$. This is not an integral domain as $(0, 1) \cdot (1, 0) = (0, 0)$. In it, $(0, 1)$ is prime, but not irreducible for $(0, 1) = (0, 1) \cdot (0, 1)$.

3. $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is a subring of the field \mathbb{C} , so an integral domain. On $\mathbb{Z}[\sqrt{-5}]$ there is the algebraic norm $N(a + b\sqrt{-5}) = a^2 + 5b^2 = (a + b\sqrt{-5})(a - \sqrt{-5})$. The norm is a multiplicative function:

$$N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5})$$

- So a unit must have norm 1, and the only units are ± 1 .

- Consider $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Claim 1: $1, 2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible. Why? They have norms 4, 9, 6, 6 so if there were a proper factorisation we'd have to have elements of norm 2 or 3. However, no $a^2 + 5b^2 = 2$ or 3 in $a, b \in \mathbb{Z}$. Neither 2 nor 3 is a square mod 5.

Claim 2: $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ are not prime. For example, $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$ because $N(2) \nmid N(1 \pm \sqrt{-5})$.

Proposition 2.3.10. *If R is a PID then any irreducible element is prime.*

Proof. Let R be a PID. Suppose $a \in R$ is irreducible. Suppose $a|bc$. Consider $\langle a, b \rangle = \{ra + sb : r, s \in R\} \triangleleft R$. As R is a PID we have $\langle a, b \rangle = \langle d \rangle$ for some d . As $a \in \langle d \rangle$, $d|a$, and so we have $a = de$ for some e . Hence as a is irreducible

EITHER, d is a unit, so $\langle a, b \rangle = \langle d \rangle = \langle 1 \rangle = R$ and so we can write $1 = ra + sb$, but then $c = 1 \cdot c = rac + sbc$. However, $a|rac$, $a|sbc$ so $a|c$.

OR, e is a unit. Then $d = e^{-1}a$ and $a|d|b$ so $a|b$. \square

We note that this means $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Example 2.3.11. $\langle 2, (1 + \sqrt{-5}) \rangle$ is not principal. Suppose it were $\langle x \rangle$, then $x|2$ and $x|(1 + \sqrt{-5})$, we must have $N(x)|4, 6$, so $N(x) = 1$ or 2, but 2 can't be. There is no way to write $1 = x \cdot 2 + y \cdot (1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.

Proposition 2.3.12. *In a PID, any non-zero element has a factorization into irreducibles.*

Lemma 2.3.13. *Suppose $a_1, a_2, \dots \in R$ a PID are such that $a_{i+1}|a_i$ for all i . Then for some k , $a_k|a_j$ for all $j \geq k$. Since $a|b$ iff $\langle b \rangle \subseteq \langle a \rangle$ we can reformulate this:*

Suppose $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots \triangleleft R$ a PID. Then for some k , $\langle a_k \rangle = \langle a_{k+1} \rangle = \dots$

Remark 2.3.14. A ring R such that whenever $I_1 \leq I_2 \leq \dots$ is an increasing chain of ideals then $I_k = I_{k+1} = \dots$ for some k is called *Noetherian*.

Proof of Lemma. Take $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$ ideals in R , a PID. Then $\bigcup_{i=0}^{\infty} \langle a_i \rangle \triangleleft R$, and so $= \langle b \rangle$ say. Then $b \in \bigcup \langle a_i \rangle$ and so $b \in \langle a_k \rangle$ for some k . Then $\langle b \rangle \subseteq \langle a_k \rangle \subseteq \langle a_{k+1} \rangle \dots \subseteq \langle b \rangle$ so done. \square

Proof of Proposition. Suppose $0 \neq a$ is non-factorisable in a PID R . Then it's not a unit and it's not irreducible, so it can be written $a = a_1 b_1$ proper factorization where moreover one or other of a_1, b_1 ; let us say a_1 is non-factorisable. Continuing in this way we get $a = a_1 b_1; a_1 = a_2 b_2; a_2 = a_3 b_3; \dots$ all proper factorisations (and where each a_i is non-factorisable). Then $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$ contradiction from Lemma. \square

Notation. Write $a \sim b$ iff $a = ub$ with u a unit. (An equivalence relation).

