

UiO : Department of Mathematics
University of Oslo

MAT2200 Spring 2026

Revision

May 22, 2026

Binary algebraic structures

A **binary operation** on a set S is a map

$$* \colon S \times S \to S$$

$$\text{Notation : } *(a, b) = a * b.$$

A pair $(S, *)$ of a set S and a binary operation $*$ is a **binary algebraic structure**.

Further concepts

- $*$ is **associative** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.
- $*$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.
- $e \in S$ is an **identity element** if $e * a = a * e = a$ for all $a \in S$.
- $a \in S$ is **inverse** to $b \in S$ if $a * b = b * a = e$.

Isomorphisms

A map $\varphi\colon (S,*) \to (S',*')$ is an **isomorphism** if φ is a bijection and

$$\varphi(a*b) = \varphi(a) *' \varphi(b) \qquad \forall a,b \in S$$

Write $(S,*) \simeq (S',*')$, say that these are **isomorphic**.

All "structural" properties are preserved under isomorphism. So if $(S,*) \simeq (S',*')$ and $(S,*)$ has property P, then $(S',*')$ has property P.

Examples of structural properties: "S has identity element", "$*$ is associative", "$*$ is commutative", S is finite, $(S,*)$ is a group, $(S,*)$ is a cyclic group, "In $(S,*)$, every element satisfies $x*x=e$".

Groups

A binary algebraic structure $(G, *)$ is a **group** if

1. $*$ is associative.
2. G has an identity element e.
3. For every $a \in G$, there is an element $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

The identity element and the inverses are *unique*: There is exactly one identity element $e \in G$ and for each a, exactly one inverse a^{-1}.

Two words

- A group is **abelian** if $*$ is commutative.
- The **order** of a group is the number of elements.

Examples of groups

- With the operation of addition, the following are groups:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}^n$$

- With the operation of multiplication, the following are groups:

$$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, GL(n, \mathbb{R}) = \{(n \times n) \text{ invertible real matrices}\}$$

- $\mathbb{Z}_n = \{0, \ldots, n-1\}$ with operation

$$a +_n b = \text{ remainder of } a + b \text{ divided by } n$$

this is the group of integers modulo n.

Group notation

Multiplicative

In group $(G, *)$, write ab instead of $a * b$. For n a positive integer, write

$$a^n = \overbrace{a \cdots a}^{n}, \quad a^{-n} = \overbrace{a^{-1} \cdots a^{-1}}^{n}, \quad a^0 = e$$

Then for all $m, n \in \mathbb{Z}$, $a^m a^n = a^{m+n}$.

Additive

If $(G, *)$ is abelian, we may write $a + b$ instead of ab. Then write $-a$ for the inverse of a, 0 for the identity element, and for n a positive integer

$$na = \overbrace{a + \cdots + a}^{n}, \quad (-n)a = \overbrace{(-a) + \cdots + (-a)}^{n}, \quad 0a = 0$$

Good properties of groups

Cancellation laws and linear equations

If $a, b, c \in G$ are such that

$$ab = ac \quad \text{or} \quad ba = ca$$

then $b = c$.

For $a, b \in G$, the equations

$$ax = b, \qquad ya = b \qquad x, y \in G$$

have unique solutions $x = a^{-1}b$, $y = ba^{-1}$.

Subgroups

If G is a group, $H \subseteq G$, then H is a **subgroup**, denoted $H \leq G$, if

1. H is closed under multiplication, that is

$$a, b \in H \Rightarrow ab \in H, \text{ and}$$

2. H is a group with the induced binary operation.

Proving H is a subgroup

Verifying $H \subseteq G$ is a subgroup can be done by checking

1. H closed under multiplication
2. $e \in H$
3. For every $a \in H$, also $a^{-1} \in H$.

Equivalently (by a trick), check that for all $a, b \in H$, $ab^{-1} \in H$.

Cyclic (sub)-groups

Let G be a group and $a \in G$. The **cyclic subgroup generated by** a is

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq G.$$

The **order** of a is the order of $\langle a \rangle$.

Theorem

Let G be a group and $a \in G$. Then either

- There is no $n > 0$ such that $a^n = e$, and $\mathbb{Z} \simeq \langle a \rangle$ via the isomorphism $k \mapsto a^k$, or
- There is a smallest positive n such that $a^n = e$, and we have

$$\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\},$$

and $\mathbb{Z}_n \simeq \langle a \rangle$ via the isomorphism $k \mapsto a^k$.

Subgroups of cyclic groups

A group G is **cyclic** if there is an $a \in G$ such that $G = \langle a \rangle$.

Theorem

If G is a cyclic group and $H \leq G$, then H is cyclic.

- Any subgroup of $\mathbb{Z}$ is generated by some $k \in \mathbb{Z}$ and is

$$\langle k \rangle = k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$$

- Any subgroup of $\mathbb{Z}_n$ is generated by some $k \in \mathbb{Z}_n$. With $d = \gcd(k, n)$, we have

$$\langle k \rangle = \langle d \rangle = \{0, d, 2d, \ldots, n - d\}$$

and $|\langle k \rangle| = \frac{n}{d}$.

