

Last lecture

- Congruences, left and right invariant equivalence relations:

Proposition 2.4

Suppose \sim is an equivalence relation and set $H = \{x \in G : x \sim 1\}$.

- 1 \sim is left invariant $\iff H$ is a subgroup of G and $\bar{x} = xH, \forall x \in G$.
- 2 \sim is right invariant $\iff H$ is a subgroup of G and $\bar{x} = Hx, \forall x \in G$.
- 3 \sim is a congruence $\iff H$ is a normal subgroup of G .

- Quotients of an equivalence relation $G/\sim = \{\bar{x} : x \in G\}$

Proposition 2.5

Suppose that \approx is a congruence on G and let $Q = G/\approx$.

Then Q is a group with multiplication $\alpha\beta = \overline{xy}$, if $\alpha = \bar{x}$ and $\beta = \bar{y}$.

- Normal subgroups and quotient groups $G/N = N/\sim$.

Soluble groups

Definition 3.1

A group G is **soluble** if it has a chain of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{1_G\}$$

such that G_i is a normal subgroup of G_{i-1}

and G_i/G_{i-1} is abelian, for $1 \leq i \leq k$

Galois theory attaches a group G to a polynomial $p(x)$ and one of its' main results says that G is **soluble by radicals** if and only if G is a soluble group.

Convention on permutations

A **permutation** of $n = \{1, 2, \dots, n\}$ is a bijective function $\sigma : n \rightarrow n$.

The set \mathfrak{S}_n of all permutations of n forms a group under composition of functions: if $\sigma, \tau \in \mathfrak{S}_n$ then $(\sigma\tau)(i) = \sigma(\tau(i))$, for $i \in n$.

Notation for permutations

If σ is a permutation write $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix}$, where $\sigma(i) = \sigma_i$ for $i \in n$.

We also write σ as a product of **cycles** (i_1, i_2, \dots, i_a)

if $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{a-1}) = i_a$ and $\sigma(i_a) = i_1$.

Every permutation can be written as a product of (commuting) disjoint cycles, which is unique up to the ordering of the cycles.

Example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1, 3, 5)(2, 4) \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = (1, 2, 5, 4)$$

$$\text{Then } \sigma\tau = (1, 3, 5)(2, 4) \cdot (1, 4, 3, 5, 2) = (1, 2, 3)(4, 5).$$

Note that when multiplying cycles we work from **right to left**.

The definition of a ring

Definition 3.2

A **ring** is a set R equipped with two operations, **addition** $+$ and **multiplication** \cdot , such that for $a, b, c \in R$

- 1 $(R, +)$ is an **additive** (abelian) group:
 $a + (b + c) = (a + b) + c$, $a + 0 = a = 0 + a$,
 $a + (-a) = 0 = (-a) + a$, $a + b = b + a$
- 2 Multiplication is **associative**: $a(bc) = (ab)c$
- 3 The two **distributive** laws hold:
 $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Examples Any **field** $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$ is a ring, but the ring axioms are much weaker than the field axioms \implies rings are more exciting!

Importantly, rings do not necessarily have a multiplicative identity and the elements of a ring need not have multiplicative inverses.

Examples of rings

- \mathbb{Z} , the ring of integers
- \mathbb{Z}^n , the ring of n -tuples of integers
- $\mathbb{Z}[i]$, the ring of Gaussian integers
- $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$, the ring of even integers
- $3\mathbb{Z} = \{3z : z \in \mathbb{Z}\}$, the ring of three divisible integers
- $\text{Mat}_n(\mathbb{R})$, the ring of all $n \times n$ matrices over \mathbb{R}
- $\text{Mat}_n(\mathbb{C})$, the ring of all $n \times n$ matrices over \mathbb{C}
- $\text{Mat}_n(\mathbb{Z})$, the ring of all $n \times n$ matrices over \mathbb{Z}
- $\text{Mat}_n(R)$, the ring of all $n \times n$ matrices over a ring R
- $\mathbb{Z}[x]$, the ring of polynomials in x with coefficients in \mathbb{Z}
- $R[x]$, the ring of polynomials in x with coefficients in the ring R
- $\mathcal{C}_0(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} : f \text{ continuous}\}$
- $\mathcal{C}_1(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} : f \text{ differentiable}\}$

Basic properties of rings

Suppose that R is a ring.

The **zero** additive identity $0 = 0_R$ of R .

If $a \in R$ then the **negative** of a is the additive inverse $-a$.

The ring R is **commutative** if $ab = ba$, for all $a, b \in R$.

An **identity element** in R is any element $1_R \in R$ such that

$$a \cdot 1_R = a = 1_R \cdot a, \quad \text{for all } a \in R.$$

Lemma 3.3

The identity element of a ring is unique if it exists.

Proof See Tutorials.

Suppose that R is a **ring with one**; ie. R has an identity element.

A **left inverse** of $a \in R$ is an element $a_l \in R$ such that $a_l a = 1_R$.

A **right inverse** of $a \in R$ is an element $a_r \in R$ such that $aa_r = 1_R$.

An **inverse** if $a \in R$ is an element a^{-1} such that $aa^{-1} = 1_R = a^{-1}a$.

Left inverses, right inverses and fields

Lemma 3.4

*Suppose that $a \in R$ has both a left and a right inverse.
Then a has an inverse and $a^{-1} = a_l = a_r$*

Proof We have, $a_l = a_l \cdot 1_R = a_l(aa_r) = (a_l a)a_r = 1_R \cdot a_r = a_r$. \square

Definition 3.5

A **field** is a commutative ring with $1_R \neq 0_R$ such that all non-zero elements of R have (multiplicative) inverses.

Examples

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields
- $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime (**Check!**)
- $\text{Mat}_n(\mathbb{R})$ is a field if and only if $n = 1$ (**Check!**)

The zero element of a ring

Lemma 3.6

Suppose that R is a ring. Then $a \cdot 0_R = 0_R = 0_R \cdot a$, for all $a \in R$.

Proof Now, $a \cdot 0_R = a(0_R + 0_R) = a \cdot 0_R + a \cdot 0_R$.

Subtracting $a \cdot 0_R$ from both sides shows that $0_R = a \cdot 0_R$.

Similarly, $0_R = 0_R \cdot a$. \square

Warning!!!!

It is **not** always true that $ab = 0 \implies a = 0$ or $b = 0$!!!

Example $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.