If p, q are irreducible then if $p|q$ then $p \sim q$, for $q = cp$, say, and as q is irreducible and p is not a unit, then c is a unit. Note that this holds for primes in an integral domain.

Theorem 2.3.15. *In a PID, any element $a \neq 0$ has a prime factorisation; this is essentially unique in that if $a = up_1 \dots p_k = vq_1 \dots q_l; u, v$ units, p_i 's and q_i 's prime then $k = l$ and after re-ordering we'll have $p_i \sim q_i$.*

Understood that $k = l = 0$ possible; a unit has factorisation $u = u$.

Proof. We had factorisation into irreducibles, so primes (in a PID). Remains to show uniqueness which we can do by induction on k . $k = 0$ is trivial. Suppose $up_1 \dots p_k = vq_1 \dots q_l$. Then $p_k|q_1 \dots q_l$ and so, as p_k prime, p_k divides some q_j . After re-ordering, $p_k|q_l$, so then $p_k \sim q_l$ and $q_l = wp_k$, w unit. Now cancelling p_k , $up_1 \dots p_{k-1} = vwq_1 \dots q_{l-1}$ and by induction we have $k-1 = l-1$ and $p_i \sim q_i$ (after re-ordering). \square

Recall. In an integral domain, prime implies irreducible.

In a PID, irreducible implies prime.

Proposition 2.3.16. *If R is a PID the any non-zero prime ideal $0 \neq P \triangleleft R$ (P prime) is maximal.*

Proof. Take $0 \neq P \triangleleft R$. Then $I = \langle b \rangle$, say, and $b|a$. Thus $a = bc$, but as a prime it is irreducible and so either b unit and so $I = R$; or c unit and so $a|b$ and so $P = \langle a \rangle = \langle b \rangle = I$. \square

As a consequence, if f is an irreducible polynomial in $k[X]$ where k is a field, then $k[X]/(f)$ is a field.

If $k = \mathbb{C}$, only have $f = (X - \alpha)$ and then $\mathbb{C}[X]/(X - \alpha) \cong \mathbb{C}$. If $k = \mathbb{R}$ we get as well, polynomials $f(X) = X^2 + bX + c$ where $b^2 < 4ac$, then $\mathbb{R}[X]/(f) \cong \mathbb{C}$.

If $k = \mathbb{Q}$ there are lots of irreducibles, $\mathbb{Q}[X]/(X^4 - 2) \cong \mathbb{Q}[\sqrt[4]{2}] \cong \mathbb{Q}[i\sqrt[4]{2}]$.

2.4 The Gaussian Integers

Consider $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \leq \mathbb{C}$. This is Euclidean via $N(a + bi) = a^2 + b^2$.

Proof. Take $a + bi, c + di \neq 0$ in $\mathbb{Z}[i]$. Let $\frac{a+bi}{c+di} = \alpha + \beta i \in \mathbb{Q}[i]$. Let $s, t \in \mathbb{Z}$ be such that $|\alpha - s|, |\beta - t| \leq \frac{1}{2}$. Then $N((\alpha + \beta i) - (s + ti)) \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{4} < 1$. Then $a + bi = (s + ti)(c + di) + ((\alpha + \beta i) - (s + ti))(c + di)$ and $N(\dots) < N(\dots)$. \square

- So $\mathbb{Z}[i]$ is a PID and hence we have unique factorisation.
- By solving $a^2 + b^2 = 1$ we find that the units are $\pm 1, \pm i$.
- Suppose $a + bi$ is prime. Then $(a + bi)(a - bi) = a^2 + b^2 = m$ say. If $m = rs$ is properly composite, then $(a + bi)|r$ say and then $(a - bi) = r's$ so r' a unit. It follows that $(a - bi) = \pm s / \pm is$ and so $r = s$ and $a + bi \sim r \sim a - bi$.

If $a + bi$ is prime then either of form $p \in \mathbb{Z}$ where p prime, or $N(a + bi)$ is prime is \mathbb{Z} .

The primes are $a + bi$ where $a^2 + b^2 = \text{prime} \in \mathbb{Z}$; or $p \in \mathbb{Z}$ where p can't be of form $a^2 + b^2$.

