Year 3 — Groups, Rings and Fields

Based on lectures by Professor Mohamed Saïdi

Notes taken by James Arthur

Autumn Term 2021

Contents

1 Basics of Groups

We start by defining a group, it is an example of an algebraic structure. *Lecture 1*

Definition 1.1 (Group)**.** G is a nonempty set and endowed with a composition rule $(\cdot)$. We denote this $(G, \cdot)$. $(\cdot)$ is well defined, so we can associate another element $a \cdot b \in G$ and $a \cdot b$ is unique. $(\cdot)$ must be associative,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

The brackets are irrelevant when combining more than two elements. We also have **natural element**, so,

$$c \cdot e_G = c = e_G \cdot c$$

There are also inverses, so,

$$a \cdot a^{-1} = e_G = a^{-1} \cdot a$$

So the inverse naturalises the element.

If we just have a group usually $a \cdot b \neq b \cdot a$, if $a \cdot b = b \cdot a$ are called abelian or commutative groups. This is in reference to the mathematician Abel.
If G is finite as a set, then we can say that G is a finite group and we denote the size or cardinality of G as $|G|$, sometimes this is said to be the order. The cardinality can be infinite.

Example. We know a very important group, the group of integers $\mathbb{Z}$. This set is infinite as $n \neq n + 1$ and the composition law is $+$ and we know that it's associative and natural element of 0 and each element n has an inverse of $-n$. We can also say,

$$k_1 + k_2 = k_2 + k_1$$

and so we have an infinite abelian group.

Example. We can also consider groups of integers module n, denoted,

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

where we have modulo classes (see Number Theory notes week 2). We can say, if $[k]_n = [l]_n$ if and only if $n \mid k - l$. Also if you have $[k_1]_n$ and $[k_2]_n$, then $[k_1]_n + [k_2]_n = [k_1 + k_2]_n$. We have to check if this addition is well defined and it is, as you can just multiply by a constant as $[k + rn]_n = [k]_n$. This is also a group with natural element of $[0]_n$ the inverse of $[k]_n$ is just $[-k]_n$ as $[k]_n + [-k]_n = [0]_n$. This is a finite abelian group and $|\mathbb{Z}_n| = n$.

There is two worlds, non-commutative and commutative. Nature is not commutative, things aren't that nice. Our best example of the non-commutative group is the group of permutations. Let $n \in \mathbb{Z}^+$ and then let there be a set $S_n = \{1, 2, \ldots, n\}$ and consider all possible bijections σ from that set to itself. As these are finite sets and of the same cardinality, it suffices to check it's injective.

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

saying this is a bijection says the bottom row, given they are integers from 1 to n, appear only once, they don't appear twice.

Example. Let us take S_4, then we can take an element,

$$\sigma = \begin{pmatrix} 4 & 3 & 2 & 1 \end{pmatrix}$$

and we can call this σ and is an element of the group.

New question, what is $|S_n|$, how many σ are there? It's $n!$.

Proof. Define σ and you have to consider $\sigma(1)$ and theres n possibilities, then for $\sigma(2)$ theres $n-1$ possibilities, then we can't use $\sigma(1)$ or $\sigma(2)$ and hence theres $n-2$ possibilities for $\sigma(3)$ and so on. So we have,

$$n(n-1)\cdot(n-2)\cdot(n-3)\ldots 2\cdot 1 = n!$$

□

We can form a group where the composition is just $\circ$ on our set of bijections σ. If we take a $\sigma\circ\tau$ then this is also a bijection into S_n. This is associative and we get a natural element of id_{S_n}. Then every bijection has an inverse σ^{-1}, which is unique. What is σ^{-1}, just reverse the order of the rows,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

This group is non-commutative if $n \geq 3$ then S_n is not commutative. If we an integer $1 \leq k \leq n$ and take k elements $\{a_1, a_2, \ldots, a_k\} \subset \{1, 2, 3, \ldots, n\}$. Then we define

Definition 1.2 (k-cycle)**.** A k cycle, $\sigma = (a_1, a_2, \ldots, a_k) \in S_n$ is a permutation,

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ a_2 & a_3 & \ldots & a_k & a_1 \end{pmatrix}$$

A k-cycle is a permutation and a bijection as you only write each number from 1 to n once. The 1-cycle is just the identity. The 2-cycle is the transposition. Then onwards it just shifts elements around. We can count the number of k-cycles, which is,

$$\frac{n(n-1)\ldots(n+k-1)}{k}$$

We can now see the dihedral group D_{2n},

Definition 1.3 (Dihedral Group)**.** Let us take the n-gon ($n \geq 3$) and depending on when n is odd or even we have a vertex along with the vertex one, you get them lying on the y-axis. Then you get all the rotations symmetries in the plane, which maps the n-gon to itself. There are $2n$ of them, the rotation clockwise with angle $\frac{2\pi}{n}$, there are n of these. Then we have the elements where we flip the shape, s, first where $s^2 = 1$.

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

Then this is our $2n$ elements. This is indeed a group with composition of rotations and $n \geq 3$ then the group isn't abelian. We also have the interesting rule which spits out the non-commutative behavior, *Lecture 2*

$$sr^i = r^{-i}s = r^{n-i}s$$

We can describe the group by it's elements and it's composition rule. We can define D_4 quite nicely,

$$D_4 = \{1, r, s, sr\}$$

and we find this to be commutative. Hence, D_4 is abelian.

Lemma 1.4. The following are true:

- The natural element is unique
- The inverse of each element is unique
- $(ab)^{-1} = b^{-1}a^{-1}$
- $au = av \implies u = v$ and $ub = vb \implies u = v$.
- Exponentiation makes sense
- Associativity means that any string of elements combined with the composition rule can be done in any order.

1.1 Subgroups and Orders

Definition 1.5 (Subgroup)**.** A subgroup, $H \subset G$, of a group $(G, \cdot)$,

- $\forall x, y \in H, x \cdot y \in H$
- $\forall x \in H, x^{-1} \in H$

This leads to also us being able to say $x \cdot x^{-1} = e_G \in H$, so the natural element must also be in H.

Example.
- $(G, \cdot)$ is a subgroup of itself.
- We can take the trivial subgroup $\{e_G\}$.
- Given a $m \in \mathbb{Z}$ the subset $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ of integers is a subgroup of $(\mathbb{Z}, +)$.
- If we take $\{1, r, r^2, \dots, r^{n-1}\}$ this is a subgroup of D_{2n}.

Definition 1.6 (Order of an element)**.** Let G be a group and $a \in G$. The order of a is,

$$\operatorname{ord}(a) = \min\{n \geq 1 : a^n = e_G\}$$

If you never reach the natural element, we call $\operatorname{ord} a$ to be infinite.

Lemma 1.7. The following are true,

- $\operatorname{ord} a = 1$ if and only if $a = e_G$
- Let $0 \neq n \in \mathbb{Z}$, then $\operatorname{ord} n = \infty$
- Every element in a finite group must have finite order. As if the order was infinite, then you must have infinitely elements, namely, $\{1, a, a^2, a^3, \dots, a^i, a^{i+1}, \dots\}$ which are all distinct and so G cannot be finite.
- Consider some $k = \operatorname{ord} a < \infty$ and $n \geq 1$ with $a^n = e_G$, then $k \mid n$

  Proof. We have instantly that $n \geq k$ and now let $n = tk + r$ with $0 \leq r < k$. Then, $a^n = a^{tk+r} = a^{tk} \cdot a^r = (a^k)^t a^r = e_G^t a^r = a^r = e_G$. Hence, we can say that $r = 0$ as n is the smallest number such that $a^n = e_G$. □

If we consider the symmetric group, then we can say,

Lemma 1.8. Let $n \geq k \geq 1$ and $\sigma = (a_1, a_2, \dots, a_k) \in S_n$ and is a k-cycle. Then $\operatorname{ord} \sigma = k$. Further, if $\sigma \in S_n$ then one can write $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_m$ and we can find the order of this disjoin composition of cycles. We find that this is, $\operatorname{ord}(\operatorname{lcm}(\tau_i))_{i=0}^m$

Remark. Disjoint cycles commute and the decomposition is unique.

Lecture 3

Lemma 1.9. If we take $\mathbb{Z}_n$, then we can take the order of say $[k]$, then we say that,

$$\operatorname{ord}[k] = \frac{n}{\gcd(n, k)}$$

Definition 1.10 (Generator)**.** If G is a group, $a \in G$, the subset $H = \{a^n : n \in \mathbb{Z}\}$ of G consisting of all powers of the element a is a subgroup, and is called the cyclic subgroup of G generated by a, and a is called a generator of H. The subgroup is denoted by $\langle a \rangle$.

Definition 1.11 (Cyclic Group)**.** A group G is called cyclic if $\exists\, a \in G$ such that $G = \langle a \rangle$ equals the (sub)group generated by a.

Lemma 1.12. If a group is generated by a, it is also generated by a^{-1}

Proof. If we have any a, then we can write this: $a = (a^{-1})^{-1}$ and so the generator is not unique. □

We notice that this works because we can cycle around n and this can be proved using Euclidean division.

Example.
- $\mathbb{Z} = \langle 1 \rangle$, is an infinite cyclic group generated by 1. NB! Here $a^n = a \cdot n$
- on a similar note, $\mathbb{Z}_n = \langle [1]_n \rangle$. However, we can go further! If $k \geq 1$, with $\gcd(k, n) = 1$, then $\mathbb{Z}_n = \langle [k]_n \rangle$ is also generated by $[k]_n$. This is proved as $\text{ord}[k]_n = \frac{n}{\gcd(k,n)} = n$ and so the order is the group and so $H = \langle k \rangle = \mathbb{Z}_n$.
- We can talk about $H = \langle (1234) \rangle$, which is a cyclic subgroup of S_4.

Definition 1.13 (Product of Groups)**.** Let $(G, \circ)$ and $(H, *)$ be two groups. We define a new group $(G \times H, \cdot)$ called the product group of G and H, as follows,

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

is the set-theoretic product of G and H. The composition law $(\cdot)$ is defined by,

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$$

The from this, the rest of the group axioms follow trivially.

Lemma 1.14. Let $(G, \circ)$ and $(H, *)$ be groups. If G and H are abelian, then so is $G \times H$. If both G and H are finite, then so is $G \times H$ and $|G \times H| = |G||H|$

Proof. Assume that G, H are abelian, and $g_1, g_2 \in G$ and $h_1, h_2 \in H$ then $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) = (g_2 \circ g_1, h_2 * h_1) = (g_2, h_2) \cdot (g_1, h_1)$, hence abelian. If both groups are finite, then the number of elements in $G \times H$ is the same as the number of pairs of elements and so that must be $|G| \times |H|$. □

1.2 Homomophism

Lecture 4

Definition 1.15 (Homomophism)**.** Let there be a group $(G, \circ)$ and $(H, *)$ and define a homomophism from $G \to H$ which satisfy,

(i) For $g_1, g_2 \in G$, $f(g_1 \circ g_1) = f(g_1) * f(g_2)$

(ii) $f(e_G) = e_H$

If we take $\mathbb{Z} \to \mathbb{Z}_n$ then we define the map $f(k) = [k]_n$ and we can see this by, $f(k_1 + k_2) = [k_1 + k_2]_n = [k_1]_n + [k_2]_n = f(k_1) + f(k_2)$

$$\begin{aligned} f(k_1 + k_2) = [k_1 + k_2]_n & \\ &= [k_1]_n + [k_2]_n \\ &= f(k_1) + f(k_2) \end{aligned}$$

So this is a homomophism and it's surjective. If we let $f : \mathbb{Z} \to \mathbb{Z}$ and have $m \to km$ and this is also a homomorphism.

$$\begin{aligned} f(k_1 + k_2) &= m(k_1 + k_2) \\ &= mk_1 + mk_2 \\ &= f(k_1) + f(k_2) \end{aligned}$$

Definition 1.16 (Image)**.** Let $f : G \to H$ be a homomorphism, we define the image as,

$$\operatorname{Im} f = \{h \in H \mid \exists\, g \in G, h = f(g)\}$$

Definition 1.17 (Kernel)**.** Let $f : G \to H$ be a homomorphism, we define the kernel as,

$$\operatorname{Ker} f = \{g \in G \mid f(g) = e_G\}$$

For example, consider $f : \mathbb{Z} \to \mathbb{Z}_n$ where $f(k) = [k]_n$ and so we can say $\operatorname{Ker} f = \{nz \mid z \in \mathbb{Z}\}$, we notice this is a subgroup. However, if $g : \mathbb{Z} \to \mathbb{Z}$ where $z \mapsto mz$ we say $\operatorname{Ker} g = \{0\}$ if $m \neq 0$, another subgroup. This leads us to the following lemmas,

Lemma 1.18. $\operatorname{Im} f$ is a subgroup of H and $\operatorname{Ker} f$ is a subgroup of G.

Proof. The first part, follows quite nicely from absorbing and splitting using the definition of group homomorphisms. the second part is also follows nicely, so we verify the subgroup axiom,

- Closure, $g_1, g_2 \in \operatorname{Ker} f$ and so, $f(g_1) = f(g_2) = e_H$ and show $f(g_1 \circ g_2) = f(g_1) * f(g_2) = e_H * e_H = e_H$.
- If $f(g) = e_H$ then prove $f(g^{-1}) = e_H$ and so, $e_H = f(g \circ g^{-1}) = f(e_G) = f(g) * f(g^{-1})$, hence, $f(g^{-1}) = (f(g))^{-1}$. Hence, $f(g)^{-1} \in \operatorname{Ker} f$.

□

Lemma 1.19. Let $f : G \to H$ be a homomorphism.

- f is surjective if and only if $\operatorname{Im} f = H$.
- f is injective if and only if $\operatorname{Ker} f = e_G$

Proof. Assume that f is injective, so $\operatorname{Ker} f = \{e_G\}$, so if $g \in \operatorname{Ker} f$ then $g = e_G$. We also know that the kernel also always contains e_G and g and we know f is injective and so $g = e_G$ as they both map to e_H. Now suppose that $\operatorname{Ker} f = \{e_G\}$ and show that f is injective. Take $g_1, g_2 \in G$ and assume that $f(g_1) = f(g_2)$. We get $f(g_1) \circ f(g_2)^{-1} = e_H$ and so, $f(g_1 \circ g_2^{-1}) = e_H$ and hence, we must have $g_1 \circ g_2^{-1} \in \operatorname{Ker} f$. However $\operatorname{Ker} f = \{e_G\}$ and so, $g_1 \circ g_2^{-1} = e_G$ and so, $g_1 = g_2$. □

2 Cosets and Normal Subgroups

Consider G be a group an consider a subgroup H of G. We want to define the left coset, but before we define a relation, *Lecture 5*

Definition 2.1 (Relation)**.** $x \sim y \implies x^{-1}y = h \in H$

This can then be proved to be an equivalence relation,

Proof. (i) Reflexive, $x \sim x$ which means $x^{-1}x = e_G \in H$ as H is a subgroup.

(ii) Symmetry, $x \sim y \implies y \sim x$. If $x \sim y$, $y = xh$ implies $yh^{-1} = x$ but $h^{-1} \in H$ and so $y \sim x$.

(iii) Transitivity, $x \sim y$ and $y \sim z$ then $x \sim z$. We have $y = xh$ and $z = yh'$ and so $z = yhh'$ and $hh' \in H$ and so $x \sim z$.

□

Now we can consider equivalence classes of elements of this relation, which is,

$$\overline{x} = \{x \sim y \mid y \in G\} = \{xh \mid h \in H\} = xH$$

Definition 2.2 (Left Coset)**.** We define the left coset as this equivalence relation.

