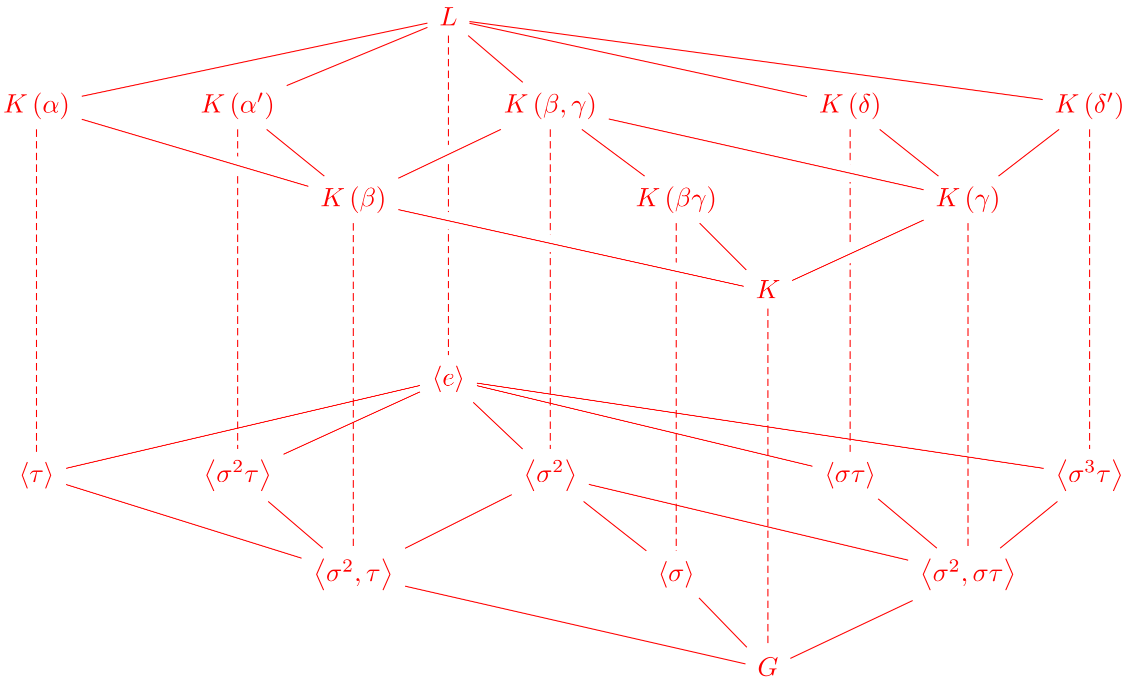
MATH40003B Groups

Lectured by Dr Michele Zordan
Typed by Yu Coughlin

Autumn 2023



$G = \mathrm{Gal}(L/K) \cong \mathcal{D}_8$

Syllabus

This module provides a transition towards the way you will be thinking about, and doing, Mathematics during your degree. It will stress the importance of precise definitions and rigorous proofs, but also discuss their relationship to more informal styles of reasoning which are often encountered in applications of Mathematics. Topics to be covered will include an introduction to abstract sets, functions and relations, common proof strategies, the naturals, rationals and reals, and elementary vector operations and geometry.

Contents

0 Introduction

Lecture 1
Thursday
10/01/19

The following are references.

- E Artin, Galois theory, 1994
- A Grothendieck and M Raynaud, Revêtements étales et groupe fondamental, 2002
- I N Herstein, Topics in algebra, 1975
- M Reid, Galois theory, 2014

Notation. If K is a field, or a ring, I denote the **ring of polynomials** with coefficients in K.

1 Binary operations and groups

Definition 1 (Binary operation)**.** Given a set G a **binary operation** on G is a mapping $\cdot : G \times G \to G$ written $\cdot(g, h) = g \cdot h$ (and sometimes gh) for all $g, h \in G$.

Definition 2 (Group)**.** A **group** is a pair $G = (G, \cdot)$, for some set G and a binary operation $\cdot$, satisfying the following properties:

G1 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$ - the binary operation is **associative**,

G2 $\exists e \in G$ such that $\forall g \in G g \cdot e = e \cdot g = g$ - the is an **identity** element,

G3 $\forall g \in G, \exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ - every element has an **inverse**.

In some literature, the condition of **closure** is also required however this is given in the fact that $\cdot$ is a binary operation on G.

Theorem 3 (Uniqueness)**.** The identity element for some group G is unique. The inverse, g^{-1}, of any element $g \in G$ is also unique.

Lemma 4 (Inverse of product)**.** Given a group G and the elements $g_1, g_2, \ldots, g_n \in G$ we have,

$$(g_1 g_2 \ldots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}.$$

Definition 5 (Abelian Group)**.** If a group G also satisfies the condition $g \cdot h = h \cdot g$ for all $g, h \in G$ - **commutativity**, then G is said to be an **abelian group**.