Question 2.4.1. *Which primes $p \in \mathbb{Z}$ are primes in $\mathbb{Z}[i]$. p is prime in $\mathbb{Z}[i]$ iff $\mathbb{Z}[i]/(p)$ is field iff $(\mathbb{Z}[X]/(X^2 + 1))/(p)$ is field iff $\mathbb{Z}[X]/\langle X^2 + 1, p \rangle$ is field iff $(\mathbb{Z}/(p)[X])/(X^2 + 1)$ is field iff $X^2 + 1$ is irreducible in $\mathbb{Z}/(p)[X]$ iff -1 is not a square mod p .*

If $a^2 + b^2 = p$ prime then $-1 = (b/a)^2 \pmod{p}$, so -1 is a square mod p . Conversely, if -1 is a square mod p , then p is not a prime in $\mathbb{Z}[i]$ so it factorises $p = (a + bi)(a - bi) = a^2 + b^2$.

2.4.1 Basic Number Theory

-1 is a square mod p iff $p = 2$ or $p \equiv 1 \pmod{4}$. Thus the primes in $\mathbb{Z}[i]$ are: $p = 2, p \equiv 3 \pmod{4}$ and $a + bi, a - bi$ where $a^2 + b^2 = p \equiv 1 \pmod{4}$.

2.5 Unique Factorisation

Definition 2.5.1. A *unique factorisation domain* (UFD) is an integral domain R in which every $a \neq 0$ has a factorisation $a = up_1 \dots p_k$, u unit and p_i primes.

N.B. 1. Note that we have shown that every PID is a UFD.

2. The factorisation in a UFD is essentially unique; and irreducible elements are prime.

3. Given $a_1, \dots, a_n \in R$ a UFD we can find a highest common factor: take out the common primes and write $a_i = hb_i$ where the b_i have no common primes. Then $h = \gcd(a_1, \dots, a_n)$. But we cannot in general write h as an R -linear combination of the a_i (only in a PID).

Example 2.5.2. $\mathbb{Z}[X]$ is a UFD, but not a PID. For example, $\langle 2, X \rangle$ is not principle; the $\gcd(2, X) = 1$, but we cannot write $1 = r \cdot 2 + s \cdot X$.

Theorem 2.5.3. *If R is a UFD then $R[X]$ is a UFD.*

Hence $\mathbb{C}[X_1, \dots, X_n]$ and $\mathbb{Z}[X_1, \dots, X_n]$ are UFDs.

Idea behind proof. Take F the field of fractions. $F[X]$ is a PID so UFD. We show that factorisation in $R[X]$ is determined by that in R and in $F[X]$. \square

Take R to be a UFD and F its field of fractions.

Definition 2.5.4. A polynomial $f \in R[X]$ is *primitive* iff the co-efficients have no common prime factors ($f(X) = a_n X^n + \dots + a_1 X + a_0$, primitive iff $\gcd(a_n, \dots, a_0) = 1$).

Theorem 2.5.5. Gauss's Lemma

The product of primitive polynomials is primitive.

Proof. Suppose $f = a_n X^n + \dots + a_1 X + a_0$ and $g = b_n X^n + \dots + b_1 X + b_0$ are primitive. Suppose p is a prime in R . Choose i, j least such that $p \nmid a_i$ and $p \nmid b_j$. The co-efficient of X^{i+j} in the product fg is

$$a_i b_j + (a_{i-1} b_{j+1} + \dots) + (a_{i+1} b_{j-1} + \dots)$$

where p divides all the summands bar $a_i b_j$; and so $p \nmid c_{i+j}$, the X^{i+j} co-efficient in fg . Since p arbitrary, it follows that fg is primitive. \square

Corollary 2.5.6. *(To proof)*

If p is prime in R then p is prime in $R[X]$.

N.B. • If $f \in R[X]$ we can write $f = a\tilde{f}$, $a \in R$, \tilde{f} primitive.

• If $f \in F[X]$, then put the co-efficients over a common denominator, take out the common factors of the numerators, and so we write $f = \frac{a}{b}\tilde{f}$, $a, b \in R$ and \tilde{f} primitive, $f \in R[X]$.

Proposition 2.5.7. *Suppose $f \in R[X]$ is primitive and that it is irreducible = prime in $F[X]$. Then f is prime in $R[X]$.*

Proof. Suppose $f|gh \in R[X]$. Then $f|gh \in F[X]$ and so we have $f|g$ say in $F[X]$. So there is $k \in F[X]$ such that $kf = g$. Write $g = r\tilde{g}$, \tilde{g} primitive and $k = \frac{a}{b}\tilde{k}$, \tilde{k} primitive. Then $akf = br\tilde{g}$.