We also know that equivalence classes form a partition,

$$G = \bigcup_{x \in G} \overline{x} = \bigcup_{x \in G} xH$$

Cosets are also not unique, we can have $x_1H = x_2H$ when $x_1 \sim x_2$.

If we consider all of the left cosets $(G/H)_{\text{left}} = \{xH : x \in G\}$. If G is finite, so there are finitely many left cosets. This is the index of $H \in G$ and denoted, $|G : H|$

Example. Consider $\mathbb{Z}$ and $n\mathbb{Z}$ as our groups, then if we consider $a \sim b$ this is just saying $-a + b \in n\mathbb{Z}$, however this just says $b - a \in n\mathbb{Z}$ which is the definition for divisibility. Let $a \in \mathbb{Z}$, then $a = kn + r$, then we can say $a \sim r$ which is equivalent to $\overline{a} = \overline{r}$. Hence,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} = n\mathbb{Z}$$

Theorem 2.3 (Legrange's Theorem)**.** Let G be a group and H be a subgroup. Then,

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

Proof. Firstly, we aim to show that all left cosets have the same number of elements, more specifically $|H| = |xH|$. We aim to find a bijection $H \to xH$, we can try $x \mapsto xh$. Now prove this is a bijection, surjectivity is obvious, so prove injectivity. Hence we prove that if $\phi(h_1) = \phi(h_2)$ then $h_1 = h_2$. We have that $xh_1 = xh_2$ and so injectivity is clear. So we can say that $|H| = |xH|$, and as we know,

$$G = \bigcup_{x \in G} xH$$

then $|G| = |G : H||H|$ □

Corollary 2.4.

– Let G be a finite group and H a subgroup. Then $|H| \mid |G|$.

– Let G be a finite group and $x \in G$ then $\text{ord}(x) = |\langle x \rangle| \mid |G|$

Theorem 2.5 (Cauchy's Theorem)**.** Let G be finite group and let p be a prime, then if $p \mid |G|$, then you can find a subgroup and an element of order p

We will see sylows theorem later, which is a converse to Legranges theorem and instead of relating just to p, it related to p^n.

Suppose that H is a subgroup, we have seen a left coset, xH. We can do the same with Hx which is the right coset. In general $xH \neq Hx$ as the group law is not generally commutative, as we want $xh = h'x$. However this works for more than just commutativity, so we define a normal subgroup.

2.1 Normal Subgroups

Definition 2.6 (Normal Subgroup)**.** A subgroup H of G is called normal if,

$$xH = Hx = \{h'x : h' \in H\} \qquad \forall\, x \in G$$

Lets consider a non-example,

Example. Consider $K = \langle s \rangle$ of D_8 and we claim it's not normal, so $rK = Kr$. We have $H' = \{1, s\}$ and $rK = \{r, rs = sr^2\}$ and $Kr = \{r, sr\}$[1]. However, $Kr \neq rK$ as $sr \neq sr^2$. Hence, not normal.

Definition 2.7 (Conjugate)**.** Two elements $g, h \in G$ if we can find a $x \in G$ such that, *Lecture 6*

$$g = xhx^{-1}$$

and we call it the conjugate of g by x.

If we consider a subgroup to be normal we must have $Hx = xH$, this is equivalent to saying $H = xHx^{-1} = \{xhx^{-1} : h \in H\}$. This can be seen by writing $xh = hx$.

Lemma 2.8. If we have a group homeomorphism $\phi : G \to H$, then $\operatorname{Ker}\phi$ is a normal subgroup.

Proof. So we have to prove that any $g \in \operatorname{Ker}\phi$ and then $xgx^{-1} \in \operatorname{Ker}\phi$ and so consider $f(xgx^{-1}) = f(x)f(g)f(x^{-1}) = f(x)e_H f(x)^{-1} = f(x)f(x)^{-1} = e_H$ as so $xgx^{-1} \in \operatorname{Ker}\phi$ as required. □

Now we will consider the symmetry group. If we have some $\sigma \in S_n$, then we can decompose a σ uniquely as $\sigma = (a_1\, a_2\, \ldots\, a_{n_1}) \ldots (b_1\, b_2\, \ldots\, b_{n_k})$. The k-tuple of $(n_1\, n_2\, \ldots\, n_k)$ is called the cycle type of σ.

Example. The permutation $(1\,2)(3\,4\,5\,6)$ has type (2, 4).

Proposition 2.9. If two permutations are conjugate if and only if they have the same cycle type.

Proof. In notes □

Consider our permutation $\sigma = (1\,2)(3\,4\,5\,6)$ and another one of the same type $\widetilde{\sigma} = (3\,4)(1\,2\,5\,6)$ then there exists $\tau \in S_6$ such that $\widetilde{\sigma} = \tau\sigma\tau^{-1}$ we write out,

$$\begin{aligned} \sigma &\quad (1\,2)(3\,4\,5\,6) \\ \widetilde{\sigma} &\quad (3\,4)(1\,2\,5\,6) \\ \tau &\quad (1\,3)(2\,4)(5)(6) \end{aligned}$$

The important thing is that, τ is not unique. Note, that in S_3 all three elements must be conjugate. We have two three cycles and two transpositions, and we know that a two cycle can't be conjugate to a three cycle, which shows the power of this proposition.

In S_n we have a subgroup A_n (the subgroup of even permutations). If $\sigma = (a_1\, a_2\, \ldots\, a_k)$, ie. a k-cycle.

[1] Check this

Definition 2.10 (Signature)**.** If we consider $\varepsilon : S_n \to \{\overline{0}, \overline{1}\}$ and consider a new map, $\sigma \mapsto \varepsilon(\sigma)$ where we define,

$$\varepsilon(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases}$$

A k-cycle can be considered as a product of transpositions is to start with $\sigma = (a_k\, a_{k-1})\,(a_{k-2})(a_{k-3})\dots(a_1\, a_0)$. We can also say that A_n is normal as if we consider ε we really have $\mathbb{Z}/2\mathbb{Z}$ and we have a homomorphism, ie. $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$. The kernel is just the even permutations, A_n. Hence, A_n is normal.

Take two $\sigma_1, \sigma_2 \in A_n$, when are they conjugate in A_n? Hence find, $\tau \in A_n$ such that $\sigma_2 = \tau\sigma_1\tau^{-1}$. We need them to find two of the same cycle type, but we see that this τ doesn't exist. Consider $A_4 = \{e, (1\,2\,3), (a\,b)(c\,d)\}$, if we look to the product of transpositions, they are conjugate, but if we look at the three cycles, $(1\,2\,3)(1\,3\,2)$ there doesn't exist a $\tau \in A_4$.

2.2 Quotient Groups

We are going to consider a factor group, so we are going to start with H, a normal subgroup of G. *Lecture 7*

Definition 2.11 (Quotient Group Law)**.** We define a composition law $(\cdot)$ on the set of left cosets G/H by,

$$(\cdot) : G/H \times G/H \to G/H$$
$$(xH, yH) \mapsto xH \cdot yH = xyH$$

This is well defined as H is normal, $x'H = xH$ and $y' = yH \implies x'y'H = xyH$.

Proposition 2.12. $(G/H, \cdot)$ is a group and it is called the quotient group of G by H

Proof. Associativity can be checked quickly, then $e_{G/H}$ is just $e_GH = H$, we can see this by $e_GH \cdot xH = e_gxH = xH$. The inverse, is just $x^{-1}H$, then we see, $xHx^{-1}H = xx^{-1}H = e_GH = H$ □

Now consider $\phi : G \to G/H$ and get $\phi(g) = gH$. This is a group homomorphism.

Proposition 2.13. The map ϕ is a group homomorphism and $\operatorname{Ker}\phi = H$.

Proof. The fact that ϕ is surjective is clear as $gH = \phi(g)$. It is a homomorphism as,

$$\phi(g_1g_2) = g_1g_2H = (g_1H) \cdot (g_2H) = \phi(g_1)\phi(g_2)$$

We now show that $\operatorname{Ker}\phi = H$, first $H \subset \operatorname{Ker}\phi$ since if $g \in H$, then $e_G^{-1}g = g \in H$ and $e_G \sim g$ hence $\phi g = gH = e_GH$. Conversely let $g \in \operatorname{Ker}\phi$ meaning $\phi g = gH = e_GH$, then $e_G \sim g$ and $e_G^{-1}g = g \in H$. □

2.2.1 First Isomorphism Theorem

Theorem 2.14 (First Isomorphism Theorem)**.** Suppose $f : G \to H$ is a group homomorphism. The quotient group $G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$

Proof. Consider $\pi : G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ defined by $\pi(g\operatorname{Ker}(f)) = f(g)$ and we show π is a group isomorphism. Firstly, check π is well defined. Assume $g\operatorname{Ker}(\pi) = g'\operatorname{Ker}(\pi)$ meaning $g'^{-1}g = \widetilde{g} \in \operatorname{Ker}(\pi)$. Then,

$$\begin{aligned} f(g) &= f(g'\widetilde{g}) \\ &= f(g')f(\widetilde{g}) \\ &= f(g')e_H \\ &= f(g') \end{aligned}$$

since $\widetilde{g} \in \operatorname{Ker}(f)$. Further π is a homomorphism:

$$\begin{aligned}\pi(g\operatorname{Ker}(f) \cdot g'\operatorname{Ker}(f)) &= \pi(gg'\operatorname{Ker}(f)) \\ &= f(gg') \\ &= f(g)f(g') \\ &= \pi(g\operatorname{Ker}(f))\pi(g'\operatorname{Ker}(f))\end{aligned}$$

The homomorphism is surjective, if $f(g) \in \operatorname{Im}(f)$, $g \in G$, then $f(g) = \pi(g\operatorname{Ker}(f))$. It is also injective, assume $f(g) = \pi(g\operatorname{Ker}(f)) = \pi(g'\operatorname{Ker}(f)) = f(g')$, then $f(g')^{-1}f(g) = f(g'^{-1}g) = e_H$ and $g'^{-1}g \in \operatorname{Ker}(f)$and so $g\operatorname{Ker}(f) = g'\operatorname{Ker}(f)$. □

Corollary 2.15. Suppose G is finite, and we have a group homomorphism, $f : G \to H$, then,

$$\frac{|G|}{|\operatorname{Ker}(f)|} = |\operatorname{Im}(f)|$$

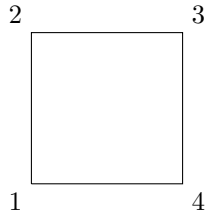
Proof. As $G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$ then if G is finite, then everything is finite. Further, we can say $|G/H| = |\operatorname{Im} f|$, now applying Legranges Theorem, we get the result,

$$\frac{|G|}{|\operatorname{Ker} f|} = |\operatorname{Im} f|$$

□

3 Group Actions

Groups acts on sets and so we can focus our attention to something called group actions. Let's start with a motivating example. Consider D_8, which is linked to the four vertices of a square. We can consider a rotation of $\frac{\pi}{2}$ and s which is just the symmetry. D_8 acts on the vertices $1, 2, 3, 4$ *Lecture 8*



What it does to this square is just a group action.

Definition 3.1 (Group Action)**.** Let $(G, *)$ be a group and a set A. A group action is a map,

$$(\cdot) : G \times A \to A$$

$$(g, a) \mapsto g \cdot a$$

satisying,

$$(g_1 * g_2) \cdot a = g_1 \cdot (g_2 \cdot a) \quad \forall\, g_1, g_2 \in G, \quad a \in A \tag{1}$$

$$e_G \cdot a = a \quad \forall\, a \in A \tag{2}$$

A group can act on itself, in two ways; by left multiplication and conjugation.

Definition 3.2 (Action by left multiplication)**.** Consider $(\cdot) : G \times G \to G$ and define $(h, g) \mapsto h \cdot g = h * g$. Axiom (1) is satisfied,

$$(h_1 * h_2) \cdot g = (h_1 * h_2) * g = h_1 * (h_2 * g) = h_1.(h_2.g)$$

and axiom (2) is also satisfied.

Definition 3.3 (Action by conjugation)**.** A group $(G, *)$ acts on itself defined by $(h, g) \mapsto (h \cdot g) = h * g * h^{-1}$. Now check the axioms,

$$\begin{aligned}(h_1 * h_2) \cdot g &= (h_1 * h_2) * g * (h_1 * h_2)^{-1} \\ &= (h_1 * h_2) * g * (h_2^{-1} * h_1^{-1}) \\ &= h_1 * (h_2 * g * h_2^{-1}) * h_1^{-1} \\ &= h_1 \cdot (h_2 \cdot g)\end{aligned}$$

The second axiom is also satisfied.

We are now going to consider a permutation action, if we have a map, $\tau_g : A \to A$ such that $\tau_g(a) = g \cdot a$ and this is a bijection. It has an inverse, $t_{g^{-1}} : A \to A$,

$$\tau_{g^{-1}} \circ \tau_g = \tau_g \circ \tau_{g^{-1}} = \mathrm{id}_A$$

Or more precisely,

$$\begin{aligned}(\tau_{g^{-1}} \circ \tau_g)(a) &= \tau_{g^{-1}}(\tau_g(a)) \\ &= \tau_{g^{-1}}(g \cdot a) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} * g) \cdot a \\ &= e_G \cdot a \\ &= a\end{aligned}$$

Definition 3.4 (Permutation Representation)**.** Let $(S_A, \circ)$ be the group of all bijections from $A \to A$; S_A is the group of symmetries of A, the group law is just composition of bijections. The map,

$$\tau : G \to S_A$$

is defined by,

$$\tau(g) = \tau_g$$

is a group homomorphism,

$$\begin{aligned}\tau(g_1 * g_2)(a) &= (g_1 * g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \tau_{g_1}(\tau_{g_2}(a)) \\ &= (\tau(g_1) \circ \tau(g_2))(a)\end{aligned}$$

and we call τ the permutation representation associated to the action $(\cdot)$.

If A is finite, say $|A| = n$, then we can list the elements of $A = \{a_1, \ldots, a_n\}$ and label them. This isn't unique, but then what is the group of bijections? It's just S_n.

We now define the kernel of a representation,

Definition 3.5 (Kernel of representation)**.** The kernel of $\tau : G \to S_A$

$$\operatorname{Ker} \tau = \{g \in G : \tau_g = \mathrm{id}_A\} = \{g \in G : g \cdot a = a\}$$

is just the kernel of the representation τ. If we find $\operatorname{Ker} \tau = \{e_G\}$, or τ is injective, we say $(\cdot)$ is faithful.

Lecture 9

3.1 Stabilisers and Orbits

Consider a group G acting on a set A,

Definition 3.6 (Stabiliser)**.** We define the following set called the stabiliser

$$\operatorname{Stab}(a) = \{g \in G : g \cdot a = a\}$$

Remark. These are the elements that when acted on g doesn't change it. They fix g.

The interesting thing is that

Proposition 3.7. $\operatorname{Stab}(a)$ is a subgroup of G.

Proof. We begin by seeing that $e_G \cdot a = a$ and so $e_G \in \text{Stab}(a)$. Then we can prove that $g^{-1} \in \text{Stab}(a)$,

$$a = e_G \cdot a = (g^{-1} \cdot g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$$

Furthermore, let $g_1, g_2 \in \text{Stab}(a)$ and then,

$$(g_1 * g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$$

□

Let us define a relation amoung elements of a non-empty set, $a \sim b \iff \exists\, g \in G : a = g \cdot b$

Proposition 3.8. This relation is an equivalence relation.

Proof. Simple. □

Definition 3.9 (Orbit)**.** Let $a \in A$. The equivalence class of a for the relation $\sim$ is,

$$\overline{a} = \{b \in A : \exists\, g \in G, b = g \cdot a\} = \{g \cdot a : g \in G\}$$

is called the orbit of a, for the given action, ad is denoted $\text{orb}(a)$.

