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

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,

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

$\square$

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.

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 $\{1, r, r^2, \ldots, r^{n-1}\}$ 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, $\{1, a, a^2, a^3, \ldots, a^i, a^{i+1}, \ldots\}$ 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 $\sigma = (a_1, a_2, \ldots, a_k) \in S_n$ 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.

Lecture 3