Direct products

Given groups $G_1, \ldots, G_n$, the **direct product group** is

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

with multiplication given by

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

Theorem

Let $n_1, \ldots, n_k \geq 1$. The group

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

is cyclic if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$. If G is cyclic, then $G \simeq \mathbb{Z}_{n_1 \cdots n_k}$.

Generators for a group

Let G be a group, $g_1, \ldots, g_n \in G$. Say the elements $g_1, \ldots, g_n$ **generate** G if every element g can be written in the form

$$g = g_{i_1}^{e_1} g_{i_2}^{e_2} \cdots g_{i_m}^{e_m}$$

with the $i_j \in \{1, \ldots, n\}$, $e_j \in \mathbb{Z}$. A group G is **finitely generated** if there exists a finite set of elements $g_1, \ldots, g_n$ such that the g_i generate G.

Examples

Every finite group is finitely generated, $\mathbb{Z}$ is finitely generated, $\mathbb{Q}$ is not finitely generated.

Finitely generated abelian groups

Structure theorem for finitely generated abelian groups

Let G be an abelian group. If G is finitely generated, we have an isomorphism

$$G \simeq \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{b} \times \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}},$$

where the p_i are primes, the e_i are positive integers.
If G is finite and abelian,

$$G \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}},$$

where the p_i are primes, the e_i are positive integers.
Up to reordering factors, the product groups above are unique.

Permutation groups

Given a set A, a bijection $\sigma\colon A \to A$ is called a **permutation** of A. These form a group

$$S_A = \{\sigma \mid \sigma \text{ is a permutation of } A\}$$

with the binary operation of composition:

$$\sigma_1\sigma_2 = \sigma_1 \circ \sigma_2.$$

For the set $A = \{1, \ldots, n\}$, write $S_n = S_A$.

Cayley's theorem

Every group G is isomorphic to a subgroup of S_G.

More on symmetric groups

In S_n, write

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

A **cycle** in S_A is an element of the form

$$\sigma = (a_1 \ a_2 \ \cdots \ a_l),$$

meaning

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leq i \leq l-1$$
$$\sigma(a_l) = a_1$$
$$\sigma(b) = b \text{ if } b \notin \{a_1, \ldots, a_l\}$$

Even more on symmetric groups

Two cycles

$$(a_1 \cdots a_l) \text{ and } (b_1 \cdots b_m)$$

are **disjoint** if $a_i \neq b_j$ for all i, j. In S_n, every element σ can be written as

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$$

where the σ_i are pairwise disjoint cycles.

Example

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4).$$

Transpositions and the alternating groups

A cycle of length two, $\tau = (a_1\ a_2)$ is called a **transposition**.

Theorem

Every $\sigma \in S_n$ can be written as a product of transpositions, and if

$$\sigma = \tau_1\tau_2\cdots\tau_k = \tau_1'\ldots\tau_l'$$

with all τ_i and τ_i' transpositions, then k and l have the same parity.

If σ is a product of an even (resp. odd) number of transpositions, we say that σ is even (resp. odd). Define the **alternating group** on n letters

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\} \leq S_n$$

Subgroups and cosets

Let G be a group, $H \leq G$. The **left coset of** H containing a is

$$aH = \{ah \mid h \in H\} \subseteq G,$$

the **right coset of** H containing a is

$$Ha = \{ha \mid h \in H\} \subseteq G.$$

Every element of G lies in a unique left[1] coset of H. We have

$$aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH.$$

Write

$$G/H = \{\text{left cosets of } H\}.$$

The **index** of H in G is

$$(G : H) = |G/H|.$$

[1] All statements about left cosets have equivalent versions for right cosets – we omit those here.

Size of cosets

Let $H \leq G$, and $a \in G$. Then

$$|aH| = |H|$$

If G is finite, we have

$$|G| = |H|(G : H),$$

which gives

Lagrange's theorem

If $H \leq G$ and G is finite, then $|H|$ divides $|G|$.

Images and inverse images

Let $\varphi\colon A \to A'$ be a map of sets, let $S \subset A$ and $S' \subset A'$. Then the **image of S under φ** is

$$\varphi[S] = \{\varphi(s) \mid s \in S\}.$$

The **inverse image of S' under φ** is

$$\varphi^{-1}[S'] = \{a \in A \mid \varphi(a) \in S'\}$$

Homomorphisms

Let G, G' be groups. A map $\varphi\colon G \to G'$ is a **homomorphism** if

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in G.$$

Theorem

Let $\varphi\colon G \to G'$ be a homomorphism, let $a \in G$, let $H \leq G$, $K' \leq G'$. Then

1. $\varphi(e) = e'$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$
3. $\varphi[H]$ is a subgroup of G'
4. $\varphi^{-1}[K']$ is a subgroup of G

Kernels

Let $\varphi\colon G \to G'$ be a homomorphism of groups. The **kernel** of φ is

$$\operatorname{Ker}\varphi = \varphi^{-1}[\{e'\}] = \{g \in G \mid \varphi(g) = e'\}.$$

Cosets of $\operatorname{Ker}\varphi$

Write $H = \operatorname{Ker}\varphi$. For each $a \in G$, we have

$$\varphi^{-1}[\{\varphi(a)\}] = \{g \in G \mid \varphi(g) = \varphi(a)\} = aH = Ha$$

Corollary: A homomorphism of groups $\varphi\colon G \to G'$ is injective if and only if $\operatorname{Ker}\varphi = \{e\}$.