We note that also,

$$A = \bigcup_{a \in A} \text{orb}(a)$$

meaning A is equal to the disjoint union of its orbits under the given action of G.
The action is transitive if there is only one orbit in which case this orbit necessarily contains all elements of A. In this case, $A = \text{orb}(a)$ for every $a \in A$.

Example. For example consider the action,

$$\begin{aligned} S_n \times \{1, 2, \ldots, n \ &\to \{1, 2, \ldots, n\} \\ (\sigma, i) &\mapsto \sigma(i) \end{aligned}$$

Then this is transitive as we just have to find that for any i and j we can map i to j. Hence, if $i = j$, then take the identity. Otherwise, take the transposition (ij).

Theorem 3.10 (The Orbit-Stabiliser Theorem)**.** Assume $(G, *)$ is a group acting on a set A and G is finite. Then the orbit $\text{orb}(a)$ of an element $a \in A$ is finite and,

$$|\,\text{orb}(a)| = \frac{|G|}{|\,\text{Stab}(a)|}$$

Proof. Consider the map,

$$f : \text{orb}(a) to (G/\,\text{Stab}(a))$$

defined by,

$$f(g \cdot a) = g \cdot \text{Stab}(a)$$

We check that this map is well defined, it is. Then we prove that this is injective and it is surjective. Then f is a bijection. Hence, we get nicely the result. □

Recall the left regular representation of G on itself by left multiplication. Assume G is of finite cardinality n. If we lavel the elements of G as $\{g_1, \ldots, g_n\}$ the regular representation defined a faithful permutation representation (an injective homomorphism), *Lecture 10*

$$\rho : G \to S_n$$

called the regular permutation representation defined as followed,

Definition 3.11 (Regular permutation representation)**.** If $g \in G$, $\rho(g)$ is the permutation defined for $i, j \in \{1, \ldots, n\}$ by,

$$\rho(g)(i) = j \qquad \text{if } g * g_i = g_j$$

The permutation representation ρ depends on the give labelling of the elements of G. In particular, since $\operatorname{Ker}\rho = \{e_G\}$ we obtain by the FIT that G is isomorphic to it's image $\rho(G)$; a subgroup of S_n. Hence, we obtain,

Theorem 3.12 (Cayley's Theorem)**.** A finite group of cardinality n is isomorphic to a subgroup of S_n.

Next, we define the left action of a group G on the set of left cosets of a given subgroup. Let H be a subgroup of G and $A = (G/H)_{left}$ the set of left cosets of H. The group G acts on A by

$$g \cdot (g'H) = (g * g')H$$

This action is called the action of G on the left cosets of H by left multiplication. If $|G : H| = m$ is finite, and we lavel the elementsof A as $\{g_1H, \ldots, g_mH\}$, then the above representation defines a homomorphism

$$\tau : G \to S_m$$

as follows: if $g \in G$, $\tau(g)$ is the permutation defined for $i, j \in \{1, \ldots, m\}$ by

$$\tau(g)(i) = j \qquad \text{if } g \cdot g_jH = (g * g_i)H = g_jH$$

The permutation representation τ depends on the given labelling of the elements of A.

Let $\tau_H : G \to S_{G/H}$ be the permutation representation associated to the action of G by left multiplication on the left cosets of H. Thus if $g \in G$,

$$\tau_H(g) : G/H \to G/H$$

is the bijection defined by,

$$\tau_H(g)(g'H) = (g * g')H$$

Theorem 3.13. The following hold,

- G acts transitively on G/H.
- The stabiliser of e_GH is the subgroup H.
- $\operatorname{Ker}(\tau_H) = \bigcap_{x \in G} xHx^{-1}$, and $\operatorname{Ker}(\tau_H)$ is the largest normal subgroup of G contained in H.

Proof.

- Let $aH, bH \in G/H$ and $g = b * a^{-1}$. Then

$$\begin{aligned} g \cdot (aH) &= (b * a^{-1}) \cdot aH \\ &= (b * a * a^{-1})H \\ &= bH \end{aligned}$$

- The stabiliser of e_GH is

$$\begin{aligned} \{g \in G : g.(e_GH) = gH = H\} &= \{g \in G : gH = H\} \\ &= H \end{aligned}$$

– By definition,

$$\begin{aligned}\mathrm{Ker}(\pi_H) &= \{g \in G : g \cdot (xH) = xH, \forall\, x \in G\} \\ &= \{g \in G : (g * x)H = xH, \forall\, x \in G\} \\ &= \{g \in G : (x^{-1} * g * x)H = H, x \in G\} \\ &= \{g \in G : x^{-1} * g * x \in H, \forall\, x \in G\} \\ &= \{g \in G : g \in xHx^{-1}, \forall\, x \in G\} \\ &= \bigcap_{x \in G} xHx^{-1}\end{aligned}$$

Further $\mathrm{Ker}(\pi_H)$ is a normal subgroup of both G and H. Now let N be a normal subgroup of G contained in H then $N = xHx^{-1} \subset xHx^{-1}$, $\forall\, x \in G$ hence, $N \subset \bigcap_{x \in G} xHx^{-1} = \mathrm{Ker}(\pi_H)$. This shows that $\mathrm{Ker}(\pi_H)$ is the largest subgroup of G contained in H.

□

Corollary 3.14. Let G be a finite group of cardinality n and p the smallest prime number dividing $n = |G|$, then any subgroup of G of index p is normal. In particular, if G has a subgroup of index 2 then this subgroup must be normal.

Proof. Let $H \leq G$ and then π_H is the permutation representation by the multiplication of left cosets of H in G. Let $K = \mathrm{Ker}\, pi_H$ and so $|G : K| = |G : H||H : K| = pm$.

Since H has p left cosets, G/K is isomorphic to a subgroup of S_p ($\pi_H(G)$) by the FIT. By Lagrange's Theorem, $pm = |G/K| \mid |S_p| = p!$. Thus $m \mid \frac{p!}{p} = (p-1)!$. But all prime factors of $(p-1)! < p$ and by the minimality of p, every possible prime divisor of $m \geq p$. This forces $m = 1$ as $m \mid |G|$, so $H = K$ is a normal subgroup of G (since K is normal): the equality $|H : K| = 1$ just means that $H = K$. □

4 Class Equation

4.1 Normalisers, Centralisers and Centers

Lecture 11

We are going to consider the class equation which relates to conjuagtion. We are going to consider the subsets of G, $\mathcal{S}(G) = \{A \subset G\}$, these arent necessarily subgroups, they are just subsets. Then we have the following action,

$$(\cdot) : G \times \mathcal{S}(G) \to \mathcal{S}(G)$$
$$(g,\, A) \mapsto gAg^{-1} = \{gag^{-1} : a \in A\}$$

If you have a group action, you have a stabiliser and an orbit.

$$\text{Stab}(A) = \{g \in G : gAg^{-1} = A\}$$

and this is the normaliser.

Definition 4.1 (Normaliser)**.** The stabiliser of the above group action,

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

The normaliser is a subgroup of G as it is just a stabiliser. The normaliser of a acts on A itself,

$$\phi_A : N_G(A) \times A \to A$$
$$(g, a) \mapsto gag^{-1}$$

this is a group action and we are interested in this group action. We can go deeper and find the stabiliser of ϕ_A,

$$\text{orb}(a) = \{gag^{-1} : g \in N_G(A)\}$$
$$\text{Stab}(a) = \{g \in N_G : gag^{-1} = a \iff ga = ag\}$$

Hence the stabiliser is just the commuting elements of this. Hence, we now look towards the kernel of ϕ_A and we say that,

Definition 4.2 (Centraliser)**.** We say that the kernel of the ϕ_A is the centraliser,

$$C_G(A) = \text{Ker}\,\phi_A = \bigcap_{a \in A} \text{Stab}(a) = \{g \in N_A(a) Lgag^{-1} = a,\, \forall\, a \in A\}$$

and these are just all the commuting elements.

and we know that

Lemma 4.3. The $C_G(A)$ is always a normal subgroup of $N_G(A)$.

Now we ask, what happens when $A = G$ and so we ask, what is $N_G(G)$? G, and what is $C_G(G)$? Well we write it out,

$$Z(G) = \{g \in G : gh = hg,\, \forall\, h \in G\}$$

and this is called the center of G.

Definition 4.4 (Center of G)**.** The center is a normal abelian subgroup of G such that,

$$Z(G) = \{g \in G : gh = hg,\, \forall\, h \in G\}$$

Example. If G is abelian, then $Z(G) = G$, so we are only interested when G is not abelian.

We also note that the center is contained in the centraliser of every subset of A. The center is the intersection of all subsets of $A \in G$.[2]

[2] check this

4.2 The Class Equation

Let us consider $g \in G$ and the subset $\{g\} \subset G$, then,

$$N_G(\{g\}) = C_G(\{g\}) = \{h \in G : hgh^{-1} = g\} = \{h \in G : hg = gh\}$$

This is then the subgroup of elements that commute with g. We note that $C_G(g) = \mathrm{Stab}(g)$ is precisely the stabiliser of g under the conjugation action of G onto itself. The orbit of $\{g\}$ under conjuagtion is,

$$\mathrm{orb}(g) = \{hgh^{-1} : h \in G\}$$

and consists of all elements of G which are conjugate to g.
We note that $\mathrm{orb}(g) = \{g\} \iff hgh^{-1} = g$ for all $h \in G$ and this is equivalent to $g \in Z(G)$. Thus,

$$|\,\mathrm{orb}(g)| = 1 \iff g \in Z(G)$$

Now assume that G is finite. The orbit-stabiliser theorem states that,

$$|\,\mathrm{orb}(g)| = \frac{|G|}{|C_G(g)|}$$

The congugacy classes of elements of G form a partition of G

$$G = \bigcup_{g \in G} \mathrm{orb}(g)$$

where the union is disjoint. By the above discussion, we have,

$$Z(G) = \bigcup_{g \in G,\, |\,\mathrm{orb}(g)| = 1} \mathrm{orb}(g)$$

where the union is over all of these elements of G with $|\,\mathrm{orb}(g)| = 1$. Let $\{\mathrm{orb}(g_1), \ldots, \mathrm{orb}(g_r)\}$ be the distinct conjuagacy classes of G that are **not** contained in $Z(G)$. Then,

$$G = Z(G) \bigcup \left(\bigcup_{i=1}^{r} \mathrm{orb}(g_i) \right)$$

Counting the number of elements of G, and soncisdering the relation $|\,\mathrm{orb}(g_i)| = |G : C_G(g_i)|$, we find the class equation:

Theorem 4.5 (The Class Equation)**.** Let G be a finite group and $\{\mathrm{orb}(g_1), \ldots, \mathrm{orb}(g_r)\}$ be the distinct conjuagacy classes of G which are **not** contained in $Z(G)$, then,

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Lecture 12

Theorem 4.6. If p is a prime and $|G| = p^m$ then $Z(G)$ is non-trivial.

Proof. Considering the class equation, we know $p \mid |G|$ and we claim $p \mid |G : C_G(g_i)|$, this is true as $|G : C_G(g_i)| \mid |G|$ but as $|G| = p^m$ we must know that $|G : C_G(g_i)|$ is a power of p and so $p \mid |G : C_G(g_i)|$ and so hence know that $p \mid Z(G)$ and it must be non-trivial. □

Here a weaker version of sylows theorem,

Theorem 4.7 (Cauchy's Theorem)**.** Let G be a finite group and p a prime number which divides $|G|$. Then there exists an element of G of order p, and a subgroup of G of cardinality p.

4.2.1 Conjuagacy Classes of S_n

We will now look to find all of the cycles that commute with some cycle σ.

Take $1 \leq m \leq n \in \mathbb{Z}$ and say $\sigma = (a_1\, a_2\, \dots\, a_m) \in S_m$. There are $\frac{n(n-1)\dots(n+m-1)}{m}$ and this is $|\operatorname{orb}(\sigma)|$ and so using orbit-stabiliser theorem,

$$\frac{n!}{|C_{S_n}(\sigma)|} = \frac{n(n-1)\dots(n+m-1)}{m}$$

and so we get that,

$$|C_{S_n}(\sigma)| = (n-m)!m$$

We can determine this centraliser in a nicer way. The centraliser is just $\{\tau \in S_n : \tau\sigma = \sigma\tau\}$ and we know that $\{\sigma^i\tau, \}$ where $0 \leq i \leq m-1$ and τ is disjoint. Looking at the cardinality of this set, we find that it's just $m(n-m)!$, which says that we must just have the centraliser as $C_{S_n}(\sigma) = \{\sigma^i\tau\}$.

4.3 Simple Groups

Simple groups are not simple.

Definition 4.8 (Simple Groups)**.** G is simple if the only normal subgroups of G are $H = G$ and $H = \{e_G\}$.

Theorem 4.9. A_5 is a simple subgroup.

Proof. We consider all the different cycles in A_5, you have

$$1 \qquad (1\,2\,3) \qquad (1\,2\,3\,4\,5) \qquad (1\,2)(3\,4)$$

Now we count the amount of each cycle. There are one 1-cycles. There are 20 3-cycles, 24 5-cycles and 15 of the rest. Now let us find their orbits.
We consult the orbit-stabiliser theorem. We see that,

$$|\operatorname{orb}_{A_5}((1\,2\,3))| = \frac{|A_5|}{|C_{A_5}((1\,2\,3))|}$$

We can find the centraliser in S_5 so we then take that and consider $C_{A_5}((1\,2\,3)) = C_{S_5}((1\,2\,3)) \cap A_5$ and so we see that $C_{A_5}((1\,2\,3)) = 3$. Hence,

$$|\operatorname{orb}_{A_5}((1\,2\,3))| = \frac{|A_5|}{|C_{A_5}((1\,2\,3))|} = \frac{60}{3} = 20$$

and so all 3-cycles conjugate in S_5 are conjugate in A_5.
We now do the same for the 5-cycles. We find that $|\operatorname{orb}_{A_5}((1\,2\,3\,4\,5))|$. Then we see that there are two conjugacy classes with both cardinality 12.
Now for the last type. We can check that there is no odd permutation such that it commutes. Hence the cardinality of the centraliser of this is even and it divides $|A_5|$ and so we see it must be 15.

Now suppose H is normal, now it must be the union of the conjuagacy classes. Find ways to sum, $\{1, 12, 12, 15, 20\}$ to make 60. There is only way to do this, by adding them all together. Hence it's either 1 or 60 and so A_5 is simple. □

5 Sylow's Theorems

Suppose we have a finite group G, $|G| = n$. We know if we have a subgroup, then the cardinality of the subgroup we know this divides n. Sylows Theorems regards the converse of this, if we have some $k \mid n$, is there some H such that $|H| = k$. Sylow's Theorems provides an answer, but only for positive powers of primes. *Lecture 13*

Suppose we have some prime p, such that $|G| = p^r \cdot m$, where $r \geq 1$ and $\gcd(m, p) = 1$. If we have a group that has cardinality that is some p^r, this is a p-group. If we have some p-group, then any subgroup is also a p-group. The subgroups of some group G, that are p-groups, are called the p-subgroups of G. More formally,

Definition 5.1 (p-group)**.** Let p be a prime number. A group of cardinality p^t for some $t \geq 1$ is called a p-group. A non-trivial subgroup of a p-group is a p-group.

These p-subgroups, which have maximal cardinality, ie. if $|H| = p^r$, then we call this the Sylow p-subgroup.

Definition 5.2 (Sylow p-group)**.** If we consider a group G, such that $|G| = m \cdot p^r$, then the subgroups H_i, cardinality $|H_i| = p^r$ is called the Sylow p-groups.