Definition 6 (Powers of elements)**.** Given a group G and some $g \in G$ the nth **power** of g in G is defined recursively as,

$$g^n := \begin{cases} \text{e} & \text{if } n = 0 \\ g^{n-1} g & \text{if } n > 0 \\ (g^n)^{-1} & \text{if } n < 0 \end{cases}.$$

Definition 7 (Order of group)**.** The **order** of a group G, written $|G|$, is the cardinality of the underlying set of G.

Example 8 (Symmetric group)**.** The **symmetric group of size** n, denoted S_n, is the set of bijections on the interval $[1, n]$, for $n \in \mathbb{N}$, under function composition.

2 Subgroups

2.1 Subgroups

Definition 9 (Subgroup)**.** Given a group $(G, \cdot)$ and a subset $H \subseteq G$ we say $(H, \cdot)$ is a **subgroup** of G, written $H \leq G$, if $(H, \cdot)$ forms a group and

$$\forall h_1, h_2 \in H : h_1 \cdot h_2 \in H.$$

A subgroup, H, is a **proper subgroup** if $H \neq G$. $\{e\}$ is the trivial subgroup.

Theorem 10 (Subgroup test)**.** Given a group $(G, \cdot)$, $(H, \cdot)$ is a subgroup iff:

S1 H is non-empty - **existence**,

S2 for all $h_1, h_2 \in H$ we have $h_1 \cdot h_2 \in H$ - **closure under group operation**,

S3 for all $h \in H$ we have $h^{-1} \in H$ - **closure under inverses**.

2.2 Cyclic groups and orders

Definition 11 (Cyclic group)**.** We say a group G is **cyclic** if there is an element $g \in G$ such that

$$G = \langle g \rangle := \{g^n : n \in \mathbb{N}\}.$$

We say that G is **generated** by g or g is a **generator** of G.

Definition 12 (Order of elements)**.** Given a group G and some $g \in G$, the **order** of g in G, written $\text{ord } g$, is the smallest positive integer n such that $g^n = e$ or ∞ if no such n exists.

Theorem 13. Suppose G is a cyclic group generated by g with $|G| = n$, $\text{ord } g = |\{e, g, g^2, \dots, g^{n-1}\}| = |G| = n$.

Theorem 14. Suppose G is a cyclic group with $G = \langle g \rangle$, the three statements:

1. $H \leq G \implies H$ is cyclic,
2. suppose $|G| = n$ and $m \in \mathbb{Z}$ with $f = \gcd(m, n)$,

$$\langle g^m \rangle = \langle g^d \rangle \text{ and } |\langle g^m \rangle| = \frac{n}{d}.$$

   In particular, $\langle g^m \rangle = G$ iff gcd(m,n)=1,

3. if $|G| = n$ and $k \leq n$, then G has a subgroup of order k iff $k|n$, this subgroup is $\langle g^{n/k} \rangle$.

Definition 15 (Euler totient)**.** The **Euler totient** function ϕ is defined as $\phi(n) := |\{k \in \mathbb{N} : k \leq n \text{ and } \gcd(k, n) = 1\}|$.

Corollary 16. For $n \in \mathbb{N}$:

$$\sum_{d|n} \phi(d) = n.$$

2.3 Cosets

Definition 17 (Coset)**.** Given a group G with $H \leq G$ and $g \in G$ then

$$gH := \{gh : h \in H\},$$

is a **left coset** of H in G (the definition of a **right coset** follows clearly).

Note 18. For the rest of this section, unless specified otherwise, a coset is assumed to be a left-coset.

Theorem 19. Given a group G with $H \leq G$, all cosets of H in G have the same size.

Theorem 20. If G is a finite group with $H \leq G$, the left cosets of H for a partition of G.

2.4 Lagrange's theorem

Theorem 21 (Lagrange's theorem)**.** If G is a finite group and $H \leq G$, $|H|$ divides $|G|$.

Corollary 22. Given a group G with $H \leq G$, the relation $\sim$ on G given by: $g \sim k$ iff $g^{-1}k \in H$, is an equivalence relation with equivalence classes given by cosets of H.

Corollary 23. Given a group G of order n, for all $g \in G$, $\text{ord } g|n$ and $g^n = e$.

Corollary 24 (Fermat's little theorem)**.** Let p be prime. If $x \in \mathbb{Z}$ and $p \nmid x$, then $x^{p-1} \equiv 1 (\text{mod } p)$.

2.5 Generating groups

Definition 25. Given a group G with $S \subseteq G$, $S^{-1} := \{g^{-1} \in G : g \in S\}$.

Definition 26 (Subgroup generated by a set)**.** Let G be a group with non-empty $S \subseteq G$. The **subgroup generated by** S is defined as

$$\langle S \rangle := \{g_1 g_2 \dots g_k \in G : k \in \mathbb{N} \text{ and } g_i \in S \cup S^{-1} \text{ for all } i \in [1, k]\}.$$

Lemma 27. Given a group G with non-empty $S \subseteq G$, $\langle S \rangle \leq G$ and, $H \leq G,\ S \subseteq H \implies \langle S \rangle \leq H$. This is equivalent to saying "$\langle S \rangle$ is the smallest subgroup of G containing S".