Normal subgroups

Let G be a group, $H \leq G$. Then H is **normal** if for every $a \in G$, we have

$$aH = Ha.$$

Equivalent characterisations

Let H be a subgroup of G. The following are equivalent

1. H is normal.
2. For each $g \in G$, $gHg^{-1} = H$.
3. For each $g \in G$, $h \in H$, we have $ghg^{-1} \in H$
4. There exists a group G' and a homomorphism $\varphi\colon G \to G'$ such that $H = \operatorname{Ker}\varphi$.

Factor groups

Let G be a group, $H \leq G$. Write

$$G/H = \{\text{left cosets of } H\}.$$

If (and only if) H is normal, we can define a binary operation on G/H by

$$(aH)(bH) = abH, \qquad a, b \in G.$$

This makes G/H a group, the **factor group**/**quotient group** of G by H.

Example

Let $n \in \mathbb{Z}^+$. Then

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\},$$

and $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

Homomorphisms and factor groups

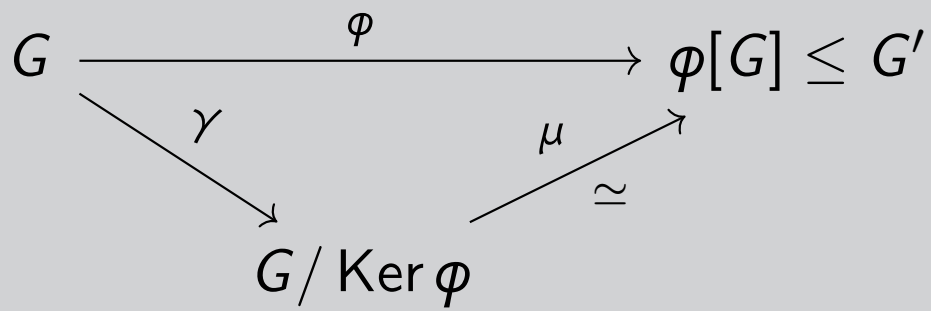
Let G be a group, $H \leq G$ a normal subgroup. There is a surjective homomorphism $\gamma\colon G \to G/H$ given by

$$\gamma(a) = aH,$$

with $\operatorname{Ker}\gamma = H$.

The fundamental theorem of homomorphisms

Let $\varphi\colon G \to G'$ be a group homomorphism. Then we can write $\varphi = \mu \circ \gamma$, with $\mu\colon G/\operatorname{Ker}\varphi \to \varphi[G]$ an isomorphism of groups.



Simple groups

A group G is **simple** if $G \neq \{e\}$ and its only normal subgroups are $\{e\}$ and G.

- An abelian group G is simple if and only if $G \simeq \mathbb{Z}_p$ with p a prime.
- If $n \geq 5$, then A_n is simple.

Group actions

Let G be a group and X a set. An **action** of G on X is a map $*\colon G \times X \to X$, written $*(g, x) = gx$, satisfying

1. $ex = x \qquad \forall x \in X$
2. $g_1(g_2x) = (g_1g_2)x \qquad \forall g_1, g_2 \in G, x \in X$

A set X with an action of G is called a G-**set**.

Actions as homomorphisms to S_X

Every action of G on X corresponds uniquely to a homomorphism $\varphi\colon G \to S_X$, such that

$$\varphi(g)(x) = gx.$$

Thus G-action can equivalently be defined by a homomorphism $G \to S_X$.

Fix point sets and isotropy groups

Let X be a G-set.

- For $g \in G$, define

$$X_g = \{x \in X \mid gx = x\},$$

  the **fix point set** of g.

- For $x \in X$, define

$$G_x = \{g \in G \mid gx = x\},$$

  the **isotropy group** of x, a subgroup of G.

Orbits of a G-action

Let X be a G-set, $x \in X$. The **orbit** of x is

$$Gx = \{gx \mid g \in G\}.$$

Every element of X lies in one orbit, so X is partitioned into its orbits.

Orbits versus isotropy groups

We have a bijection

$$Gx \leftrightarrow G/G_x.$$

If G and X are finite, then

$$|G| = |Gx||G_x|.$$

Counting orbits

Let G be a finite group and X a finite G-set.

Burnside's formula

Let r be the number of G-orbits in X. Then

$$r = \frac{\sum_{g \in G} |X_g|}{|G|}.$$

The right hand side is the average number of fixed points for an element $g \in G$.

Rings

A **ring** is a set R equipped with two binary operations, addition denoted by $a + b$ and multiplication denoted by ab, which satisfy

1. $(R, +)$ is an abelian group
2. multiplication is associative: For $a, b, c \in R$

$$a(bc) = (ab)c.$$

3. The left and right distributive laws hold: For $a, b, c \in R$

$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$

Basic properties/notation of rings

Notation in a ring R

- Write $0 \in R$ for additive identity.
- Given $a \in R$, write $-a$ for additive inverse
- Given integer $n > 0$ and $a \in R$, let

$$n \cdot a = \overbrace{a + \cdots + a}^{n}, \quad (-n) \cdot a = \overbrace{(-a) + \cdots + (-a)}^{n}, \quad 0 \cdot a = 0$$

Basic properties

If $a, b \in R$, we have

$$0a = a0 = 0, \qquad (-a)b = a(-b) = -(ab), \qquad (-a)(-b) = ab$$

Examples

- With the usual operations of addition and multiplication, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are rings.
- With the usual operation of matrix addition and multiplication

$$M_n(\mathbb{R}) = \{(n \times n)\text{-matrices}\}$$

  forms a ring.
- With the usual operation of addition and multiplication of functions,

$$C(\mathbb{R}) = \{\text{functions } f : \mathbb{R} \to \mathbb{R}\}$$

  forms a ring.
- There is a unique ring with one element, $\mathbf{0} = \{0\}$, called the **zero ring**.