Remark. We can consider a Sylow p-group for each prime in the prime decomposition of $|G|$.

If we consider the set of all Sylow p-groups,

$$\operatorname{Syl}_p(G) = \{H \subset G : |H| = p^r\}$$

and we consider $|\operatorname{Syl}_p(G)|$, we say $|\operatorname{Syl}_p(G)| = n_p(G)$

Sylow's Theorem tells us that for any power of $p^i \mid |G|$ there exists a subgroup with cardinality p^i, in particular there exists p-Sylow Subgroups, ie. $n_p(G)$ is non-empty.

Example. Let's consider S_3 and we know $|S_3| = 6$ and so we can consider a 3-Sylow subgroup. We get $\{1, (1\,2\,3), (1\,3\,2)\}$, ie. the subgroup generated by a 3-subgroup. Now we consider the 2-Sylow subgroups, there are 3 of them. There are something very special about the number of these subgroups.

There are four statements,

Theorem 5.3 (Sylows Theorems)**.** Let p be a prime such that $p \mid |G|$,

(i) $n_p(G)$ is nonempty, there exists subgroups of cardinality p^i for every $p^i \mid |G|$. Every p-subgroup is contained a p-Sylow subgroup. In fact we find that a p-Sylow subgroup is just the elements of order p^i.

(ii) Any two p-Sylow groups must be conjugate. They form an orbit on G by the action of conjuagation.

(iii) (a) The number of p-Sylow subgroups $\equiv 1 \mod p$. It also says that the number of Sylow subgroups must divide m.

(b) The number of p-Sylow subgroups is just the index of the normaliser of the p-sylow subgroups.

We now are going to try and focus on the proof of each of these. We need more than orbit-stabiliser theorem. Let us consider a finite p-group which acts on a finite set. We consider the congruence and point formula.

Suppose we have a group $|H| = p^r$ and H acts on a finite set, then let's look at what happens to the orbits of some $x \in X$.

$$\operatorname{orb}(x) = \{h \cdot x : h \in H\}$$

and we know

$$|\operatorname{orb}(x)| = \frac{|H|}{|\operatorname{Stab}(x)|}$$

let us see what happens, the first possibility is that $|\operatorname{orb}(x)| > 1$, this means that $\operatorname{Stab}(x) \neq H$ and $p \mid |\operatorname{orb}(x)|$ as $|H| = p^r$. Conversely, if $|\operatorname{orb}(x)| = 1$, then $\operatorname{Stab}(x) = H$, hence $h \cdot x = x$ for any $h \in H$. If you have a group action and an element that satisfies this, then we call it the fixed point.

Definition 5.4 (Fixed Point)**.** Consider a group H acting on a set X and take a $x \in X$. Then if $h \cdot x = x$ for all $h \in H$, then we say that x is a fixed point of the action.

We know that,

$$X = \bigcup_{x \in X} \operatorname{orb}(x)$$

and now we can distinguish the elements of cardinaliy one and not one.

$$X = \bigcup_{|\operatorname{orb}(x)|=1} \operatorname{orb}(x) + \bigcup_{|\operatorname{orb}(x)|>1} \operatorname{orb}(x)$$

Then, of course as X is finite we can count this, we get the cardinality of the set of fixed points in the first union. In the second union, we get a sum of some powers of p.

$$X = |\{x \in X : \forall\, h \in H, h \cdot x = x\}| + \bigcup_{|\operatorname{orb}(x)|>1} \operatorname{orb}(x)$$

Then we consider this $\mod p$, then the second union disappears, for conveniance, let us call $\operatorname{Fix}_H(X) = \{x \in X : \forall\, h \in H, h \cdot x = x\}$

$$|X| \equiv |\operatorname{Fix}_H(G)| \mod p$$

This is the congruence point formula, or fixed point congruence formula.

Theorem 5.5 (Fixed Point Congruence)**.** Let H be a finite p-group acting on a finite set X and $\operatorname{Fix}_H(X)$ is the subset of fixed points of X under this action. Then,

$$|X| \equiv |\operatorname{Fix}_H(G)| \mod p$$

Corollary 5.6. Let H be a finite p-group on a finite set X. Suppose $\gcd(|X|, p) = 1$, then there exists fixed points.

5.1 Proof of Sylow I

Proof of Sylow I. We will prove a stronger result, take any $1 \leq i \leq r-1$ and take a subgroup of G of cardinality of p^i. There exists some $H \subset H' \subset G$ and $|H'| = p^{i+1}$. We will prove this by induction on i.
For $i = 1$, this is just Cauchy's Theorem. This implies $\exists\, H = \langle x \rangle \subset G$ and $|H| = p$.
Now we assume that there is a H' such that $H \subset H' \subset G$ where $|H| = p^r$, and hence prove that there exists some other H'' that satifies the chain condition but $|H''| = p^r$. To do this we consider the action,

$$H \times G/H \to G/H$$

$$(h, gH) \mapsto hgH$$

and now we consider the fixed points of this action. Hence,

$$|G/H| \equiv |\operatorname{Fix}_H(G/H)| \mod p$$

Let $gH \in \operatorname{Fix}_H(G/H)$. Then $\forall\, h \in H$ we have,

$$hgH = gH \iff hg \in gH \iff g^{-1}hg \in H$$
$$g^{-1}Hg \subset H \iff g^{-1}Hg = H \iff g \in N_g(H)$$

where the forth step follows from $|g^{-1}Hg| = |H|$. Thus,

$$\operatorname{Fix}_H(G/H) = \{gH : g \in N_G(H)\} = N_G(H)/H$$

and so,

$$|G/H| \equiv |N_G(H)/H| \mod p$$

We know that $|H| = p^i$ and then $p \mid |G/H| = p^{r-i}m$ it then divides $|N_G(H)/H|$ by the fixed point congruence formula. Then we consult Cauchy's Theorem, $N_G(H)/H$ has a subgroup of order p which is of the form $\hat{H}/H$ where $\hat{H} \subset N_G(H)$ containing H. Thus, we can say $|\hat{H}/H| = p$ and so, $|H'| = p|H| = p^{i+1}$.
Then we can continue this, until we reach a subgroup of order G of order p^r which must be a p-sylow subgroup of G. □

5.2 Proof of Sylow II

Sylow II says that all p-sylow subgroups are conjugate. *Lecture 14*

Proof of Sylow II. Let P and Q be Sylow subgroups of G, we show there exists some $g \in G$ such that $Q = pPg^{-1}$. Consider the action,

$$Q \times G/P \to G/P$$
$$(g',\, gP) \mapsto g'gP$$

Since Q is a finite p- group we have the fixes point congruence,

$$|G/P| \,|\, |\operatorname{Fix}_Q(G/P)| \mod p$$

As P is a Sylow p-group of G, $|G/P| = m$ is not $0 \mod p$, hence $|\operatorname{Fix}_Q(G/P)|$ is not $0 \mod p$. The later implies that $g'g \in gP$ for all $g' \in Q$, which implies $g' \in gPg^{-1}$ for all $g' \in Q$ hence $Q \subset gPg^{-1}$. This implies the equality $Q = gPg^{-1}$ since both Q and gPg^{-1} have the same cardinality p^r. Hence, P and Q are conjugate. □

5.3 Proof of Sylow III

Sylow III says that the number of Sylow subgroups is congruent to $1 \mod p$.

Proof of Sylow III. We know that there are at least one sylow subgroups. Let us take $P \in \operatorname{Syl}_p(G)$. Consider the action,

$$P \times \operatorname{Syl}_p(G) \to \operatorname{Syl}_p(G)$$
$$(g,\, Q) \mapsto gQg^{-1}$$

due to Sylow II we know that gQg^{-1} is also a p-subgroup. We apply the fixed point congruence theorem,

$$|\operatorname{Syl}_p(G)| \equiv |\operatorname{Fix}_P(\operatorname{Syl}_p(G))| \mod p$$

Sylow III says that $|\operatorname{Fix}_P(\operatorname{Syl}_p(G))| \equiv 1 \mod p$, but in fact $|\operatorname{Fix}_P(\operatorname{Syl}_p(G))| = 1$. Hence we claim,

Claim. $\operatorname{Fix}_P(\operatorname{Syl}_p(G)) = \{p\}$

Proof. Let $Q \in \operatorname{Fix}_P(\operatorname{Syl}_p(G))$, this means that $gQg^{-1} = Q$, $\forall\, g \in P$. This just means that $g \in N_G(Q)$ and so $P \subset N_G(Q)$, but also we know $Q \subset N_G(Q)$ and Q is always normal in it's normaliser. Apply Sylow II, as we know that both P and Q are p-Sylow subgroups of the normaliser, we can say that under the normaliser $P = hQh^{-1}$ for some $h \in N_Q(G)$ and hence as Q is normal, then $hQh^{-1} = Q = P$. Hence, the only fixed point is just P. Hence, we have proved our claim.

Note when we proved Sylow III, we considered an action by conjuagation, but when we proved Sylow II we considered left multiplication. Here we will consider a slightly different action.

$$G \times \operatorname{Syl}_p(G) \to \operatorname{Syl}_p(G)$$

$$(g, G) = gGg^{-1}$$

Let $P \in \mathrm{Syl}_p(G)$, we consider $\mathrm{orb}(P) = \{g \in G : gPg^{-1}\}$. The orbit is contained in $\mathrm{Syl}_p(G)$ as it's just lots of p-Sylow subgroups. In Sylow II, we proved that any two p-Sylow subgroups are conjuagate, and so we can say that these two subgroups are going to be equal. Hence, there is only one orbit for all p-Sylow subgroups. Now apply Orbit-Stabiliser Theorem,

$$|\operatorname{orb}(g)| = \frac{|G|}{|\operatorname{Stab}(g)|}$$

and so as we know that $|G| = p^r \cdot m$ and $\gcd(p, m) = 1$ and so by Sylow III, we know that $\gcd(|n_p(G)|, p) = 1$. Here we have an integer which is coprime to p which is coprime to $|n_p(G)|$, hence it must divide m. □

Hence, we have proved that $\mathrm{Fix}_P(\mathrm{Syl}_p(G))| = 1$ and that $n_p(G) \mid m$ so we have proved Sylow III. □

In fact we can go further and say precisely that $n_p(G)$ is the number of p-Sylow groups. We aim to show that $n_p(G) = \frac{|G|}{|N_G(P)|}$

Proof of Sylow III †. Let $P \in \mathrm{Syl}_p(G)$, then there is only one orbit by conjugation and so we use a the Orbit Stabiliser Theorem, we know that $\mathrm{Stab}(g) = N_G(P)$. This then says that

$$n_p(G) = |\operatorname{Syl}_p(G)| = |\operatorname{orb}(P)| = \frac{|G|}{|\operatorname{Stab}_G(\{P\})|} = \frac{|G|}{|N_G(P)|}$$

□

Let us take a p-Sylow subgroup of a group G, which is a subgroup of the normaliser of G. This subgroup is normal in the normaliser. We proved $n_p(G) \mid m$, which is the index. If we consider $|G/N_G(P)| = \beta$, we know that $\beta \mid m$. In Sylow III we proved that $n_p(G) \mid m$ and in dagger we proved that $n_p(G) = \beta$.

Corollary 5.7. Let P be a Sylow p-subgroup of a finite group G. Then P is the unique subgroup of G (ie. $n_p(G) = 1$) if and only if P is a normal subgroup of G.

Proof. Note that every conjugate gPg^{-1} of P is a Sylow p-group, and the converse holds by (Sylow II). Thus,

$$\mathrm{Syl}_p(G) = \{gPg^{-1} : g \in G\}$$

Now $n_p(G) = 1$ ($\mathrm{Syl}_p(G) = \{P\}$) if and only if $gPg^{-1} = P$ for all $g \in G$, and so P is normal. □

Again, the Sylows Theorems aren't interesting when the group is abelian as $gPg^{-1} = gg^{-1}P = P$. This means that finite abelian group is easy to understand.

An interesting theorem we never got to cover is that,

Theorem 5.8 (Structure Theorem for finite abelian groups)**.** Every finite group is isomorphic to a product of finite cyclic groups.

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}$$

then this is unique up to isomorphism modulo the following condition; there exists some unique integers such that,

$$a_1 \mid a_2 \mid \ldots \mid a_n$$

Example.

- Let G be a finite abelian group, then for any prime $p \mid |G|$, there exists only one p-Sylow subgroup.
- Take $\mathbb{Z}/2^2\mathbb{Z}$ and $\mathbb{Z}/3^3\mathbb{Z}$ and consider the product. We get an abelian group, with cardinality of $2^2 \times 3^3$ for a 2-subgroup is 2 or 4 and for a 3-subgroup, we must have $3, 6, 9$ and so the 2-sylow must have cardinality 4 and the 3-sylow subgroup must have cardinality 9. We can go further and say that there is only 1 2-sylow and it is $\mathbb{Z}/2^2\mathbb{Z} \times \{0\}$ and the 3-sylow is just $\{0\} \times \mathbb{Z}/3^3\mathbb{Z}$
- Sylows Theorems only tell us about groups with cardinality with one prime, it can't go further. There is no more general theorem past Sylow Theorems.

5.4 Classifying groups through Sylow

We want to use Sylow's Theorems to classify small groups. Cosnider the following example, $|G| = p$, then we know that it's cyclic and we know the subgroup. If we go forward and consider $|G| = pq$, where p and q are distinct. Assume $p < q$ wlog, if we look to the number of q-Sylow subgroups. We know $n_q(G) = 1 + tq$ where $t \geq 0$, but we also know that $n_q(G) \mid p$. As $q > p$, it cannot divide p and so we know that $t = 0$ and so if $Q \in \mathrm{Syl}_q(G)$ then Q must be normal. *Lecture 15*

If we consider p, then we know that $n_p(G) = 1 + sp$ and we know that $n_p(G) \mid q$, but q is a prime, so $n_p(G) = 1$ or $n_p(G) = q$. If $n_p(G) = q = 1 + sp$ and so $q \equiv 1 \mod p$. Hence we either have one normal subgroup or $p \mid q - 1$.

Example. If $p = 5$ and $q = 13$, we know that the 13-Sylow subgroup must be unique and the 5-Sylow subgroup is also unique as $13 \not\equiv 1 \mod 5$.

However, if we take $p = 3$ and $q = 7$, then the 7-Sylow subgroup is unique and normal and the 7-Sylow subgroup is not necessarily unique as $7 \equiv 1 \mod 3$.

If we take $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ here $n_p(G) = n_q(G) = 1$. If we have a group of cardinality of 21 and has 7 3-Sylow subgroups can't be abelian. This can be constructed through semi-direct product.

Let us consider a general group of cardinality 12. Consider $|G| = 2^2 \times 3$, we can say that $n_3(G) \equiv 1 \mod 3$ and it must divide 4 and so it's either 1 or 4. If it's one then G has a normal sylow subgroup. If it's 4, then G is isomorphic to A_4.

Claim. Let G be a group, if $|G| = 12$ and G has four 3-Sylow subgroups then it is isomorphic to A_4.