The hcf of co-efficients on the LHS is a , and on the RHS is br , and so $a = ubr$; u a unit in R .

Then $(ur\tilde{k})f = r\tilde{g} = g$ and so $f|g$ in $R[X]$. This shows f is prime in $R[X]$. \square

Proof of Theorem. Take $f \in R[X]$. Write $f = c\tilde{f}$, \tilde{f} primitive. We can factorise $c = uc_1 \dots c_k$ into prime factors in R , (there are prime in $R[X]$). Factorise \tilde{f} in $F[X]$, $\tilde{f} = g_1 \dots g_l$ say. We can write each $g_i = \frac{a_i}{b_i}h_i$; h_i primitive in $R[X]$ and so $\tilde{f} = \frac{a}{b}h_1 \dots h_l$ where $h_1 \dots h_l$, prime in $F[X]$ and primitive. Now, $b\tilde{f} = ah_1 \dots h_l$, hcf on LHS= b , hcf on RHS= a , so $a \sim b$ and $a = vb$ (v unit) and so $\tilde{f} = vh_1 \dots h_l$. But then $f = (uv)c_1 \dots c_k h_1 \dots h_l$. \square

Suppose R is a UFD and F its field of fractions. Suppose we have $f(X) \in R[X]$ which is irreducible in $R[X]$. Then it is irreducible in $F[X]$. This is just the proof of the theorem². Were f reducible in $F[X]$ we'd get a proper prime factor in $R[X]$.

2.5.1 Eisenstein's Irreducibility Criterion

Suppose R is an integral domain, $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ is a monic polynomial in $R[X]$, and p is a prime in R such that $p|a_{n-1}, \dots, a_0$ and $p^2 \nmid a_0$. Then f is irreducible.

Application 2.5.8. *If p is prime then $\phi(x) = x^{p-1} + \dots + 1$ is irreducible in $\mathbb{Z}[X]$. For $\phi(x)$ is irreducible iff $\phi(y+1)$ is irreducible and*

$$\phi(y+1) = \frac{(y+1)^p - 1}{y+1-1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{p-1}$$

satisfies Eisenstein's irreducibility criterion.

Proof. Suppose $f = (X^r + b_{r-1}X^{r-1} + \dots + b_0)(X^s + \dots + c_0)$ is a proper factorisation. Take i least such that b_i is not divisible by p ($i = r$ included) and j similarly for c_j . However, as $p^2 \nmid a_0 = b_0c_0$, p cannot divide both b_0 and c_0 , and so one of i, j is zero; hence $i + j < n = r + s$.

The co-efficient $a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + \dots) + (b_{i+1}c_{j-1} + \dots)$. Now, p divides everything on the RHS, bar $b_i c_j$, but p divided the RHS. So p divides $b_i c_j$, and p prime implies p divides b_i or c_j , contradiction. \square

2.5.2 Appendix on Number Theory

- -1 is a square mod p iff $p = 2$ or $p \equiv 1 \pmod{4}$.
- 2 is a square mod p iff $p \equiv \pm 1 \pmod{8}$.
- For p, q odd primes: p is a square mod q iff q is a square mod p except in the special case $p, q \equiv 3 \pmod{4}$ when p is a square mod q iff q is not a square mod p .

Note $\mathbb{Z}[X]/\langle n, f \rangle \cong (\mathbb{Z}/n\mathbb{Z})[X]/\langle \bar{f} \rangle$ where \bar{f} is the image of f in $\mathbb{Z}/n\mathbb{Z}$.

²You will sometimes find Gauss's Lemma stated as being this fact

Chapter 3

Invariants

3.1 Rings of Invariants

The idea is that we have a vector space V , over a field k , on which some group of symmetries acts as linear transformations. We seek functions of vectors in V which are “invariant” under the action of G :

$$f : V^m \rightarrow k, f(gv_1, \dots, gv_m) = f(v_1, \dots, v_m) \text{ for all } g \in G$$

Example 3.1.1. $V = \mathbb{C}^n$ and the symmetric group S_n acts on V by permuting the co-ordinates on functions $f : V \rightarrow \mathbb{C}$,

$$\sigma.f(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

These functions are the symmetric functions. Examples are

$$\begin{aligned} e_1 &= X_1 + X_2 + \dots + X_n = \sum_i X_i \\ e_2 &= X_1X_2 + X_1X_3 + \dots = \sum_{i < j} X_iX_j \\ e_3 &= X_1X_2X_3 + \dots = \sum_{i < j < k} X_iX_jX_k \end{aligned}$$

It is a fact that any symmetric polynomial is a polynomial in the e_i 's.