Example: Integers modulo n

Let $n > 0$ be an integer. Given integers i, j, we say i and j are **congruent modulo** n and write

$$i \equiv j \pmod{n}$$

if i and j have the same remainder upon division by n.
The set of **integers modulo** n,

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

forms a ring, with addition $+_n$ and multiplication defined by

$$a +_n b = c \text{ if } a + b \equiv c \pmod{n}$$

and

$$ab = c \text{ if } ab \equiv c \pmod{n}$$

Special properties of rings, I: Unity

Let R be a ring.

- A multiplicative identity, that is an element $a \in R$ such that

$$ab = ba = b \qquad \forall b \in R$$

  is called **unity**.
- A unity of a ring is unique if it exists, and denoted $1 \in R$.
- If such an element exists, we say that R is a **ring with unity**.[2]

Examples

The ring $\mathbb{Z}$ has unity $1 \in \mathbb{Z}$, the ring

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$$

does not have a unity element.

[2] Many sources use the word ring exclusively for rings with unity.

Special properties of rings II: Commutativity

We say a ring R is **commutative** if for all $a, b \in R$, we have

$$ab = ba.$$

Examples

- The rings $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative
- If $n \geq 2$, the ring $M_n(\mathbb{R})$ of $(n \times n)$ real matrices is not commutative, e.g.

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

Zero-divisors and units

Let R be a ring.

- If $0 \neq a \in R$ is such that there exists a $b \in R, b \neq 0$, with either $ab = 0$ or $ba = 0$, we say that a is a **0-divisor**.
- If R has unity, we say that $a \in R$ is a **unit** if there exists a $b \in R$ such that
$$ba = ab = 1.$$
- If a is a unit, then a is not a 0-divisor.

Integral domains and fields

- If $R \neq \mathbf{0}$ is commutative, has unity, and has no 0-divisors, we say that R is an **integral domain**.
- If $R \neq \mathbf{0}$ is commutative, has unity, and every non-zero element is a unit, we say that R is a **field**.
- If R is a field, then R is an integral domain.

Examples

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields (and so also integral domains).
- $\mathbb{Z}$ is an integral domain, but not a field.

Notation

If F is a field and $a, b \in F$, with $b \neq 0$, we write $1/b$ or $\frac{1}{b}$ for the multiplicative inverse of b, and $\frac{1}{b}a = \frac{a}{b} = a\frac{1}{b}$.

Properties of $\mathbb{Z}_n$

Let $n > 0$ be an integer.

0-divisors in $\mathbb{Z}_n$

The 0-divisors in $\mathbb{Z}_n$ are the d with $1 \leq d \leq n-1$ such that

$$\gcd(d, n) \neq 1.$$

Units in $\mathbb{Z}_n$

The units of $\mathbb{Z}_n$ are the d with $1 \leq d \leq n-1$ such that

$$\gcd(d, n) = 1$$

If n is prime, then $\mathbb{Z}_n$ is a field. If n is not prime, then $\mathbb{Z}_n$ is not (even) an integral domain.

Fermat's and Euler's theorems

Let p be a prime.

Fermat's theorem

Three versions:

1. If $0 \neq a \in \mathbb{Z}_p$, then $a^{p-1} = 1$ in $\mathbb{Z}_p$.
2. If $a \in \mathbb{Z}_p$, then $a^p = a$ in $\mathbb{Z}_p$.
3. If $k \in \mathbb{Z}$, then $k^p \equiv k \pmod{p}$.

Euler's theorem (recovering Fermat's if n is prime)

Let $n > 0$ be an integer. If $k \in \mathbb{Z}$ is such that $\gcd(k, n) = 1$, then $k^{\varphi(n)} \equiv 1 \pmod{n}$, where

$$\varphi(n) = |\{d \in \{1, \ldots, n\} \mid \gcd(d, n) = 1\}| = \text{ no. of units in } \mathbb{Z}_n.$$

The field of fractions

Let D be an integral domain.