Proof. We will have four 3-sylow subgroups, $\mathrm{Syl}_3(G) = \{P_1, P_2, P_3, P_4\}$ and we know they form an orbit under conjuagation.

$$G \times \mathrm{Syl}_3(G) \to \mathrm{Syl}_3(G)$$
$$(g, P_i) \mapsto gP_ig^{-1}$$

If we label the three subgroups, we get a permutation representation, hence a homomorphism, $\phi : G \to S_4$ such that $g \mapsto \sigma_g$. We also know that $n_3(G) = \frac{|G|}{|N_G(P_i)|} = 4$ but also we know that $P_i \subset N_G(P_i)$ both of them has three elements and so they must be equal, $P_i = N_G(P_i)$. We consider $\operatorname{Ker}\phi$, we know this is just the intersection of the stabilisers. However, the stabilisers are just the normalisers. Hence,

$$\operatorname{Ker}\phi = \bigcap_{i=1}^{4} N_G(P_i) = \bigcap_{i=1}^{4} P_i$$

P_i are distinct and their cardinality is a prime. Hence, their intersection must be trivial.

$$\bigcap_{i=1}^{4} P_i = e_G$$

Hence, ϕ is injective and so by FIT we have that $G \cong \phi(G)$ as G has eight elements of order 3 and hence so does $\phi(G)$. All three cycles in S_4 are in A_4. So consider $\phi(G) \cap A_4$, $8 \leq |\phi(G) \cap A_4| \mid 12$. Hence $|\phi(G) \cap A_4| = 12$, therefore $\phi(G) \cong A_4$. By transitivity of isomorphisms as $G \cong \phi(G)$, then $G \cong A_4$. □

More generally, $|G| = p^2q$ where p and q are distinct primes. We first consider $q < p$, then $n_p(G) \equiv 1 \mod p \implies n_p(G) = 1 + tp$ and $n_p(G) \mid q$ and these both imply that $t = 0$. Hence there is a unique p-Sylow subgroup that is normal. Now suppose $p < q$, then consider $n_q(G) = 1 + sq$ and $q \mid p^2$. Hence $n_q(G) = 1, p$ or p^2 either $s = 0$, hence we have a unique Sylow subgroup. If $s > 0$ then we have that $q = p^2$ as $q > p$. Hence $sq = p^2 - 1 = (p + 1)(p - 1)$. Hence $q \mid p + 1$. Hence $q = p + 1$. So $p = 2$ and $q = 3$. Hence we have a group of cardinality 12. Therefore $n_q(G) = 1$ or $p = 2$ and $q = 3$ and $|G| = 12 \implies G \cong A_4$. We now move into the second part of the module, we shall now consider sets that have more than one binary operation that follows the group axioms and we call these rings and fields. Firstly, we will formally define polynomials and use this as a motivating example.

6 Polynomials

We start by defining a polynomial, *Lecture 16*

Definition 6.1 (Polynomial)**.** A polynomial with coefficients in $\mathbb{Q}$ is an infinite sequence

$$(a_0, a_1, \dots, a_n, \dots)$$

such that $\exists\, N \geq 0$ with $a_i = 0 \,\forall\, i \geq N$

Further we say that,

$$(a_0, a_1, \dots, a_n, \dots) = (b_0, b_1, \dots, b_n, \dots) \iff a_i = b_i \forall\, i \geq 0$$

Then we can add and multiply polynomials, if we have

$$(a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (c_0, c_1, \dots, c_n, \dots)$$

where $c_i = a_i + b_i \,\forall\, i \geq 0$. We can multiply polynomials, this is slightly more complicated,

$$(a_0, a_1, \dots, a_n, \dots) \times (b_0, b_1, \dots, b_n, \dots) = (d_0, d_1, \dots, d_n, \dots)$$

where, $d_n = \sum_{s+t=i} a_s b_t$.

Notation. Let $X = (0, 1\, 0, \dots)$ and $n \geq 1$ then,

$$X^n = X \times \dots \times X = (0, 0, \dots, 1, 0, \dots)$$

where we see 1 is shifted to the n^{th} digit. Further for all i, $j \geq 0$ we have $X^i X^j = X^{i+j}$

For $a \in \mathbb{Q}$ the polynomial,

$$a = (a, 0, 0, \dots)$$

is called the constant polynomial.

Every polynomial $(a_0, a_1, \dots, a_n, 0, \dots)$ with $a_i = 0$ for all $i > n$ can be written,

$$\begin{aligned}(a_0, a_1, \dots, a_n, 0, \dots) &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, a_n) \\ &= (a_0, 0, \dots) + (a_1, 0, \dots)(0, 1, 0, \dots) + \dots + (a_n, 0, \dots)(0, \dots, 1)\end{aligned}$$

and hence we denote this as $f(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$, then $\{a_i\}_{0 \leq i \leq n}$ are called the coefficients of f. If $a_n \neq 0$, then n is called the degree of the polynomial f and denoted $\deg(f)$. The coefficient of a_n is called the leading coefficient and a_0 is the constant coefficient of f.

Finally, we write,

$$\mathbb{Q}[X] = \{f(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n : n \geq 0,\, a_i \in \mathbb{Q}\}$$

and call it the set of polynomials with rational coefficients. Identifying thr set of constant polynomials with $\mathbb{Q}$ we can view $\mathbb{Q}$ as a subset of $\mathbb{Q}[X]$.

We look at the set $\mathbb{Q}[X]$ and see that $\mathbb{Q} \subset \mathbb{Q}[X]$. We also note that $\mathbb{Q}[X]$ is endowed with two operations $+$ and $\times$.

Lemma 6.2. Given $f, g \in \mathbb{Q}[X]$ we have that $\deg(f + g) \leq \max(\deg(f), \deg(g))$, with equality when $\deg(f) \neq \deg(g)$ and $\deg(f \times g) = \deg(f) \deg(g)$ if f and g are both non-zero.

Proof. Exercise □

Proposition 6.3. $(\mathbb{Q}[X], +)$ is an abelian group.

Proof. It follows from the definition of polynomials that this is commutative, so just prove that it's a group.

(i) The natural element is just the constant polynomial $0 = (0, 0, \dots, 0, \dots)$ as called the zero polynomial, $f(X) + 0 = 0 + f(X) = f(X) \forall f \in \mathbb{Q}[X]$.

(ii) Further the inverse element for $f(X) = a_0 + a_1X + \cdots + a_nX^n$ is just $f(X) = -a_0 + (-a_1)X + \cdots + (-a_n)X^n$. This satisfies $f(X) + (-f(X)) = 0$ hence it is the inverse of $f(X)$.

(iii) Closure and Associativity follow from the definiton.

□

Definition 6.4 (Division)**.** Let $f, g \in \mathbb{Q}[X]$. We say that g divides f if $\exists\, h \in \mathbb{Q}[X]$ such that[3]

$$f(X) = g(X)h(X)$$

Lemma 6.5. Let $u \in \mathbb{Q}[X]$. Then u divides the constant polynomial 1 if and only if u is a non-zero constant polynomial, ie. $u \in \mathbb{Q} \setminus \{0\}$. Such u is called a unit of $\mathbb{Q}[X]$.[4]

Proof. Assume that $u \neq 0 = a_0 \in \mathbb{Q}$ is a non zero constant polynomial. Let $v = \frac{1}{a_0}$ and then $uv = 1$ and u divides 1.
Conversely, let $f(X)$ be a unit with $n = \deg(f)$, ie. $a_n \neq 0$. Then $\exists\, g \in \mathbb{Q}[X], \deg(g) = m$; thus $b_m \neq 0$, such that $fg = 1$. In particular $a_nb_m \neq 0$ and $\deg(fg) = n + m = \deg(1) = 0$, hence $n = m = 0$ and $u = a_0 \neq 0$ □

Definition 6.6 (Irriducible)**.** Let $f \in \mathbb{Q}[X]$ be a non constant polynomial, $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ and $\deg(f) \geq 1$. We say that f is irreducible if whenever $f(X) = g(X)h(X)$ then either g or h is a unit.

We can consider some examples, *Lecture 17*

Example. Here are two examples,

- We can prove that $f(X) = a_0 + a_1X$ is irreducible. This is because $\deg(f) = 1$ and so for $\deg(fg) = 1$, then we must have that $\deg(g) = 0$.
- Consider $f(X) = X^2 - 3$, suppose $X^2 - 3 = (aX + b)(cX + d) = bd + (ad + bc)X + acX^2$ and so we know that $ac = 1$ and $ad + bc = 0$ and $bd = -3$. We claim that these have no solutions, $ad + bc = \frac{d}{c} - \frac{3c}{d} = -\frac{d^2-3c^2}{cd} = 0$ and so $d^2 - 3c^2 = 0$ and so $d^2 = 3c^2$ this must be $c = d = 0$ as we would have an irrational number. This is a contradiction from our original equations. Hence $f(X)$ is irreducible.

Here is the main theorem for polynomials,

Theorem 6.7 (Polynomial Division)**.** Let $f, g \in \mathbb{Q}[X]$ with $g \neq 0$. Then $!\exists\, h, r \in \mathbb{Q}[X]$ such that,

$$f = hg + r$$

where $r = 0$ or $r \neq 0$ and $\deg(r) < \deg(g)$.

Proof. We assume wlog $m \geq n$ and set $d = m - n \geq 0$ (if $m < n$ take $h(X) = 0$ and $r(X) = f(X)$) and continue via induction on d.

For unicity we assume we have h, h' and r and r' then manipulate and reach that they are equal. □

[3] I hold that this is NOT a definition, it is a lemma as this can be proved.
[4] This should be split into a lemma and then a definition

Now we can talk about the uniqueness of our division,

Theorem 6.8 (Unique Factorisation of Polynomials)**.** Let $f \in \mathbb{Q}[X]$ be a non zero polynomial which is not a unit. Then,

$$f = g_1 g_2 g_3 \dots g_n$$

with g_i is irreducible for all $1 \leq i \leq r$. Further if

$$f = h_1 h_2 \dots h_s$$

is another such factorisation, with h_i irreducible for $1 \leq i \leq s$, then $r = s$ and after rearranging the $\{g_i\}$ one has $g_i = u_i h_i$ where u_i is a unit.

This theorem will be superseded with a more general result relating to a ring with prime elements as the factorisation. Hence, I ommit the proof here.

Suppose we have $f(X) \in \mathbb{Q}[X]$ and $c \in \mathbb{Q}$. We define the value $f(c)$ by,

$$f(c) = a_0 + a_1 c + a_2 c^2 + \dots + a_n c^n$$

Thus, f can be viewed as,

$$f : \mathbb{Q} \to \mathbb{Q}$$

defined by,

$$c \mapsto f(c)$$

If $g \in \mathbb{Q}[X]$ is another polynomial then,

$$fg(c) = f(c)g(c) \qquad (f+g)(c) = f(c) + g(c)$$

We also say $\alpha \in \mathbb{Q}$ is a root of f if $f(\alpha) = 0$. In this case we say f has a root in $\mathbb{Q}$.

Lemma 6.9. Let $f \in \mathbb{Q}[X]$, where $\deg(f) \geq 1$. If $c \in \mathbb{Q}$ is a root of f then $X - c$ divides f.w

Proof. By the division algorithm we have that $f(X) = h(X)(X-c) + r(X)$ and $\deg(r) < \deg(X-c) = 1$. Thus $r(X)$ is a constant. Furthermore,

$$\begin{aligned} f(c) &= h(c)(c-c) + r \\ &= 0 + r \\ &= r \end{aligned}$$

Hence, $r = f(c) = 0$ and $f(X) = h(X)(X-c)$. □

Lemma 6.10. Let $f \in \mathbb{Q}[X]$ with $\deg(f) = n \geq 1$. Then f has at most n roots in $\mathbb{Q}$.

Proof. We argue by induction on $n = \deg(f)$. If $n = 1$, then $f(X) = a_0 + a_1 X$ and we see that $X = -\frac{a_0}{a_1}$ is the only root. Suppose the lemma is true for polynomials of degree $< n$. Assume $c \in \mathbb{Q}$ is a root of f. Then by Lemma 6.9 there exists $g \in \mathbb{Q}[X]$ with,

$$f(X) = (X - c)g(X)$$

and $\deg(g) = n - 1$. Assume $c' \neq c$ is another root of f, then,

$$f(c') = (c' - c)g(c') = 0$$

Hence $g(c') = 0$ as $c \neq c'$. By induction there are at most $n - 1$ such c', hence there are at most n roots of f. □

We note here that $\mathbb{Q}$ was not special, we could have done this analysis over any algebraically closed field, so we could have chose $\mathbb{C}$. *Lecture 18*

Theorem 6.11 (The fundemental Theorem of Algebra)**.** Let $f \in \mathbb{C}[X]$ be a polynomial with $\deg(f) \geq 1$. Then $\exists\, c \in \mathbb{C}$ with $f(c) = 0$.

Proof. Because it's me and I have one, here is my favourite proof of this theorem.

Take a polynomial $(p(z) = z^n + a_1 z^{n-1} + \cdots + a_n)$ that has no roots in $\mathbb{C}$ and then consider,

$$f_r(s) = \frac{p(re^{2\pi is})/p(r)}{|p(re^{2\pi is})/p(r)|}$$

which is a loop and as you vary r, you get a homotopy of loops based at 1. Hence, $[f_r] \in \pi_1(S^1)$. Now choose an $r > 1$ and $r > |a_1| + \cdots + |a_n|$. Then for $|z| = r$ we have,

$$|z^n| > (|a_1| + \cdots + |a_n|)|z^{n-1}| > |a_1 z^{n-1}| + \cdots + |a_n| \geq |a_1 z^{n-1} + \cdots + a_n|$$

Now define a $p_t = z^n + t(a_1 z^{n-1} + \cdots + a_n)$ and then define a lift and then use Theorem 1.12 (from my AlgTop notes). This gives, $[\omega_n] = [f_r] = 0$ and hence $n = 0$ and so $p(z) = a_0$ and so that is the only polynomial with no roots and so FTA proved.

□

This tells us that if $n \geq 1$, this polynomial is not irreducible and so there is only polynomials of degree one that are irreducible.

7 Rings and Fields

We consider a set with two composition laws such that $(R, +, \times)$,

Definition 7.1 (Commutative Ring)**.** If we have a set $(R, +, \times)$, then the following is true,

(i) $(R, +)$ is an abelian group.

(ii) $\times$ must be commutative and associative

(iii) Addition and multiplication are distributive, ie.

$$a \times (b + c) = a \times b + a \times c$$

Remark. If $(R, +, \times)$ is not commutative, then (ii) is not true.

We say that R has an identity element if $\exists\, 1_R \in R$ such that,

$$a \times 1_R = a \,\forall\, a \in R$$

Remark. Every ring does not have to have an identity element (See rng).

Notation. We will say $a \times b = ab$ and $a - b = a + (-b)$.

Example. (i) $(\mathbb{Z}, +, \times)$ is a ring with identity 1.

(ii) $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are rings with identity one.

(iii) For $m \geq 1$, $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ is a ring with identity the class $\overline{1}$ of 1.

(iv) $(\mathbb{Q}[X], +, \times)$ is a ring with identity of constant polynomial $f(X) = 1$.

Here are a load of properties of these rings,

Lemma 7.2. Let R be a ring. Then the following hold,

(i) $0_R a = a 0_R = 0_R$, for all $a \in R$

(ii) $\forall\, a,\, b \in R, (-a)b = a(-b)$

(iii) $\forall\, a, b \in R, (-a)(-b) = ab$

(iv) If R has an identity element 1_R then $-a = (-1)_R a$ for all $a \in R$.

Definition 7.3 (Zero Divisor)**.** Let R be a ring. An element $a \in R \setminus \{0_R\}$ is called a zero divisor if $\exists\, b \in R \setminus \{0\}$ such that

$$ab = 0_R$$

Example. Take $\overline{2} \in \mathbb{Z}/4\mathbb{Z}$, this is a zero divisor since $\overline{2} \times \overline{2} = \overline{4} = \overline{0}$.

Proposition 7.4. $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is a prime.