Example 3.1.2. Let $V = \mathbb{R}^n$ and consider the groups $O(n)$ and $SO(n)$ of orthogonal, special orthogonal transformations (with respect to the Euclidean inner product).

In the case of $O(n)$, consider functions $f : V \times V \rightarrow \mathbb{R}$ invariant under $O(n)$: three obvious functions:

$$(\mathbf{x}, \mathbf{y}) \rightarrow \|\mathbf{x}\|^2, \mathbf{x} \cdot \mathbf{y}, \|\mathbf{y}\|^2$$

Any invariant polynomial is in fact generated by these three. This result will extend to functions of many variables.

Consider also $SO(n)$. Then there is also an invariant function of n variables $(x^{(1)}, \dots, x^{(n)}) \mapsto \det(\mathbf{x}^{(1)} | \dots | \mathbf{x}^{(n)})$. This provides a complete set of invariants.

In case $n = 3$, this is “familiar”. δ_{ij} and ϵ_{ijk} . Even $\epsilon_{ijk}\epsilon_{ilm} = \delta_{jl}\delta_{km} - \delta_{jm}\delta_{kl}$ “has to be true”¹.

\mathbb{C}^n space of n roots of a polynomial in order. \mathbb{C}^n/S_n space of roots without regard to order. But $(t - x_1) \dots (t - x_n) = t^n - e_1t^{n-1} + e_2t^{n-2} + \dots + (-1)^n e_n$ and the e_i uniquely determined the set of roots: $\mathbb{C}^n/S_n \xrightarrow{\sim} \mathbb{C}^n$.

We consider functions of one vector variable. A polynomial functions on $V = k^n$ is an $f(x_1, \dots, x_n) \in k[X_1, \dots, X_n]$. For $A \in GL(V) = GL_n(k)$, $A = (a_{ij})$ we let A act on $k[X_1, \dots, X_n]$:

$$A.f(X_1, \dots, X_n) = f\left(\sum a_{1j}X_j, \dots, \sum a_{nj}X_j\right)$$

As an aside, this is really a “right action”, for

$$B.A.f(X_i) = B.f\left(\sum a_{ij}X_j\right) = f\left(\sum a_{ij}b_{jk}X_k\right) = (AB).f(X_i)$$

¹You'll see similar sorts of arguments in the 1B Methods course

So a better notation is f^A . To get a left action we'd define $A * f(X_i) = A^{-1} \cdot f(X_i)$. All this has no effect on the ring of invariants, so we'll ignore it.

Definition 3.1.3. Let $G \leq GL_n(k)$. The ring of invariants for G is

$$k[X_1, \dots, X_n]^G := \{f \in k[X_1, \dots, X_n] : A \cdot f = f \ \forall A \in G\}$$

Remark 3.1.4. As a vector space over k , $k[X_1, \dots, X_n]$ has basis consisting of the monomials $X_1^{r_1} \dots X_n^{r_n}$. The degree of $X_1^{r_1} \dots X_n^{r_n}$ is $\sum r_i$. (There are finitely many monomials of a given degree). We can write any $h \in k[X_1, \dots, X_n]$ uniquely as $h = \sum h_d$, where h_d is homogeneous of degree d , i.e. all the monomials occurring in it are of degree d . The action of $GL_n(k)$ preserves homogeneous polynomials of given degree and hence $h \in k[X_1, \dots, X_n]^G$ iff all $h_d \in k[X_1, \dots, X_n]^G$.

3.1.1 Explanation of Main Result

Let k be a field. A k -algebra is a ring R equipped with a ring homomorphism $k \rightarrow R$.

This means R is a ring with k -vector space compatibility, i.e. the addition and multiplication is k -bilinear.

This also means that R is a ring with k a subring (Only case left is R is zero ring).