- There exists a "smallest" field F containing a subring isomorphic to D. The field F is called the **field of fractions** of D.
- Objects of F are formal fractions a/b, $a, b \in D$, $b \neq 0$, where

$$\frac{a}{b} = \frac{c}{d} \text{ in } F \Leftrightarrow ad = bc \text{ in } D$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

- The subring

$$\{a/1 \mid a \in D\} \subset F$$

  is isomorphic to D.
- Motivating example: $D = \mathbb{Z}$, $F = \mathbb{Q}$

Rings of polynomials

Let R be a ring. The **ring of polynomials with coefficients** in R is denoted $R[x]$. Its elements are formal expressions

$$\sum_{i=0}^{\infty} r_i x^i \qquad r_i \in R.$$

where there are only finitely many i such that $r_i \neq 0$. Addition is given by

$$\sum_{i=0}^{\infty} r_i x^i + \sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{\infty} (r_i + s_i) x^i,$$

and multiplication by

$$\left(\sum_{i=0}^{\infty} r_i x^i\right)\left(\sum_{i=0}^{\infty} s_i x^i\right) = \sum_{i=0}^{\infty} t_i x^i, \text{ with } t_i = \sum_{j=0}^{i} r_j s_{i-j}.$$

Rings of polynomials II

If $\sum_{i=0}^{\infty} r_i x^i \in R[x]$, we omit terms $0x^i$ and write e.g.

$$1 + 2x + 14x^2 + 0x^3 + 0x^4 + \cdots = 1 + 2x + 14x^2.$$

The **degree** of a polynomial $f(x) = \sum_{i=0}^{\infty} r_i x^i$ is the maximal i such that $r_i \neq 0$ (and is undefined if $f(x) = 0$).

Properties of $R[x]$

- If R has unity, then $R[x]$ has unity.
- If R is commutative, then $R[x]$ is commutative.
- If R is an integral domain, then $R[x]$ is an integral domain.

Polynomial division

Let F be a field, and let $f(x), g(x) \in F[x], g(x) \neq 0$.

Polynomial division of $f(x)$ by $g(x)$

There exist unique polynomials $q(x)$ ("the quotient") and $r(x)$ ("the remainder") in $F[x]$ satisfying

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

If $r(x) = 0$, so that $f(x) = g(x)q(x)$, we say that $g(x)$ **divides** $f(x)$.

Zeros of polynomials

Let F be a subfield of a field E and let $\alpha \in E$. The **evaluation homomorphism** $\varphi_\alpha \colon F[x] \to E$ is given by, for any

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in F[x],$$

$$\varphi_\alpha(f(x)) = f(\alpha) = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_0 \in E$$

If $f(\alpha) = 0$, then we say that α is a **zero** of $f(x)$.

Theorem

The element $\alpha \in F$ is a zero of $f(x)$ if and only if $(x - \alpha)$ divides $f(x)$.

Theorem

A polynomial $f(x) \in F[x]$ of degree n has at most n zeros in F.

Irreducible polynomials

Let F be a field, and let $f(x) \in F[x]$ be a nonconstant polynomial. We say that $f(x)$ is **irreducible** (over F) if there is no way to write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ of lower degree than $f(x)$.

Criteria for irreducibility

- If $f(x)$ has a zero in F and deg $f(x) > 1$, then $f(x)$ is reducible.
- If $f(x)$ has degree 2 or 3 and no zeros in F, then $f(x)$ is irreducible.

The Eisenstein criterion

Let p be a prime and $f(x) = c_n x^n + \cdots + c_0 \in \mathbb{Q}[x]$ with all c_i integers. If p divides c_i for $i < n$, p does not divide c_n, and p^2 does not divide c_0, then $f(x)$ is irreducible over $\mathbb{Q}$.

Factorisation of polynomials

Theorem (Unique factorisation into irreducible polynomials)

For any nonconstant $f(x) \in F[x]$, we can write

$$f(x) = p_1(x)p_2(x)\cdots p_n(x)$$

with the $p_i(x) \in F[x]$ irreducible. The $p_i(x)$ are unique up to reordering and multiplying by constants, e.g.

$$x^2 + 3x + 2 = (x+1)(x+2) = (x+2)(x+1) = (2x+4)(\frac{x}{2} + \frac{1}{2}).$$

Ring homomorphisms

Let R and S be rings. A map $\varphi\colon R \to S$ is a **ring homomorphism** if for any $a, b \in R$, we have

$$\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$$

and

$$\varphi(ab) = \varphi(a)\varphi(b).$$

If φ is moreover a bijection, we call φ an isomorphism and write $R \simeq S$. The **kernel** of φ is

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}.$$

A homomorphism φ is injective if and only if $\ker \varphi = \{0\}$.

Ideals

Let R be a ring and $I \subseteq R$. The set I is an **ideal** of R if

1. I is a subgroup of $(R, +)$, and
2. for every $a \in R$ and $b \in I$ we have

$$ab \in I \text{ and } ba \in I.$$

Examples

- For any ring R, the sets $\{0\}, R \subset R$ are ideals.
- For any homomorphism $\varphi\colon R \to S$, $\ker\varphi \subset R$ is an ideal.
- The ideals of $\mathbb{Z}$ are all of the form

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$$

for some $n \geq 0$.

Quotient rings

Let R be a ring and let I be an ideal. Thinking of I as a subgroup of the abelian group $(R, +)$, for each $a \in R$ we have the left (=right) coset

$$a + I = \{a + r \mid r \in I\}.$$

The set

$$R/I = \{\text{cosets of } I\} = \{a + I \mid a \in R\},$$

has structure of a ring by setting for $a, b \in R$

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I)(b + I) = ab + I.$$

We call R/I the **quotient ring** of R by I.