3 Group homomorphisms

Definition 28 (Group homomorphism)**.** If $(G, \cdot)$ and $(H, *)$ are goups, $\phi : G \to H$ is a **group homomorphism** iff $\phi(g_1) * \phi(g_2) = \phi(g_1 \cdot g_2)$ for all $g_1, g_2 \in G$. If ϕ is bijective then it is called a **group isomorphism** with G and H being **isomorphic**, written $G \cong H$.

Example 29. The **determinant** is a group homomorphism, suppose $\mathbb{F}$ is a field:

$$\det : \mathrm{GL}(n, \mathbb{F}) \to (\mathbb{F}^*, \times).$$

Lemma 30. If G,H are groups with $\phi : G \to H$,

1. $\phi(e_G) = e_H$,
2. $\phi(g^{-1})(\phi(g))^{-1}$ for all $g \in G$.

Definition 31 (Image and kernel of group homomorphism)**.** If G,H are groups with $\phi : G \to H$, the **image** of ϕ is:

$$\operatorname{im} \phi := \{h \in H : \exists g \in G, h = \phi(g)\}.$$

and the **kernel** of ϕ is

$$\ker \phi := \{g \in G : \phi(g) = e_H\}.$$

These are each subgroups of H and G respectively.

Lemma 32. A group homomorphism, $\phi : G \to H$, is injective iff $\ker \phi = \{e_H\}$.

Theorem 33. The composition of two compatible group homomorphisms is also a group homomorphism.

Theorem 34. All cyclic groups of the same order are isomorphic.

4 Symmetric groups

4.1 Disjoint cycle decomposition

Definition 35. If $f, g \in S_n$ and $x \in [1, n]$ then f **fixes** x if $f(x) = x$ and f **moves** x otherwise.

Definition 36. The **support** of $f \in S_n$ is the set of points f moves, $\operatorname{supp}(f) := \{x \in [1, n] : f(x) \neq x\}$.

Definition 37. If $f, g \in S_n$ satisfy $\operatorname{supp}(f) \cap \operatorname{supp}(g) = \emptyset$, f and g are **disjoint**.

Lemma 38. If $f, g \in S_n$ are disjoint, $fg = gf$.

Definition 39 (Cycles)**.** If $f \in S_n$ with $i_1, i_2, \ldots, i_r \in [1, n]$ for some $r \leq n$ such that,

$$f(i_s) = i_{s+1 \mod (r)} \text{ for all } s \in [1, r],$$

with f fixing all other elements of $[1, n]$, then f is a **cycle of length** r or an r**-cycle** and we write $f = (i_1 i_1 \ldots i_r)$.

Theorem 40 (Disjoint cycle form)**.** if $f \in S_n$ then there exists $f_1, f_2, \ldots, f_k \in S_n$ all with disjoint supports such that $f = f_1 f_2 \ldots f_n$. If we further have, for all $i \in [1, k]$, both f_i is not a 1-cycle when $f \neq \mathrm{id}$ and $\operatorname{supp}(f_i) \subseteq \operatorname{supp}(f)$. We say f is in **disjoint cycle form** or **d.c.f**.

Theorem 41 (Uniqueness of disjoint cycles)**.** The disjoint cycle form of some $f \in S_n$ is unique up to rearrangement.

Theorem 42. If $f \in S_n$ is written in d.c.f as $f = f_1 f_2 \ldots f_k$ where f_i is an r_i-cycle for $i \in [1, k]$ then,

1. $f^m = \mathrm{id}$ iff $f_i^m = \mathrm{id}$ for all $i \in [1, k]$,
2. $\operatorname{ord}(f) = \operatorname{lcm}(r_1, r_2, \ldots r_k)$.

4.2 Alternating groups

Theorem 43. Every permutation in S_n can be written as the product of 2-cycles.

Definition 44 (Sign of a permutation)**.** We define the **sign** of a permutation with the group homomorphism, $\text{sgn} : S_n \to \{-1, 1\}$ with $\text{sgn}(i\ j) := -1$ for all $i, j \in [1, n]$ with $i \neq j$. This is defined over all permutations by the decomposition into 2-cycles, the sign of a permutation is unique. We say $f \in S_n$ is **even** if $f \in \ker(\text{sgn})$ and **odd** otherwise.

Definition 45 (Alternating group)**.** The **alternating group** of size n is $A_n := \ker(\text{sgn})$ with $A_n \leq S_n$.

4.3 Dihedral groups

Definition 46 (Dihedral group)**.** The **dihedral group** of order $2n$, denoted D_{2n}, is the group of symmetries of a regular n-gon in $\mathbb{R}^3$ centered at the origin, it is often written at

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

where r is a rotation by $\frac{2\pi}{n}$ and s is the reflection along the centre of the polygon and the first vertex.

Theorem 47. The elements of D_{2n} can be written as elements of S_n giving $D_{2n} \leq S_n$. Specifically, $r = (1\ 2\ \dots\ n)$ and $s = (1)(2\ n)(3\ n-1)\dots$ or $(1\ n)(2\ n-1)\dots$ if n is odd or even respectively.