3.1.2 Basic Examples

$k[X_1, \dots, X_n]$ and subrings of it containing k (e.g. all rings of invariants).

A k -algebra R is finitely generated iff $\exists r_1, \dots, r_k \in R$ such that any $a \in R$ can be written $a = f(r_1, \dots, r_k)$ for some $f \in k[X_i]$, i.e. there exists a surjective ring homomorphism

$$k \rightarrow k[X_1, \dots, X_n] \rightarrow R$$

extending k .

Theorem 3.1.5. Let $G \leq GL_n(k)$ be a finite group of matrices over a field of characteristic 0. Then $k[X_1, \dots, X_n]^G$ is finitely generated.

3.2 Symmetric Functions

The symmetric group S_n acts on $V = k^n$ by permuting the coefficients

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix}$$

The corresponding matrix has a 1 in $(i\sigma(i))$ place, 0's otherwise.

σ acts on $f(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$, $\sigma \cdot f = f(X_{\sigma(i)})$.

Define the elementary symmetric functions e_1, \dots, e_n by

$$\prod_{i=1}^n (t - X_i) = t^n - e_1 t^{n-1} + e_2 t^{n-2} + \dots + (-1)^n e_n$$

or better, $e_0 = 1$ and e_1, \dots, e_n has the generating function

$$E(t) = \prod_{i=1}^n (1 + X_i t) = \sum_{i=0}^n e_i t^i$$

For example, in $[X, Y, Z]$, $e_0 = 1$, $e_1 = X + Y + Z$, $e_2 = XY + XZ + YZ$ and $e_3 = XYZ$.

Theorem 3.2.1. The elementary symmetric functions e_1, \dots, e_n generate the ring of invariants

$$k[X_1, \dots, X_n]^{S_n} = \Lambda$$

(freely) as a ring.

1. $k[X_1, \dots, X_n]^{S_n} = k[e_1, \dots, e_n]$
2. $k[e_1, \dots, e_n] \cong k[Y_1, \dots, Y_n]$

Proof. Order monomials by reverse lexicographic ordering, RLO

$$X_1^{r_1} \dots X_n^{r_n} > X_1^{s_1} \dots X_n^{s_n}$$

the least i such that $r_i \neq s_i$ has $r_i > s_i$. For example, with X, Y, Z we have $X^3 > X^2Y > X^2Z > XY^2 > XYZ > XZ^2 > Y^3 > Y^2Z > YZ^2 > Z^3$

Then for $f \in k[X_1, \dots, X_n]$ write $\text{hm}(f)$ to be the highest monomial occurring in f .

If f is symmetric then $\text{hm}(f) = X_1^{r_1} \dots X_n^{r_n}$ satisfies $r_1 \geq r_2 \geq r_3$.

hm is multiplicative, i.e. $\text{hm}(fg) = \text{hm}(f)\text{hm}(g)$.

So in particular, $\text{hm}(e_1^{k_1} e_2^{k_2} \dots e_n^{k_n}) = X_1^{k_1+\dots+k_n} X_2^{k_2+\dots+k_n} \dots X_n^{k_n}$.

Take f , symmetric and homogeneous of degree d . Let $\text{hm}(f) = X_1^{r_1} \dots X_n^{r_n}$. Then $f = aX_1^{r_1} \dots X_n^{r_n} + \text{lower terms}$. So then $g = f - ae_1^{r_1-r_2} e_2^{r_2-r_3} \dots e_n^{r_n}$ is homogeneous of degree d with $\text{hm}(g) < \text{hm}(f)$. Thus inductively we can write f as a polynomial in the e_1, \dots, e_n .

Thus $k[X_1, \dots, X_n]^{S_n} = k[e_1, \dots, e_n]$.

