Groups, Rings and Fields Definitions

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 (especially the typos!).

Contents

1 Basics of Groups

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.

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

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

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*

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

1.1 Subgroups and Orders

Definition 1.4 (Subgroup)**.** A subgroup, $H \subset G$, of a group $(G, \cdot)$,

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

Definition 1.5 (Order of an element)**.** Let G be a group and $a \in G$. The order of a is,

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

Definition 1.6 (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 1.7 (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.

Definition 1.8 (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.

1.2 Homomophism

Definition 1.9 (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) $f(e_G) = e_H$

Definition 1.10 (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 1.11 (Kernel)**.** Let $f : G \to H$ be a homomorphism, we define the kernel as,

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

2 Cosets and Normal Subgroups

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

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

2.1 Normal Subgroups

Definition 2.3 (Normal Subgroup)**.** A subgroup H of G is called normal if,

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

Definition 2.4 (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.

Definition 2.5 (Signature)**.** If we consider $\varepsilon : S_n \to \{\overline{0}, \overline{1}\}$ and consider a new map, $\sigma \mapsto \varepsilon(\sigma)$ where we define,

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

2.2 Quotient Groups

Definition 2.6 (Quotient Group Law)**.** We define a composition law $(\cdot)$ on the set of left cosets G/H by,

$$\begin{aligned} (\cdot) : G/H \times G/H &\to G/H \\ (xH, yH) &\mapsto xH \cdot yH = xyH \end{aligned}$$

2.2.1 First Isomorphism Theorem

3 Group Actions

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,

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

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

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.

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 $(\cdot)$.

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.

3.1 Stabilisers and Orbits

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

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

Definition 3.7 (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 $\mathrm{orb}(a)$.

Definition 3.8 (Regular permutation representation)**.** If $g \in G$, $\rho(g)$ is the permutation defined for $i, j \in \{1, \dots, n\}$ by,

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

4 Class Equation

4.1 Normalisers, Centralisers and Centers

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

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

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

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

and these are just all the commuting elements.

Definition 4.3 (Center of G)**.** The center is a normal abelian subgroup of G such that,

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

4.2 The Class Equation

4.2.1 Conjuagacy Classes of S_n

4.3 Simple Groups

Definition 4.4 (Simple Groups)**.** G is simple if the only normal subgroups of G are $H = G$ and $H = \{e_G\}$.

5 Sylow's Theorems

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.

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.

Definition 5.3 (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.

5.1 Proof of Sylow I

5.2 Proof of Sylow II

5.3 Proof of Sylow III

5.4 Classifying groups through Sylow

6 Polynomials

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 $a_i = 0\, \forall\, i \geq N$

Definition 6.2 (Division)**.** Let $f, g \in \mathbb{Q}[X]$. We say that g divides f if $\exists\, h \in \mathbb{Q}[X]$ such that[1]

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

Definition 6.3 (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.

[1] I hold that this is NOT a definition, it is a lemma as this can be proved.

7 Rings and Fields

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.

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

Definition 7.2 (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

$$ab = 0_R$$

Definition 7.3 (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 7.4 (Group of Units)**.** Let R be a ring with identity 1. The set of units of R is denoted

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

Definition 7.5 (Integral Domain)**.** A ring is called an integral domain if it has no zero divisors

Definition 7.6 (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.

Definition 7.7 (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.

Definition 7.8 (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.

8 Ring Homorphisms and Ideals

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 $a \in A$.

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.

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.

Definition 8.4 (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.

8.1 Construction of the quotient ring

Definition 8.5 (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,

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

Definition 8.6 (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.

9 Prime and Maximal Ideals

9.1 Maximal Ideals

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

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.

9.2 Prime Ideals

Definition 9.3 (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 $b \in I$

9.3 Field of Fractions

9.4 Chinese Remainder Theorem

Definition 9.4 (Comaximal)**.** We call two ideal comaximal, if $I + J = R$, if two ideals are comaximal, then $I + J = IJ$.

10 Divisibility and Factorisation

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 $a, b \in R \setminus \{0\}$.

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 $N(r) < N(b)$.

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.

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

Definition 10.4 (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.

Definition 10.5 (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

Definition 10.6 (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 $u \in R^\times$

Definition 10.7 (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) $r = p_1 p_2 \ldots p_n$ is a product of irreducible elements $p_1, p_2, \ldots, p_n$.

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