Proof. Firsly assume n is not a prime, $n = n_1 n_2$ with $1 < n_i < n$ hence $\overline{n} = 0 = \overline{n_1 n_2}$ and $\overline{n_i} \neq 0$ is a zero divisor. Converly assume $n = p$ is a prime integer and $\overline{a}\overline{b} = 0 = \overline{p} = \overline{ab}$, then $p \mid ab$ and hence $p \mid a$ or $p \mid b$. □

Proposition 7.5. $\mathbb{Q}[X]$ has no zero divisors.

Proof. Suppose $f(X) \neq 0$, thus $\deg(f) = n \geq 0$ and $a_n \neq 0$ and $g(X)$ similarly but $\deg(g) = m \geq 0$. Then,

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_nb_nX^{n+m} \neq 0$$

since $a_nb_m \neq 0$. □

From now on whenever we assume that R has an identity we suppose $1_R \neq 0_R$ as if $a \in R$ gives $a = a1_R = a0_R = 0_R$ and you get the zero ring.

Definition 7.6 (Unit)**.** Assume R has an identity 1. An element $u \in R$ is called a unit if $\exists\, v \in R$ such that $uv = 1$. We denote v by u^{-1} and call it the inverse of u.

Definition 7.7 (Group of Units)**.** Let R be a ring with identity 1. The set of units of R is denoted

$$R^\times = \{u \in R : u \text{ is a unit}\}$$

We now prove it's a group,

Lemma 7.8. $R^\times$ is closed under multiplication and $(R^\times, \times)$ is an abelian group.

Proof. First $1 \in R^\times$. Let $u_1, u_2 \in R^\times$, there exists $v_1, v_2 \in R$ such that $u_1v_1 = u_2v_2 = 1$. Then $1 = (u_1v_1)(u_2v_2) = (u_1u_2)(v_1v_2)$ hence u_1u_2 is a unit and $(u_1u_2)^{-1} = v_1v_2 = u_1^{-1}u_2^{-1}$. Further let $u \in R^\times$, there exists $v \in R$ such that $uv = 1$ hence $v \in R^\times$ is a unit and $v = u^{-1}$. Hence $R^\times$ is a group and furthermore it's abelian. □

Proposition 7.9. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$

Proof. Suppose $\overline{a} \in (\mathbb{Z}/\mathbb{Z})^\times$ if and only if there exists $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a}\overline{b} = \overline{ab} = \overline{1}$. That is true if and only if there exists $k \in \mathbb{Z}$ such that $ab = nk + 1$ and that is precisely the definition of $\gcd(a, n) = 1$. □

Lecture 19

Example. What are the units in $\mathbb{Z}$? We need $ab = 1$ and so the units are ± 1 and so $\mathbb{Z}^\times = \{-1, 1\} = \langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

We now define an integral domain,

Definition 7.10 (Integral Domain)**.** A ring is called an integral domain if it has no zero divisors

a few motivating examples are that $\mathbb{Z}$ is an integral domain and $\mathbb{Z}/n\mathbb{Z}$ is also an integral domain if and only if n is prime.

Definition 7.11 (Field)**.** A ring F with identity is called a field if $F^\times = F \setminus \{0\}$, or F is a field if every non zero element of F is a unit.

Lemma 7.12. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime integer.

Proof. If $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ then $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\gcd(k, n) = 1$. Hence every non zero element is a unit if and only if n has no positive divisor k such that $1 < k < n$, which is precisely the definition of n being a prime. □

and moreover, we have a special name for this field,

Definition 7.13 (Finite field with p elements)**.** Let p be a prime integer. The field $\mathbb{Z}/p\mathbb{Z}$ is denoted $\mathbb{F}_p$ and called a finite field with p elements.

Now we can link integral domains and fields,

Lemma 7.14. A field is necessarily an integral domain.

Proof. Exercise □

Now for something that really should have been defined before,

Definition 7.15 (Subring)**.** A subset S of a ring R is called a subring if $(S, +)$ is a subgroup of $(R, +)$ and S is closed under multiplication.

We can prove that $\mathbb{Z}[\sqrt{D}] = \{a+b\sqrt{D} : a, b \in \mathbb{Z}\}$ are fields. We also introduce that $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\}$ are called the Gaussian Integers. The Gaussian Integers have very similar properties to the integers. We can prove that $(\mathbb{Z}[\sqrt{-1}])^\times = \{1, -1, i, -i\}$ and its also true that for $D < 0$ then there are usually finitely many units. *Lecture 20*

Let us consider $(\mathbb{Z}[\sqrt{2}])^\times$, then indeed $1 + \sqrt{2}$ is a unit as $(\sqrt{2} - 1)(1 + \sqrt{2}) = 1$. Further we can say $(1 + \sqrt{2})^n$ is a unit, because $(1 + \sqrt{2})^n(\sqrt{2} - 1)^n = 1$ and the set $\{(1 + \sqrt{2})^n : n \in \mathbb{N}_1\}$ has infinite cardinality.

Theorem 7.16 (Dirichlet's Unit Theorem)**.** tbc

8 Ring Homorphisms and Ideals

Firstly, we start with a definition,

Definition 8.1 (Ring Homomorphism)**.** Let R and S be rings. A map $\phi : R \to S$ is called a ring homomorphism if it satisfies,

(i) $\phi(a+b) = \phi(a) + \phi(b) \quad \forall\, ab \in R$

(ii) $\phi(ab) = \phi(a)\phi(b) \quad \forall\, ab \in R$

(iii) $\phi(1_R) = 1_S$

In addition, $\phi(0_R) = 0_S$ and $\phi(-a) = -\phi(a)$ for all $a \in A$.

Again, we say that a ring homomorphism which is a bijection is called an isomorphism.

Example. (i) If we let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and $\phi(a) = \overline{a}$, then this is a ring homomorphism.

(ii) Here is a non-example, let $\phi : \mathbb{Z} \to \mathbb{Z}$ and $\phi(a) = 2a$, if we consider $\phi(ab) = 2ab \neq \phi(a)\phi(b) = 4ab$.

(iii) Here is another ring homomorphism, let $\phi : \mathbb{Q}[X] \to \mathbb{Q}$ and $\phi(a_0 + a_1X + \cdots + a_nX^n) = a_0$. The axioms follow from the definition of addition and multiplication of polynomials.

Now we define the kernel and the image of the homomorphism,

Definition 8.2 (Kernel)**.** Let $\phi : R \to S$ be a ring homomorphism. We define,

$$\operatorname{Ker}\phi = \{r \in R : \phi(r) = 0_S\}$$

and call this set the kernel.

and the image,

Definition 8.3 (Image)**.** Let $\phi : R \to S$ be a ring homomorphism. We define,

$$\operatorname{Im}\phi = \{s \in S : \exists\, r \in R, \phi(r) = s\}$$

and call this set the image.

Example. If we consider $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(a) = \overline{a}$. Then, if $a \in \operatorname{Ker}\phi$, then $\phi(a) = \overline{a} = \overline{0}$ and so $n \mid a$, thus $\operatorname{Ker}\phi = n\mathbb{Z}$.

Here's a lemma,

Lemma 8.4. (i) $\operatorname{Ker}\phi$ is a subring of R

(ii) $\operatorname{Im}\phi$ is a subring of S

(iii) ϕ is surjective if and only if $\operatorname{im}\phi = S$

(iv) ϕ is injective if and only if $\operatorname{Ker}\phi = \{0_R\}$

Proof. Consider (1), then let $a, b \in \operatorname{Ker}\phi$. Then,

$$\phi(a+b) = \phi(a) + \phi(b) = 0_S + 0_S = 0_S$$

and,

$$\phi(ab) = \phi(a)\phi(b) = 0_S 0_S = 0_S$$

Hence, $a+b, ab \in \operatorname{Ker}\phi$.

If $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$ then,

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = s_1 + s_2$$

and

$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2) = s_1 s_2$$

hence $s_1 + s_2, s_1 s_2 \in \operatorname{im}\phi$

The rest follow from group homomorphisms. □

Next is an ideal, this is the interesting one. They were discovered by a german mathematician who as one of the fathers of modern ANT.

Definition 8.5 (Ideal)**.** Let R be a ring. A subset $I \subset R$ is called an ideal if the following hold,

(i) $(I, +)$ is a subgroup of $(R, +)$

(ii) $\forall\, a \in I, b \in R$, it holds that $ab \in I$. Or I is closed under multiplication by arbitrary elements in R.

an interesting thing here, is that these were introduced surrounding finding unique prime factorisations of $\mathbb{Z}[\sqrt{5}]$, it was found that you can't do this. However, if you restrict to ideals then you can define what a prime ideal is and hence you can have unique factorisations of prime ideals.

Example. (i) Let $m \in \mathbb{Z}$, then $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$. If $k \in \mathbb{Z}$, $ma \in m\mathbb{Z}$, then $kma = mka \in m\mathbb{Z}$. This is an example of a principal ideal.

(ii) If we take R a ring and $a \in R$ then consider $(a)_R = \{ab : b \in R\} \subset R$ is an ideal of R, called the ideal generated by a. We note that a, the generator, is not unique, $(a)_R = (-a)_R$, more generally it is unique up to multiplication by units.

Proposition 8.6. $(a)_R$ is an ideal of R

Proof. Exercise □

Lemma 8.7. Let $\phi : R \to S$, $\operatorname{Ker}\phi$ is an ideal of R.

Proof. The first property is known, it suffices to prove the second. Let $a \in \operatorname{Ker}\phi$ and $b \in R$. Then $\phi(ab) = \phi(a)\phi(b) = 0_S\phi(b) = 0_S$, hence $ab \in \operatorname{Ker}\phi$. □

8.1 Construction of the quotient ring

Let R be a ring and I an ideal of R. Recall the relation $\mathcal{H}$ among the elements of R defined by, $a\mathcal{H}b \iff b-a \in I$. The relation $\mathcal{H}$ is an equivalence relation. The equivalence class of $a \in I$ is $\overline{a} = \{b \in R : b = a + c, c \in I\}$. Thus,

$$\overline{a} = a + I = \{a + c : c \in I\}$$

is called the class of a modulo I. Set,

$$R/I = \{\overline{a} : a \in R\}$$

for the set of equivalence classes of elements of R modulo I. We define addition and multiplication as follows,

$$\overline{a} + \overline{b} = \overline{a+b} \qquad (a+I) + (b+I) = a + b + I$$

$$\overline{a} \times \overline{b} = \overline{ab} \qquad (a+I)(b+I) = ab + I$$

We now show this is well defined, i.e. that if $(\widetilde{a}+I)(\widetilde{b}+I)=\widetilde{a}b+I$ aswell as $(a+I)(b+I)=ab+I$ and $a+I=\widetilde{a}+I$ and $b+I=\widetilde{b}+I$. The last relations imply that $a=\widetilde{a}+\alpha$ and $b=\widetilde{b}+\beta$. This then follows from $ab=(\widetilde{a}+\alpha)(\widetilde{b}+\beta)$ and $ab-\widetilde{a}\widetilde{b}=\widetilde{a}\beta+\alpha\widetilde{b}+\alpha\beta$ and we know need to show that $ab-\widetilde{a}b\in I$ and as ideals are closed under multiplication the result follows.

If R is a ring, then R/I is also a ring with this multiplication. We know its an abelian group via addition, so we have to show it's closed under multiplication. We know $ab=\overline{ab}=\overline{ba}=\overline{b}\overline{a}$. We also have distributivity, $\overline{a}(\overline{c}+\overline{d})=\overline{ac}+\overline{ad}$. Also if R has 1_R, $\overline{1_R}=1_R+I$.

Lemma 8.8. Cosnider the map $\phi:R\to R/I$ defined by $\phi(a)=\overline{a}$ for $a\in R$. Then,

(i) ϕ is a ring homomorphism

(ii) $\operatorname{Ker}\phi=I$

Proof. We have already proved (i), so it suffices to prove (ii). Consider $a\in\operatorname{Ker}\phi$, then $\overline{a}=\overline{0}_R$, and this implies that $a-0_R=a\in I$. Hence, $\operatorname{Ker}\phi=I$ as a was arbitrary. □

Example. Here are some examples,

(i) Let $n\in\mathbb{Z}$ and $I=n\mathbb{Z}$, which is an ideal of $\mathbb{Z}$. Our relation $\mathcal{H}$ is the relation modulo n and $\mathbb{Z}/I=\mathbb{Z}/n\mathbb{Z}$ endowed with usual $+$ and $\times$. We know this is a ring.

(ii) Consider $R=\mathbb{Z}[X]$ and,

$$I=\{h(X)=b_2X^2+b_3X^3+\cdots+b_nX^n : b_i\in\mathbb{Z},\ n\geq 2\}$$

is an ideal of $\mathbb{Z}[X]$. We can write our ideas as $X^2(b_2+b_3X+\cdots+b_{n-2}X^{n-2})$ and so we have the principal ideals generated by X^2, hence $I=(X^2)_{\mathbb{Z}[X]}$. If we have $f(X)\in\mathbb{Z}[x]$ then $f(X)-(a_0+a_1X)\in I$ and so, $\overline{f(X)}=\overline{a_0+a_1X}$. Hence every class of a polynomial in $\mathbb{Z}[x]$ modulo I is represented by the class of a polynomial of degree ≤ 1 and,

$$\mathbb{Z}[X]/I=\{\overline{a_0+a_1X} : a_0,a_1\in\mathbb{Z}\}$$

We note in actuality, what happens here is that if we say $\overline{f(X)}=\overline{g(X)}$, then $X^2\mid(f(X)-g(X))$ and we remove any terms that divide X^2 after an operation.

(iii) Now consider $R=\mathbb{Q}[X]$, and,

$$I=(X^2-2)_{\mathbb{Q}[X]}$$

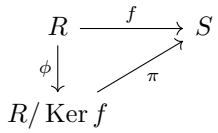
Let $g(X)\in\mathbb{Q}[X]$, then $g(X)=(X^2-2)f(X)+(a_0+a_1X)$ and so $\overline{g(X)}=\overline{r(X)}$. Hence,

$$\mathbb{Q}[X]/I=\{\overline{a_0+a_1X} : a_0,a_1\in\mathbb{Q}\}$$

Now for the first isomorphism theorem for rings, *Lecture 21*

Theorem 8.9 (The First Isomorphism Theorem for Rings)**.** Let $\phi:R\to S$ be a surjective ring homomorphism. Then $R/\operatorname{Ker}\phi\cong S$.

Here is what the theorem says pictorially,



where we say that π is a ring isomorphism. Hence, we just need to justify this, as most of it follows from the FIT for Groups.

Proof. It suffices to prove that $\pi(\overline{a}\overline{b}) = \pi(\overline{a})\pi(\overline{b})$. Firstly we know $\pi(\overline{a}\overline{b}) = \pi(\overline{ab}) = f(ab) = f(a)f(b) = \pi(\overline{a})\pi(\overline{b})$. Hence we have proved the FIT for rings. □

Ideals can be added and multiplied,

Definition 8.10 (Addition and Multiplication of ideals)**.** Suppose we have two ideals, I and J and we define addition,

$$I + J = \{a + b : a \in I, b \in J\}$$

and the product,

$$IJ = \left\{ \sum_{i=1}^{m} a_i b_j : a \in I,\, b \in J\, m \geq 1 \right\}$$

Proof. We aim to prove addition. So we have to prove that it is closed under addition, so suppose that a_1, $a_2 \in I$ and b_1, $b_2 \in J$, then,

$$(a_1 + b_1) + (a_2 + b_2) = \underbrace{(a_1 + a_2)}_{\in I} + \underbrace{(b_1 + b_2)}_{\in J} \in I + J$$

We also note that $0 \in I+J$ as we can write it as $0_R = 0_R+0_R$. The inverse of an element, $(a+b)^{-1} = \underbrace{a^{-1}}_{\in I} + \underbrace{b^{-1}}_{\in J}$. Hence it's a subgroup under addition, so now take an element $a + b \in I + J$, then prove that take a $c \in R$ and then prove $(a + b)c \in I$. Now we distribute, $(a + b)c = ac + bc$, but we know that $a \in I$ and $b \in J$ and so $ac \in I$ and $bc \in J$. Hence, $ac + bc \in I + J$.