Take a polynomial $h(Y_1, \dots, Y_n) \neq 0$. Let $Y_1^{k_1} \dots Y_n^{k_n}$ be the monomial appearing in h such that $X_1^{k_1+\dots+k_n} X_2^{k_2+\dots+k_n} \dots X_n^{k_n}$ is greatest with respect to RLO. Then $h(e_1, \dots, e_n)$ has non-zero co-efficient and so $\neq 0$. So the kernel of $k[Y_1, \dots, Y_n] \rightarrow k[e_1, \dots, e_n]; Y_i \mapsto e_i$ is 0. So $k[e_1, \dots, e_n] \cong k[Y_1, \dots, Y_n]$. \square

3.2.1 Illustration of Proof

$$\begin{aligned} X^3 + Y^3 + Z^3 &= (X + Y + Z)^3 - 3(X^2Y + XY^2 + Y^2Z + YZ^2 + Z^2X + ZX^2) - 6XYZ \\ &= (X + Y + Z)^3 - 3(X + Y + Z)(XY + YZ + ZX) \\ &= (X + Y + Z)^3 - 3(X + Y + Z)(XY + YZ + ZX) + 3XYZ \end{aligned}$$

Symmetric Powers: These are $p_k = X_1^k + \dots + X_n^k$, and there are recurrence relations connecting these with the e_i .

Recall $E(t) = \prod (1 + X_i t) = 1 + e_1 t + e_2 t^2 + \dots$. Consider

$$\frac{E'(t)}{E(t)} = \frac{d}{dt} \log E(t) = \sum \frac{X_i}{1 + X_i t} = p_1 - p_2 t + p_3 t^2 + \dots$$

Then multiply across, $(e_1 + 2e_2 t + 3e_3 t^2 + \dots) = (p_1 - p_2 t + p_3 t^2 + \dots)(1 + e_1 t + e_2 t^2 + \dots)$

$$\begin{aligned} e_1 &= p_1 \\ 2e_2 &= p_1 e_1 - p_2 \\ 3e_3 &= p_1 e_2 - p_2 e_1 + p_3 \quad \text{etc.} \end{aligned}$$

Check:

$$\begin{aligned} p_3 &= 3e_3 - p_1 e_2 + p_2 e_1 \\ &= 3e_3 - e_1 e_2 + (p_1 e_1 - 2e_2) e_1 \\ &= 3e_3 - 3e_1 e_2 + e_1^3 \end{aligned}$$

3.2.2 Invariants For The Alternating Group A_n

Suppose f is invariant under A_n . Take τ a transposition and let $g = f^\tau$.

- g is invariant under the action of A_n . ($A_n \triangleleft S_n$. Given $\tau \in A_n, \exists \tau' \in A_n$ such that $\tau\sigma = \sigma\tau'$, then $g^\sigma = f^{\tau\sigma} = f^{\sigma'\tau} = f^\tau = g$).
- Consider $(f + g)$. This is a symmetric function. (If $\sigma \in A_n$ so $\tau\sigma$ is in $S_n \setminus A_n$; $f^{\tau\sigma} = g^\sigma = g$ and $g^{\tau\sigma} = f^{\tau^2\sigma} = f^\sigma = f$).
- Consider $(f - g)$. This is alternating in the sense that $(f - g)^\sigma = \epsilon(\sigma)(f - g)$.

Suppose h is alternating, $h^\sigma = \epsilon(\sigma)h$. We claim that h is divisible by $\Delta = \prod_{i>j}(X_i - X_j)$. Write $h = h(X_i, X_j)$ suppressing other variables, we see that $h(X, X) = -h(X, X)$, i.e. $h(X, X) = 0$. Consider $h(X, Y)$ as a polynomial in Y , it has a root $Y = X$ and so it is divisible by $(Y - X)$ by the remainder theorem.

Now, the $(X_i - X_j)$ for $i \neq j$ are distinct irreducible

Bibliography

[Cohn] P.M. Cohn, *Algebra Volume One (2nd ed.)*, Wiley, £, ISBN 0471101699.

This would be an excellent book for all of the algebra you'll meet in the first two years of the Maths Tripos at Cambridge, but it's quite technical and upfront, so making learning things from it hard. Also, Cohn uses right-hand convention for mappings, which while is more logical for algebra, is hardly used outside of this branch of pure maths, and so makes reading that much harder. More of a reference guide to revise from say.

[Cameron] Peter J. Cameron, *Introduction to Algebra*, Oxford Science Publications, £16.95, ISBN 0198501943

This book is much more closely fitted to the course than Cohn's, but also doesn't cover as much material. It is an easy introduction to Groups, Rings, Vector Spaces and Modules and covers some Field theory. The pace, content and approach are very similar to this course, and I highly recommend this book. It does not, however, go much beyond the course (so would not really be suitable, for example, for the 2B course Galois Theory).