

Year 3 — Groups, Rings and Fields

Based on lectures by Professor Mohamed Saïdi

Notes taken by James Arthur

Autumn Term 2021

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Contents

1	Basics of Groups	2
1.1	Subgroups and Orders	4
1.2	Homomorphism	5
2	Cosets and Normal Subgroups	7
2.1	Normal Subgroups	8

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,

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

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 $S_n = \{1, 2, \dots, n\}$ 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.

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

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 there's n possibilities, then for $\sigma(2)$ there's $n-1$ possibilities, then we can't use $\sigma(1)$ or $\sigma(2)$ and hence there's $n-2$ possibilities for $\sigma(3)$ and so on. So we have,

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

□

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 $\{a_1, a_2, \dots, a_k\} \subset \{1, 2, 3, \dots, n\}$. Then we define

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

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

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,

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

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 $s^2 = 1$.

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

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,

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

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

Lemma 1.7. The following are true,

- $\text{ord } a = 1$ if and only if $a = e_G$
- Let $0 \neq n \in \mathbb{Z}$, then $\text{ord } n = \infty$
- 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 $k = \text{ord } a < \infty$ 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 $a^n = e_G$. \square

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 $\text{ord } \sigma = k$. Further, if $\sigma \in S_n$ then one can write $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_m$ and we can find the order of this disjoint composition of cycles. We find that this is, $\text{ord}(\text{lcm}(\tau_i))_{i=1}^m$

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,

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

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. \square

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,

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

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 $|G| \times |H|$. \square

1.2 Homomorphism

Definition 1.15 (Homomorphism). Let there be a group (G, \circ) and $(H, *)$ and define a homomorphism from $G \rightarrow H$ which satisfy,

- (i) For $g_1, g_2 \in G$, $f(g_1 \circ g_2) = f(g_1) * f(g_2)$
- (ii) $f(e_G) = e_H$

If we take $\mathbb{Z} \rightarrow \mathbb{Z}_n$ 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 homomorphism and it's surjective. If we let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ and have $m \rightarrow km$ 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 $f : G \rightarrow H$ be a homomorphism, we define the image as,

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

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

$$\text{Ker } f = \{h \in H \mid f(h) = e_G\}$$

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

Lemma 1.18. $\text{Im } f$ is a subgroup of H and $\text{Ker } f$ 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, $g_1, g_2 \in \text{Ker } f$ 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, $f(g)^{-1} \in \text{Ker } f$.

□

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

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

Proof. Assume that f is injective, so $\text{Ker } f = \{e_G\}$, so if $g \in \text{Ker } f$ 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 $\text{Ker } f = \{e_G\}$ 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 $g_1 \circ g_2^{-1} \in \text{Ker } f$. However $\text{Ker } f = \{e_G\}$ 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 and consider a subgroup H of G . We want to define the left coset, but before we define a relation,

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,

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

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

We also know that equivalence classes form a partition,

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

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 $\bar{a} = \bar{r}$. Hence,

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

Theorem 2.3 (Lagrange'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 $H \rightarrow xH$, 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 Sylow's theorem later, which is a converse to Lagrange's 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,

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

Lets consider a non-example,

Example. Consider $K = \langle s \rangle$ of D_8 and we claim it's not normal, so $rK \neq Kr$. 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,

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

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 $\phi : G \rightarrow H$, then $\text{Ker } \phi$ is a normal subgroup.

Proof. So we have to prove that any $g \in \text{Ker } \phi$ and then $xgx^{-1} \in \text{Ker } \phi$ 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 $xgx^{-1} \in \text{Ker } \phi$ as required. \square

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

Example. The permutation $(12)(3456)$ 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 \square

Consider our permutation $\sigma = (12)(3456)$ and another one of the same type $\tilde{\sigma} = (34)(1256)$ then there exists $\tau \in S_6$ such that $\tilde{\sigma} = \tau\sigma\tau^{-1}$ we write out,

$$\begin{array}{ll} \sigma & (12)(3456) \\ \tilde{\sigma} & (34)(1256) \\ \tau & (13)(24)(5)(6) \end{array}$$

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 $\sigma = (a_1 a_2 \dots a_k)$, ie. a k -cycle.

¹Check this

Definition 2.10 (Signature). If we consider $\varepsilon : S_n \rightarrow \{\bar{0}, \bar{1}\}$ 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 $A_4 = \{e, (123), (ab)(cd)\}$, if we look to the product of transpositions, they are conjugate, but if we look at the three cycles, $(123)(132)$ there doesn't exist a $\tau \in A_4$.