Now for the product, so we show it's a subgroup. Firstly, zero, $0_R0_R = 0_R$ and moreover $0_Ra = 0_R$. Now we show it's closed under addition, we show that $a_ib_i \in I$ where $a_i \in I$ and $b_i \in J$ and $c_id_i \in J$ where $c_i \in I$ and $d_i \in I$, then we consider $a_ib_j + c_id_j$, then we know this in IJ as this is just a finite sums of terms where the first term is in I and the second in J. Now we consider $(a_ib_i + c_id_i)^{-1} = (a_ib_i)^{-1} + (c_id_i)^{-1}$ and again this is a finite sum of the required form. Hence this is then just in IJ. We now seek to prove the other property, if $a_ib_i \in IJ$ and $c \in R$, then $c(a_ib_i) = \underbrace{(ca_i)}_{\in I} b_i \in IJ$. □

Remark. It only really makes sense to consider finite sums in groups and rings as we have no sense of a limit as a group does not come inbuilt with limit points. See a topological space (I think).

Lecture 22

Definition 8.11 (Principal Ideals)**.** Let R be a ring,

(i) An ideal $I \in R$ is called principal if $I = (a)_R$ is generated by one element $a \in R$, called a generator of R.

(ii) Let $a, b \in R$ and define $(a,\, b)_R = \{ac+bd : c, d \in R\}$. Then $(a,\, b)_R$ is an ideal called the ideal generated by a and b.

Here is a lemma about inclusion,

Lemma 8.12. Let R be a ring,

(i) $(b)_R \subset (a)_R$ if and only if $b = ac$ for some $c \in R$.

(ii) If R is an integral domain with identity, then,

$$(a)_R = (b)_R \iff a = bu \quad u \in R^\times$$

Proof. ($\longleftarrow$) If $b = b1_R \in (b)_R$ and if it is contained in $(a)_R$, then every element of b must be a multiple of a and so $b = ac$ for some $c \in R$.
($\longrightarrow$) If $b = ac$, then we show $(b)_R \subset (a)_R$, so take an element $br \in (b)_R$ for some $r \in R$. This is an element as $b = (ac)r = a(cr) \in (a)_R$ as it's a multiple of a.

($\longleftarrow$), if $a = bu$, then $(a)_R \subset (b)_R$ from the previous part. However, $b = au^{-1}$ and so $(b)_R \subset (a)_R$ and so $(a)_R = (b)_R$.
($\longrightarrow$) If $(a)_R = (b)_R$, we weaken our statement by using that $(a)_R \subset (b)_R$, hence $a = bu$ for some $u \in R$, now we show that u is a unit. We use the other inclusion, $(b)_R \subset (a)_R$ and so $b = ad$. We use these two identies, $a = (ad)u$, and so $a - (ad)u = 0_R$. We now distributivity, $a(1_R - du) = 0$ and as R is integral, either $a = 0$ or $du = 1_R$, but a is non-zero, so $du = 1_R$, hence, $d = u^{-1}$ and u is a unit. □

Example. (Non-Principal Ideals) Let $R = \mathbb{Z}[X]$ and $I = (2,\, X)_{\mathbb{Z}[X]} = \{2h(X) + Xg(X) : h, g \in \mathbb{Z}[X]\}$ an ideal. Claim that I is not principal. We argue by contradiction, assume that it is principal, $I = (f(X))_{\mathbb{Z}[X]}$ is pincipal generated by some $f(X) \in \mathbb{Z}[X]$. Then, $2 = 2 \times 1 + X \times 0 \in I$. So, $\exists p(X) \in R$ such that $2 = f(X)p(X)$. In particular $0 = \deg 2 = \deg f + \deg g$. which implies that $\deg f = \deg g = 0$ and f is a constant polynomial. Further, since f divides 2 it holds that $f \in \{1, -1, 2, -2\}$. If $f = \pm 1$, then $1 = 2h(X) + Xg(X)$ for some $h, g \in \mathbb{Z}[X]$ which is impossible. So consider $f = \pm 2$, but $X = 0 \times 2 + 1 \times X \in I$. Hence, $X = 2q(X)$ for some $q(X) \in \mathbb{Z}[X]$ which again is impossible.

Example. (Construction of a surjective homomorphism with a given kernel) Let $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$ and $J = (2, 1 + \sqrt{-3})_R$. We want to construct a surjective homomorphism from R to the finite field with kernel J. We want to map $2 \to 0_F$ and $1 + \sqrt{-3} \to 0$. We think about the image of an element $a + b\sqrt{-3} \to f(a + b\sqrt{-3}) = f(a) + f(b)f(\sqrt{-3})$. To make a homomorphism, we must just take the class of that integer as that's the only was to make a homomorphism in $\mathbb{F}_2$. We now consider $f(\sqrt{-3})$, we want to map this to 1, which we can as $-3 = \overline{1}$ and so $f(a + b\sqrt{-3}) = f(a) + f(b)$. Consider the map,

$$f : \mathbb{Z}[\sqrt{-3}] \to \mathbb{F}_2$$
$$f(a + b\sqrt{-3}) = \overline{a} + \overline{b}$$

Our map is surjective as we have infinitely many elements mapping to $\overline{0}$ and infinitely many mapping to $\overline{1}$, forming a dichotemy. Now to check it's a homomorphism

$$\begin{aligned} f\left[(a + b\sqrt{-3}) + (c + d\sqrt{-3})\right] &= f\left[(a + c) + (b + d)\sqrt{-3}\right] \\ &= \overline{a + c} + \overline{b + d} \\ &= \overline{a} + \overline{c} + \overline{b} + \overline{d} \\ &= (\overline{a} + \overline{b}) + (\overline{c} + \overline{d}) \\ &= f(a + b\sqrt{-3}) + f(c + d\sqrt{-3}) \end{aligned}$$

Now for multipicity,

$$\begin{aligned} f\left[(a + b\sqrt{-3})(c + d\sqrt{-3})\right] &= f((ac - 3bd) + (ad + bc)\sqrt{-3}) \\ &= \overline{ac - 3bd} + \overline{ad + bc} \\ &= \overline{ac + bd} + \overline{ad + bc} \\ &= \overline{ac} + \overline{bd} + \overline{a}\overline{d} + \overline{b}\overline{c} \\ &= (\overline{a} + \overline{b})(\overline{c} + \overline{d}) \\ &= f(a + b\sqrt{-3})f(c + d\sqrt{-3}) \end{aligned}$$

So f is a ring homomorphism, so we now show that $\operatorname{Ker} f = (2,\, 1+\sqrt{-3})_R$. Clearly, $J = (2, 1+\sqrt{-3})_R \in \operatorname{Ker} f$ as $f(2) = f(1+\sqrt{-3}) = \overline{0}$. Now for the other inclusion. Let $a+b\sqrt{-3} \in \operatorname{Ker} f$ such that $f(a+b\sqrt{-3})+\overline{a}+\overline{b} = \overline{0}$ and so $a - b = 2k$ for some $k \in \mathbb{Z}$. This $a + b\sqrt{-3} = 2k + b + b\sqrt{-3} = 2k + b(1 + \sqrt{-3}) \in J$, as required.

9 Prime and Maximal Ideals

9.1 Maximal Ideals

Notation. We now introduce some notation $\subsetneq$, this means a proper subset

Definition 9.1 (Proper Ideal)**.** Let R be a ring, then an ideal of R is proper if $I \subsetneq R$.

and now a maximal ideal,

Definition 9.2 (Maximal Ideal)**.** A proper ideal $M \subsetneq R$ is called a maximal ideal if the only ideals of R containing M are M and R.

Now for a proposition,

Proposition 9.3. Let $J \subsetneq R$ be a proper ideal. There exists a maximal ideal M of R containing J, $J \subset M$.

This basically tells us that every ring has a maximal ideal.

Proof. Let $\mathcal{S}$ be the set of all proper ideals of R containing J, $\mathcal{S}$ is nonempty and (partially) ordered by the relation of inclusion. Let $J \subset \ldots I_k \subset I_{k'} \subset \ldots$ with $k, k', \cdots \in K$: an index set, be a chain of ideals containing J. By Zorn's LEmma we need to show that $\{I_k\}_{k\in K}$ has an upper bound. Let $\mathcal{I} = \bigcup_{k\in K} I_k$. Then $\mathcal{I}$ is an ideal of R, if $a, b \in \mathcal{I}$ then $a \in I_k, b \in I_{k'}$ for some $k, k' \in K$. Since the family $\{I_k\}_{k\in K}$ is a chain either $I_k \subset I_{k'}$ or $I_{k'} \subset I_k$, say $I_k \subset I_{k'}$, hence $a + b, ab \in I_{k'} \in \mathcal{I}$. Similary $a \in \mathcal{I}$, $r \in R, \exists\, k \in K$ with $a \in I_k$, hence $ra \in I_k \subset \mathcal{I}$ since I_k is an ideal. Further $1 \notin \mathcal{I}$ for otherwise $\exists\, k \in K$ with $1 \in I_k$ hence $1_k = R$ and clearly $\mathcal{I}$ is an upperbound for $\{I_k\}_{k\in K}$. □

We now consider the Lattice Isomorphism Theorem,

Theorem 9.4 (Lattice Isomorphism Theorem)**.** Let $J \subset R$ be an ideal. There is a one-to-one correspondance between the set of ideals I of R containing J and the set of ideals of the factor ring R/J.

Proof. Let $J \subset I$ be an ideal containing J. The set,

$$I/J = \{\overline{a} \in R/J : a \in I\}$$

is an ideal of R/J. If $a, b \in I$ then $\overline{a} + \overline{b} = \overline{a + b} \in I/J$ and $\overline{a}\overline{b} = \overline{ab} \in I/J$ since $a + b, ab \in I$. Further if $\overline{r} \in R/J$ and $\overline{a} \in I/J$ then $\overline{ra} = \overline{ra}$ since $ra \in I$. Conversely if $\widetilde{I}$ is an ideal of R/J then $I = \phi^{-1}(\widetilde{I})$ where,

$$\phi : R \to R/J$$

$$a \mapsto a + J$$

and so,

$$\phi^{-1}(\widetilde{I}) = \{a \in R : \phi(a) = \overline{a}\}$$

now again we have to show this is an ideal and it contains J. Firstly is it a subgroup? Yes, it has a zero, $\phi(0) = \overline{0}_R \in \widetilde{I}$; if we take $a, b \in I$ then $\phi(a), \phi(b) \in wtI$ and moreover $\phi(a)+\phi(b) = \phi(a+b) \in \widetilde{I} \implies a+b \in I$ and so... then we have that $a \in I$, $\phi(a) \in \widetilde{I}$ we now show that if $c \in R$ then we have closure. We know that $ac \in I$ and so $\phi(ac) \in \widetilde{I}$ and so $\phi(ac) = \overline{ac} = \overline{ac} = \phi(a)\phi(c) \in \widetilde{I}$.
J is just the kernel of this map. Hence, we aim to find $\phi^{-1}(0)$. We know that $0_{R/J} \in \widetilde{I}$ and so $\phi(0_{R/J}) \subset \phi^{-1}(\widetilde{I})$. Furthermore we have that they are inverses. Hence we have a bijection. □

Here is a nice theorem that follows on,

Theorem 9.5. The ideal $M \subseteq R$ is a maximal ideal if and only if the factor ring R/M is a field.

Proof. By the Lattice Isomorphism Theorem there is a one to one correspondence between the set of ideals I of R containing M and the ideals of the factor ring R/M. Now R/M is a field if and only if the only ideals of R/M are R/M and $\{\overline{0}\}$, in which case the corresponding ideals of R containing M are $\phi^{-1}(R/M) = R$ and $\phi^{-1}(0) = \operatorname{Ker}\phi = M$; where $\phi : R \to R/M$ is the map $a \mapsto \phi(a) = \overline{a}$, hence M is a maximal ideal. □

Example. Consider $R = \{f : [0, 1] \to \mathbb{R}\}$, and consider $M_a = \{f \in R : f(a) = 0\}$, then M_a is an ideal of R. The map $\phi : R \to R$ defined by $f \mapsto \phi(f) = f(a)$ is a surjective ring homomorphism and $\operatorname{Ker}\phi = M_a$. The FIT implies R/M_a is isomorphic to $\mathbb{R}$ which is a field and so R/M_a is a field and M_a is a maximal ideal.

More generally if we have a ring isomorphic to a field, then the ring must be a field. This illustrates something important, mainly, we can show an ideal is maximal by showing existence of a surjective homomorphism from a ring to a field with kernel I.

9.2 Prime Ideals

We now talk about prime ideals, they are similar to the notion of prime numbers.

Definition 9.6 (Prime Ideals)**.** A proper ideal $P \subsetneq R$ is a prime ideal if for some $a, b \in R$ and $ab \in I$, then $a \in I$ or $b \in I$

If we consider $\mathbb{Z}/p\mathbb{Z}$ (p is a prime), then we have the ideal $I = p\mathbb{Z}$, then let $a, b \in R$ and $ab \in p\mathbb{Z}$, then $ab = pk$. Then we know that as $p \mid ab$ then $p \mid a$ or $p \mid b$. These two imply that either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Theorem 9.7. The ideal $P \subsetneq R$ is prime if and only if R/P is an integral domain.

Proof. We consider $\phi : R \to R/P$ defined by $\phi(r) = \overline{r}$. As P is prime, then either $a \in P$ or $b \in P$. Also $\overline{ab} = \overline{a}\overline{b} = \overline{0}$, which then implies $\overline{a} = 0$ or $\overline{b} = 0$. Then this is equivalent to it being an integral domain. □

We can also say that R is an integral domain if and only if $\{0\}$ is a prime ideal. If $\phi : R \to D$ is a surjective homomorphism from a ring R to an integral domain D with kernel J then J is a prime ideal. Indeed by the FIT: R/J is isomorphic to the integral domain D hence R/J itself is an integral domain and J is a prime ideal.

Proposition 9.8. A maximal ideal is a prime ideal.

Proof. If M is a maximal ideal, then R/M is a field and so is necessarily an integral domain. Hence M is prime. □

9.3 Field of Fractions

Let R be an integral domain and,

$$\widetilde{F} = \{(a,\, b) : a, b \in R\, b \neq 0_R\}$$

Define a relation $\mathcal{H}$ among the elements of F,

$$(a,\, b)\mathcal{H}(c,\, d) \iff ad = bc$$

The relation $\mathcal{H}$ is an equivalence relation. Let $F = \widetilde{F}/\mathcal{H}$ be the set of equivalence relations of $\mathcal{H}$. Then,

$$F = \left\{ \frac{a}{b} : a, b \in R,\, b \neq 0_R \right\}$$

We define the addition and multiplication in the usual way. Then we have $1_F = \frac{1_R}{1_R}$ and $0_F = \frac{0_R}{1_R}$. Furthermore, F is a field as $\frac{a}{b} \times \frac{b}{a} = 1_F$ where $\frac{a}{b} \neq 0_F$. We call this the field of fractions of R and denote it $\operatorname{Frac}(R)$
Let $K[X]$ be a field, then we can construct the field of fractional polynomials, namely,

$$K(X) = \left\{ \frac{f(X)}{g(X)} : f, g \in K[X],\, g \neq 0 \right\}$$

and it can proved that this is just a field. Every non-zero polynomial has an inverse, $\frac{f}{g} \times \frac{g}{f} = 1_{K(X)}$
We constructed this from an integral domain because we wanted to make every non-zero element invertible.