Examples of quotient rings

- Take $I = R$. Then

$$R/R = \{a + R \mid a \in R\} = \{R\}$$

  has one element, so $R/R \simeq \{0\}$.

- Take $I = \{0\}$. Then

$$R/\{0\} = \{a + \{0\} \mid a \in R\} = \{\{a\} \mid a \in R\} \simeq R.$$

- For $n > 0$, we have

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\} \simeq \mathbb{Z}_n.$$

The fundamental homomorphism theorem

Let $\varphi\colon R \to S$ be a homomorphism of rings. Then

- $\varphi[R]$ is a subring of S
- We have an isomorphism

$$\psi\colon R/\ker\varphi \to \varphi[R]$$

given by

$$\psi(a+\ker\varphi) = \varphi(a).$$

Example

- Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ be $\varphi(k) =$ the remainder of k divided by n. Then $\ker\varphi = n\mathbb{Z}$, and $\varphi[\mathbb{Z}] = \mathbb{Z}_n$, so we find

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker\varphi \simeq \varphi[\mathbb{Z}] = \mathbb{Z}_n.$$

- If $\ker\varphi = \{0\}$, then $R/\ker\varphi \simeq R$, so that $R \simeq \varphi[R] \leq S$.

Prime and maximal ideals

Let R be a commutative ring with unity, and let $I \subseteq R$ be an ideal. Then

- I is a **prime ideal** if for $a, b \in R$, $a \notin I$ and $b \notin I$ implies $ab \notin I$.
- I is a **maximal ideal** if there is no ideal J such that $I \subsetneq J \subsetneq R$.

Main theorem

Let R and I be as above.

- The ideal I is prime if and only if R/I is an integral domain.
- The ideal I is maximal if and only if R/I is a field.
- If I is maximal, then I is prime.

Example

If n is prime, then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ is a field, so $n\mathbb{Z} < \mathbb{Z}$ is a maximal ideal. If n is not prime, $\mathbb{Z}_n$ is not an integral domain, so $n\mathbb{Z}$ is not a prime ideal.

Principal ideals

If $a \in R$ and R is commutative, the **principal ideal** generated by a is

$$\langle a \rangle = \{ra \mid r \in R\} \subseteq R.$$

Examples

- For any ring R, $\langle 0 \rangle = \{0\}$.
- If R has unity and $a \in R$ is a unit, then $\langle a \rangle = \langle 1 \rangle = R$
- For $n \in \mathbb{Z}$, we have $\langle n \rangle = n\mathbb{Z}$.
- If F is a field and $0 \neq f(x) \in F[x]$, then

$$\langle f(x) \rangle = \{g(x) \in F[x] \mid f(x) \text{ divides } g(x)\}.$$

Theorem

Let F be a field. Then every ideal $I \subseteq F[x]$ is principal.
If $0 \neq f(x) \in F[x]$, the following are equivalent:

1. $f(x)$ is irreducible.
2. $\langle f(x) \rangle$ is a prime ideal.
3. $\langle f(x) \rangle$ is a maximal ideal.

Corollary

The ring $F[x]/\langle f(x) \rangle$ is a field if and only if $f(x)$ is irreducible.

Fields

Useful facts about fields

Let F be a field.

- The non-zero elements of F, denoted $F^\times$, form an abelian group under multiplication.
- If $I \leq F$ is an ideal, then $I = \{0\}$ or $I = F$.
- If $\varphi\colon F \to R$ is a homomorphism, then φ is either 0 or injective.

If F and E are fields so that F is a subfield of E, we call E an **extension field** of F. We write $F \leq E$ and call the pair of F and E a **field extension**.

Kronecker's theorem

Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial.

Theorem

There exists a field extension $F \leq E$ such that $f(x)$ has a zero in E.
If $f(x)$ is irreducible, we can take

$$E = F[x]/\langle f(x) \rangle,$$

and consider F as a subfield of E via

$$F \simeq \{a + \langle f(x) \rangle \mid a \in F\} \subseteq E.$$

Then $\alpha = x + \langle f(x) \rangle \in E$ is a zero of $f(x)$.

Algebraic and transcendental elements

Let $F \leq E$ be a field extension, and let $\alpha \in E$ We say α is

- **algebraic** over F if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.
- **transcendental** over F otherwise.

Complex numbers which are algebraic/transcendental over $\mathbb{Q}$ are called **algebraic/transcendental numbers**

The irreducible polynomial of an element

Let $F \leq E$ be a field extension, and let $\alpha \in E$ be algebraic over F.

Definition

The **irreducible polynomial** of α over F, denoted $\text{irr}(\alpha, F) \in F[x]$, is defined as either

- The unique monic,[a] irreducible polynomial with α as a 0, or
- The monic polynomial of minimal degree which has α as a 0.

[a] "Monic" means $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ with $c_n = 1$.

If $f(x) \in F[x]$ has α as a zero, then $\text{irr}(\alpha, F)$ divides $f(x)$.

Vector spaces

Let F be a field. A vector space over F is an abelian group V with a given operation of scalar multiplication:

$$F \times V \to V$$
$$(c, v) \mapsto cv$$

We require this operation to satisfy the following axioms, for given $c, d \in F$ and $v, w \in V$:

1. $1v = v$
2. $(c + d)v = cv + dv$
3. $c(v + w) = cv + cw$
4. $c(dv) = (cd)v$

Our main example: If $F \leq E$ is a field extension, then E is a vector space over F, with the scalar multiplication given by the product in E.

