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 Groups

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

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 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,

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

□

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 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,

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

2 Week 2 - stuff

test2