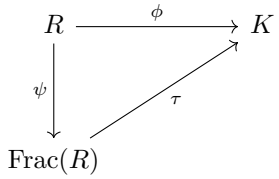
Proposition 9.9. Let R be an integral domain. Then the following holds

(i) The map $\psi : R \to \operatorname{Frac} R$ defined by $\psi(r) = \frac{r}{1_R}$ then this is injective.

(ii) Let $\phi : R \to K$ be an injective homomorphism into a field K. There exists a unique injective homomorphism $\tau : \operatorname{Frac}(K) \to R$ with the property,

$$\tau(\psi(r)) = \tau\left(\frac{r}{1}\right) = \phi(r)$$

In other words, this diagram commutes



Proof. We can see that $\psi(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = \psi(r) + \psi(s)$ and $\psi(rs) = \frac{rs}{1} = \frac{r}{1}\frac{s}{1} = \psi(r)\psi(s)$ and we can also see $\psi(1) = 1$ and so we have a homomorphism. Now we seek to prove that $\operatorname{Ker}\psi = \{0\}$, this can be seen as $\frac{r}{1} = \frac{0}{1} \implies r = 0$ and so we have an injection.

We define $\tau : \operatorname{Frac}(K) \to R$ by,

$$\tau\left(\frac{r}{s}\right) = \phi(r)\phi(s)^{-1}$$

We see that $s \neq 0_R$ and so $\phi(s) \neq 0_K$ and so this makes sense. We want to show that $\tau(\frac{r}{s} + \frac{t}{h}) = \tau(\frac{rh+ts}{sh}) = \phi(rh+ts)\phi(sh)^{-1} = [\phi(r)\phi(h) + \phi(t)\phi(s)]\phi(s)^{-1}\phi(h)^{-1} = \phi(r)\phi(s)^{-1} + \phi(t)\phi(h)^{-1} = \tau(\frac{r}{s}) + \tau(\frac{t}{h})$. Now for the multiplication is slightly simpler, $\tau(\frac{r}{s}\frac{t}{h}) = \tau(\frac{rt}{sh}) = \phi(rt)\phi(sh)^{-1} = \phi(r)\phi(t)\phi(s)^{-1}\phi(h)^{-1} = \tau(\frac{r}{s})\tau(\frac{t}{h})$. Hence, it's a homomorphism. Now we see to prove that the only thing that maps to zero is zero; to see this $\tau(\frac{r}{s}) = \phi(r)\phi(s)^{-1} = 0_K$, then $\phi(r) = 0_{\operatorname{Frac}(R)}$ and so $r = 0$ as ϕ is injective. Hence now we prove uniqueness, we can see that $\tau(\frac{r}{s}) = \tau(\psi(r)\psi(s)^{-1}) = \tau(\psi(r))\tau(\psi(s)^{-1}) = \tau(\psi(r))\tau(\psi(s))^{-1} = \phi(r)\phi(s)^{-1}$ □

The first part implies that $R \subset \operatorname{Frac}(R)$ which is exactly how we think about $\mathbb{Z}$ and $\mathbb{Q}$. The second says that if a field contains R, then it contains $\operatorname{Frac}(R)$, if a field contains $\mathbb{Z}$ then it contains $\mathbb{Q}$.

9.4 Chinese Remainder Theorem

Given two rings R_1 and R_2 we define their product

$$R_1 \times R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$$

and endow it with the operations + and × defined by,

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \qquad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

The set $R_1 \times R_2$ is a commutative ring, with $1 = (1_{R_1}, 1_{R_2})$ and $0 = (0_{R_1}, 0_{R_2})$.

Definition 9.10 (Comaximal)**.** We call two ideal comaximal, if $I + J = R$, if two ideals are comaximal, then $I + J = IJ$.

Theorem 9.11 (Chinese Remainder Theorem)**.** Let I, J be ideals of R. The map,

$$\phi : R \to R/I \times R/J$$

defined by,

$$r \mapsto (r + I,\, r + J)$$

is a ring homomorphism with kernel $I \cap J$. If I and J are co-maximal then this map is surjective and $I \cap J = IJ$, in this case $R/IJ = R/(I \cap J)$ is isomorphic to $R/I \times R/J$.

Proof. We can see that the map ϕ is a ring homomorphism as,

$$\begin{aligned}\phi(r+s) &= (r+s+I,\, r+s+J)\\ &= (r+I,\, r+J) + (s+I,\, s+J)\\ &= \phi(r) + \phi(s)\end{aligned}$$

and

$$\begin{aligned}\phi(rs) &= (rs+I,\, rs+J)\\ &= ((r+I)(s+I),\, (r+J)(s+J))\\ &= (r+I,\, r+J)(s+I,\, s+J)\\ &= \phi(r)\phi(s)\end{aligned}$$

and we can see that $\phi(1) = (1 + I,\, 1 + J) = 1_{R/I \times R/J}$ and so ϕ is a homomorphism. Now we seek to find the kernel of the homomorphism,

$$\operatorname{Ker}\phi = \{(r + I,\, r + J) = (0_{R/I},\, 0_{R/J})\} = \{r \in R : r \in I \text{ and } r \in J\} = I \cap J$$

Now we suppose that $I + J = R$, then we seek to show that ϕ is surjective. There exists some $a + b = 1$ where $a \in I$ and $b \in J$ as $I + J = R$. We see that $a = 1 - b$ and also $b = 1 - a$. Now consider $a + J = 1 - b + J = 1 + (-b + J) = 1 + J$ and also $b + I = 1 + I$. Consider $r = r_2a + r_1b$, then consider

$$\begin{aligned}\phi(r) &= \phi(r_2a + r_1b)\\ &= (r_2a + r_1b + I,\, r_2a + r_1b + J)\\ &= (r_1b + I,\, r_2a + J)\\ &= (r_1 + I,\, r_2 + J)(b + I,\, a + J)\\ &= (r_1 + I,\, r_2 + J)(1 + I,\, 1 + J) = (r_1 + I,\, r_2 + J)\end{aligned}$$

This is then just an arbitrary element of $R/I \times R/J$. Furthermore we know that $\operatorname{Ker}\phi = I \cap J = IJ$, then we can use the FIT to tell us that $R/\operatorname{Ker}\phi = R/(I \cap J) = R/IJ \cong R/I \times R/J$. □

We can generalise this to any n ideals of R.

10 Divisibility and Factorisation

We can consider a R as an integral domain and then define a norm,

Definition 10.1 (Norm)**.** A norm is map from an integral domain to $\mathbb{N}$,

$$N : R \setminus \{0_R\} \to \mathbb{N}$$

We call a norm multiplicative if $N(ab) = N(a)N(b)$ for all $a, b \in R \setminus \{0\}$.

We define a Euclidean Domain by considering division in a similar way to how we consider division in the integers. This is where the norm comes in, it defines how large an element is,

Definition 10.2 (Euclidean Domain)**.** We say that R is a euclidean domain if N is a norm and we have $a \in R$ and $0_R \neq b \in R$ then we can write $a = bq + r$ where $q \in R$ and $r = 0_R$ or $N(r) < N(b)$.

This is slightly abstract, we say that $\mathbb{Z}$ is a ED where we equipt it with the norm $a \mapsto |a|$.
Now we define a PID,

Definition 10.3 (Principal Ideal Domain)**.** Let R be an integral domain, then R is a PID if it has the property if every ideal of R is principal, ie.

$$I = (a)_R = \{ab : b \in R\}$$

Here is a nice characterisation,

Theorem 10.4. R being an Euclidean domain, means R is a principal ideal domain.

Proof. Let $\{0_R\} \neq I \subset R$ be an ideal, then we seek to show that $I = (a)_R$ for some $a \neq 0$. Let

$$n = \min\{N(a) : a \in I,\, a \neq 0\}$$

now for $a \in I$ and with $N(a) = n$. We show that $I = (a)_R$. We can see quickly that $(a)_R \subset I$ as $a \in I$, so it suffices to prove that $I \subset (a)_R$. Now let $b \in I$, then we can write $b = \alpha a + r$, we know that $r = 0$ or $N(r) < N(a)$. We see that $r = b - \alpha a \in I$; now this forces $r = 0$ as we cannot have that $N(r) < N(a)$ by the definition of a. Hence $r = 0$, and so $b = \alpha a$ and so $b \in (a)_R$ and $I \subset (a)_R$. □

Definition 10.5 (Divisble)**.** Let R be a ring, then let $a, b \in R$. Then we say b divides a means that $a = bc$ for some $c \in R$. We write b/a.

and we can define what we mean by a greatest common divisor,

Definition 10.6 (Greatest Common Divisor)**.** A greatest commmon divisor of a and b, say d is described as,

(i) d/a and d/b

(ii) If d'/a and d'/b, then d'/d

This is the same definition as for the integers. We cal note that this isn't unique, if we have $u \in R^\times$, then $ud = \gcd(a, b)$.

Proposition 10.7. Let R be a PID, then $d = \gcd(a, b)$ always exists. Moreover $(d)_R = (a)_R + (b)_R$ and d is unique up to multiplication by a unit. In particular we have a Bezout Identity,

$$d = sa + rb$$

Proof. Both a and b are in $(d)_R$ as we can write it as $a = 1a + 0b$ and $b = 0a + 1b$ and this implies that $a = d\alpha$ and $b = d\beta$. We know that $d \in (d)_R$ and so we can write it as some $d = ra + sb$ and we get the Bezout Identity.

Assume that d' is a common divisor of a and b, ie. $b = d'x$ and $a = d'y$ and so $d = rd'x + sd'y = d'(rx + sy)$ and so d'/d. □

We remark that the gcd(a, b) for some $a, b \in R$ can always be found when R is a Euclidean Domain and it can be computed using Euclidean division.

Proposition 10.8. Every non-zero prime ideal is maximal in a PID.

Proof. Let R be a PID and $P = (p)_R \subset R$. By proposition (?) there exists some maximal ideal $M \subsetneq R$ containing P. We aim to show that $M = P$. As R is a PID, then some $m \in R$ must generate a principal ideal and so $p \in (m)_R$ and so $p = mx$. Since P is prime, either $m \in P$ or $x \in P$. If $m \in P$, then $M = P$ and so the proof is done. Otherwise, if $x \in P$, then $x = py$ for some $y \in R$. Thus $p = xm = pym \implies p(1-ym) = 0$ and so we can see that $ym = 1$ and so m is unit. If m is unit, then $(m)_R = R$, but this violates our assumption for $M \subsetneq R$ and so $M = P$. □

Definition 10.9 (Irreducible, Prime, Associate)**.** Let R be an integral domain,

(i) An element $r \in R \setminus \{0, R^\times\}$ is called irreducible if $ab \in R$ then $a \in R^\times$ or $b \in R^\times$.

(ii) An element $p \in R \setminus \{0, R^\times\}$ is called prime if p/ab then p/a or p/b

(iii) Two elements $a, b \in R$ are associate we write $a \sim b$ if $a = bu$ where $u \in R^\times$

Proposition 10.10. In an integral domain R, a prime element is irreducible

Proof. Let $p \in R$ we show that p is irreducible. Assume that $p = ab$, then p/a then p/b. Suppose that p/a then $a = pr$ for some $r \in R$. Then $p = ab = prb$ and so $p(1 - rb) = 0$ and as $p \neq 0$ then we must have $1 - rb = 0$ as R is an integral domain. Hence we have $rb = 1$ and so b is a unit. □

Definition 10.11 (Unique Factorisation Domain)**.** A UFD is an integral domain R in which every element $r \in R \setminus \{0, R^\times\}$ has the following properties,

(i) $r = p_1 p_2 \dots p_n$ is a product of irreducible elements $p_1, p_2, \dots, p_n$.

(ii) The above factorisation is unique up to associates if $r = q_1 q_2 \dots q_m$ is another factorisation of r as a product of irreducible elements $q_1, q_2, \dots, q_m$ then $n = m$ and after possible renumbering the factors $p_i \sim q_i$ for all i.

We see that $\mathbb{Z}[\sqrt{-5}]$ is the problemed child as $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and we can prove that these factors are irreducible, but not associate. They can proved to be irreducible by considering the norm, for example 2. We consider 2 and say $2 = xy$ and consider the norm and so $4 = N(x)N(y)$ and so if we consider $N(x)$ this must be $1, 2$ or 4. If it is 1, then x is a unit, if $y = a + b\sqrt{-5}$, then $N(y) \neq 2$ and so we now consider $N(x) = 4$, then $N(y) = 1$ and so y is a unit. Hence 2 is irreducible. The non-associate part of the argument follows neatly from inspection.

Proposition 10.12. In a UFD R, an element is prime if and only if it is irreducible.

Proof. We only need to prove that an irreducible element is prime. Let $p \in R$ be an irreducible element and suppose that p/ab, thus $ab = pr$ for some $r \in R$, we must show that p/a or p/b. Write a, b and r as a product of irreducible elements $a = p_1 p_2 \dots p_n$, $b = q_1 q_2 \dots q_m$ and $r = r_1 r_2 \dots r_t$. Thus we have,

$$p_1 p_2 \dots p_n q_1 q_2 \dots q_m = p r_1 r_2 \dots r_t$$

and so, $n + m = 1 + t$ and p must be associate to one of the p_i or q_i. If $p \sim p_i$, then p/a and if $p \sim q_i$, then p/b. □

Proposition 10.13. Let a, b be non-zero elements of a unique factorisation domain R and suppose $a = up_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, $a = vp_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$ are the factorisations of a and b where $u, v \in R^\times$, the primes $p_1, p_2, \dots p_n$ are distinct and the exponents are positive then,

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_n^{\min(e_n, f_n)}$$

Proof. Ommited □

Theorem 10.14 (The Unifying Theorem)**.** A PID is a UFD. In particular an ED is a UFD.

Proof. Ommited □

Remark. Note that there is not a strict subset here,

$$\text{ED} \subsetneq \text{PID} \subsetneq \text{UFD}$$

10.1 Addendum: Why is $\mathbb{Z}[\sqrt{-5}]$ so annoying?

Gauss did a lot of theorems related to Gaussian integers and Cumer and looked at $\mathbb{Z}[\sqrt{-5}]$. We know this isn't a UFD. We proved that $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. He considered a way to return the uniqueness. He worked with the ideals, he considered the ideals $(6)_R = (2)_R(3)_R = (1 + \sqrt{-5})_R(1 - \sqrt{-5})_R$ where $R = \mathbb{Z}[\sqrt{-5}]$. The ideals we considered weren't prime and we can still factorise them and after we **full** factorise them we reach a unique factorisation.

We can construct $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (3)_R$ but neither $1 \pm \sqrt{-5} \in (3)_R$ and so we can still factorise them. We can write $(2)_R = (1 + \sqrt{-5}, 2)_R(1 + \sqrt{-5}, 2)_R = (1 + \sqrt{-5}, 2)_R^2 = p$ and $(3)_R = (1 + \sqrt{-5}, 3)_R(1 - \sqrt{-5}, 3)_R = p_1p_2$ (Exercise). Therefore we now have a prime ideal factorisation. Now if we look to the original identity, $(6)_R = p^2p_1p_2 = pp_1pp_2$ as multiplication of ideals are commutative. Now, we can see a miricle, $pp_1pp_2 = (1 + \sqrt{-5})_R(1 - \sqrt{-5})_R$. Hence the factorisation is unique, but only for ideals. This is exactly why they are called ideals, ideal numbers! Cumer went on to prove several cases of Fermat's Last Theorem. Unfortunately in his full proof he had a mistake that factorisation of irreducible elements is unique and so he discovered this.