Basis of a vector space

Let V be a vector space over a field F.

- A sequence of vectors $v_1, \ldots, v_n \in V$ **spans** V if every $v \in V$ can be written as
$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$$
for some $c_i \in F$.
- A sequence $v_1, \ldots, v_n \in V$ is **linearly independent** if
$$c_1 v_1 + \cdots + c_n v_n = 0$$
with $c_i \in F$ implies that $c_i = 0$ for all i.
- A sequence $v_1, \ldots, v_n \in V$ is a **basis** for V if it spans V and is linearly independent. Equivalently: $v_1, \ldots, v_n$ is a basis if every $v \in V$ can be written *uniquely* as
$$v = c_1 v_1 + \cdots + c_n v_n, \quad c_i \in F$$

Dimension of a vector space

Let V be a vector space over a field F. If there exists a finite basis $v_1, \ldots, v_n$ of V, we say V is **finite-dimensional**.

Theorem (Invariance of basis size)

If $v_1, \ldots, v_n$ and $v_1', \ldots, v_m'$ are bases of V, then $n = m$.

Definition

If V has a basis $v_1, \ldots, v_n$, then we say V has **dimension** n.

Theorem

Suppose V has dimension n. Then

- If $v_1, \ldots, v_k \in V$ span V, $k \geq n$
- If $v_1, \ldots, v_k \in V$ are linearly independent, then $k \leq n$.

Finite and algebraic extensions

Let $F \leq E$ be a field extension.

- If E is finite-dimensional as a vector space over F, we say that the field extension is **finite**.
- If $F \leq E$ is finite, its **degree**, denoted $[E : F]$, is the dimension of E as a vector space over F.
- If every $\alpha \in E$ is algebraic over F, we say that the field extension is **algebraic**.

Theorem

If the field extension $F \leq E$ is finite, then it is algebraic.

Example

The extension $\mathbb{R} < \mathbb{C}$ is finite (and hence algebraic) of degree 2, since $1, i$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$.

Simple extensions

Let $F \leq E$, and let $\alpha \in E$. The field

$$F(\alpha) \leq E$$

is the smallest subfield of E which contains F and α. If there is an $\alpha \in E$ such that $E = F(\alpha)$, we say $F \leq E$ is a **simple** extension.

Theorem

If α is algebraic, then

$$F(\alpha) = \varphi_\alpha[F[x]] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle.$$

If the degree of $\text{irr}(\alpha, F)$ is n, we have $[F(\alpha) : F] = n$, and one basis for $F(\alpha)$ as a vector space over F is given by

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in F(\alpha)$$

Adjoining elements

Let $F \leq E$ be a field extension, and let $\alpha_1, \ldots, \alpha_n \in E$. The field

$$F(\alpha_1, \ldots, \alpha_n) \leq E$$

is the smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$. An extension $F \leq F(\alpha_1, \ldots, \alpha_n)$ can be obtained as a tower of extensions

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n),$$

where for each i,

$$F(\alpha_1, \ldots, \alpha_i) \leq F(\alpha_1, \ldots, \alpha_{i+1}) = F(\alpha_1, \ldots, \alpha_i)(\alpha_{i+1})$$

is a simple extension.

Theorem

$F \leq E$ is finite if and only if we can find $\alpha_1, \ldots, \alpha_n \in E$, algebraic over F such that $E = F(\alpha_1, \ldots, \alpha_n)$.

Degrees and towers of extensions

Theorem

Let $F \leq K \leq E$ be finite field extensions. Then

$$[E : F] = [E : K][K : F].$$

If $\alpha_1, \ldots, \alpha_{[E:K]} \in E$ is a basis for E as a vector space over K, and $\beta_1, \ldots, \beta_{[K:F]} \in K$ is a basis for K as a vector space over F, then the collection of all products $\alpha_i \beta_j$ is a basis for E as a vector space over F.

Algebraically closed fields

Definition

A field F is **algebraically closed** if every non-constant polynomial $f(x) \in F$ has a zero in F.

Theorem

Let F be an algebraically closed field.

- If $F \leq E$ is an algebraic field extension, then $F = E$.
- If $f(x) \in F[x]$ with $f(x) \neq 0$, then $f(x)$ is a product of polynomials of degree ≤ 1.

Algebraic closures

Definition

Let $F \leq E$ be a field extension. We say E is an **algebraic closure** of F if

1. $F \leq E$ is algebraic, and
2. E is algebraically closed.

Theorem

Every field F has an algebraic closure $F \leq \overline{F}$. It is "unique up to isomorphism": If $\overline{F}$ and $\overline{F}'$ are algebraic closures of F, there is an isomorphism of fields $\psi\colon \overline{F} \to \overline{F}'$ fixing F.

Finite fields

Let F be a finite field, i.e. a field with finitely many elements.

Theorem

The number of elements of F equals p^n for some prime p and integer $n \geq 1$.

Theorem

For every prime p and integer $n \geq 1$ there exists a field $GF(p^n)$ with p^n elements. If $\overline{\mathbb{Z}}_p$ is an algebraic closure of $\mathbb{Z}_p$, we have

$$GF(p^n) = \{\alpha \in \overline{\mathbb{Z}}_p \mid \alpha^{p^n} = \alpha\} < \overline{\mathbb{Z}}_p.$$

This is, up to isomorphism, the unique field with p^n elements: If F is a field with p^n elements, then $F \simeq GF(p^n)$.

If $E < F$ is an extension of finite fields, then $|E| = |E|^{[F:E]}$

Homomorphisms fixing a field

From this point on we fix a field F, an algebraic closure $\overline{F}$, and assume that every field extension $F \leq E$ is such that $E \leq \overline{F}$.

Definition

Let $F \leq E$ and $F \leq E'$. A field homomorphism $\tau\colon E \to E'$ **fixes** F if for every $a \in F$ we have $\tau(a) = a$.

Conjugate elements

Definition

Let F be a field with algebraic closure $\overline{F}$, and let $\alpha, \beta \in \overline{F}$. Then α and β are **conjugate** over F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

Theorem

Let $F \leq E$ be an algebraic extension, and let $\tau \colon E \to \overline{F}$ be a homomorphism fixing F. Then for every $\alpha \in E$, $\tau(\alpha)$ must be a conjugate of α.

Theorem

If $\alpha, \beta \in \overline{F}$ are conjugate over F, there exists a unique isomorphism $\psi_{\alpha,\beta} \colon F(\alpha) \to F(\beta)$ which fixes F, and is such that $\psi_{\alpha,\beta}(\alpha) = \beta$.

Automorphisms

Let $F \leq E$ be a finite field extension.

Definition

An **automorphism** of E is an isomorphism $\sigma\colon E \to E$. The set of automorphisms of E which fix F forms a group with multiplication

$$\sigma\tau = \sigma \circ \tau,$$

which we denote $G(E/F)$.

Index

Let $F \leq E$ be a finite field extension.

Definition

The **index** of the field extension, denoted $\{E : F\}$, is the number of homomorphisms $\tau\colon E \to \overline{F}$ fixing F.

- If α is algebraic over F, then $\{F(\alpha) : F\}$ equals the number of conjugates of α in $\overline{F}$.
- If $F \leq K \leq E$ is a tower of field extensions,

$$\{E : F\} = \{E : K\}\{K : F\}$$

Splitting fields

Definition

- Let $f(x) \in F[x]$. The **splitting field** over F of $f(x)$ is $F(\alpha_1, \ldots, \alpha_m) \leq \overline{F}$, where $\alpha_1, \ldots, \alpha_m$ is the set of zeros of $f(x)$.
- A finite extension $F \leq E$ is **a splitting field** if there exists an $f(x) \in F[x]$ for which E is the splitting field.

Theorem

Let $F \leq E$ be a finite extension. The following are equivalent:

1. $F \leq E$ is a splitting field.
2. Every homomorphism $\tau\colon E \to \overline{F}$ fixing F is an automorphism of E.
3. $|G(E/F)| = \{E : F\}$.

Separable extensions

Let $F \leq E$ be a finite extension.

Definition

The extension is **separable** if $\{E : F\} = [E : F]$.

Definition

A field F is **perfect** if every finite extension $F \leq E$ is separable.

Theorem

If F is of characteristic 0 or if F is finite, then F is perfect.

Galois theory, I

Let $F \leq E$ be a finite extension.

Definition

If the extension is separable and E is a splitting field, we say that $F \leq E$ is **finite normal**.[a]

[a] We follow Fraleigh's terminology here – most other sources call such extensions **Galois**.

In this case,

$$|G(E/F)| = \{E : F\} = [E : F].$$

Galois theory, II

Let $F \leq E$ be a finite extension. We can map subgroups of $G(E/F)$ to fields K with $F \leq K \leq E$ and vice versa.

Subgroup/subfield correspondence

Let $H \leq G(E/F)$ be a subgroup. The **fixed field** of H is

$$E_H = \{\alpha \in E \mid \tau(\alpha) = \alpha \ \forall \tau \in H\},$$

and we have $F \leq E_H \leq E$.
Conversely, given a field K with $F \leq K \leq E$, we get the group $G(E/K)$ as a subgroup of $G(E/F)$.

Galois theory, III

Theorem

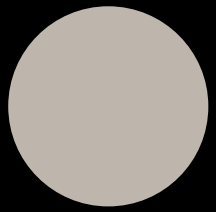
Let $F \leq E$ be a finite normal extension. There is a bijection of sets

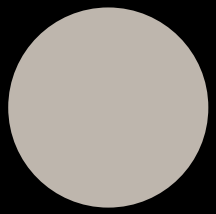
$$\{\text{subgroups } H \leq G(E/F)\} \leftrightarrow \{\text{fields } K \mid F \leq K \leq E\}.$$
$$H \mapsto E_H$$
$$G(E/K) \hookleftarrow K$$

- For all $H \leq G(E/F)$, $|H| = [E : E_H]$
- The subgroup H is normal (as a subgroup) if and only if $F \leq E_H$ is normal (as a field extension). If so

$$G(E/F)/H \simeq G(E_H/F).$$

UiO : Department of Mathematics
University of Oslo





MAT2200 Spring 2026

Revision

