Modern Algebra 1

University of Houston, Fall 2023

MATH 6302 (Dr. Kalantar)

---

1 Groups

1.1 Definitions

group

A **group** is a set with an associative binary operation that has an identity element and every element has an inverse.
Notation: blah blah blah

subgroup

Let G be a group. A non-empty subset $H \subseteq G$ is a **subgroup** if and only if for all $a, b, \in H$,

1. $ab \in H$
2. $a^{-1} \in H$

If H is a subgroup of G it is denoted $H \leq G$.

coset

Let H be a subgroup of G and $g \in G$. The **left coset** of H corresponding to g is $gH := \{gh : h \in H\}$. The **right coset** of H corresponding to g is $Hg := \{hg : h \in H\}$. The set $G/H := \{gH : g \in G\}$ is the **left coset space of** $G \mod H$. Any element of a coset is called a **representative** for the coset.

normal subgroup

A subgroup H of G is a **normal subgroup** if for all $a \in G$, $aHa^{-1} = \left\{aha^{-1} : h \in H\right\} = H$. This is denoted $H \trianglelefteq G$.

quotient group

Let H be a normal subgroup of G. G/H is the **quotient group** of $G \mod H$ with the operations

$$aH \star bH := (ab)H$$
$$(aH)^{-1} := a^{-1}H$$

group homomorphism

Let G_1, G_2 be groups. A **group homomorphism** from G_1 to G_2 is a function $\phi : G_1 \to G_2$ satisfying $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. ϕ is an **isomorphism** if and only if ϕ is a bijection. If there exists an isomorphism between G_1 and G_2, then G_1 is **isomorphic** to G_2, denoted $G_1 \cong G_2$.

kernel

Let $\phi : G \to H$ be group homomorphism. The set $\ker(\phi) \coloneqq \{g \in G : \phi(g) = e_H\}$ is the **kernel** of ϕ.

direct product

Let G_1, G_2 be groups. The **direct product** of G_1 and G_2 is $G_1 \times G_2$, with operation $\star$ defined componenetwise:

- $(g_1, g_2) \star (h_1, h_2) = (g_1 h_1, g_2 h_2)$
- $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$

projection homomorphism

Let $i = 1, 2$. The **projection homomorphism** is $\pi_i : G_1 \times G_2 \to G_i$ defined by $\pi_i(g_1, g_2) = g_i$. This is a surjective homomorphism.

subgroup generated by set

Let G be a group and $S \subseteq G$ be a non-empty subset. The **subgroup generated by** S is the smallest subgroup of G that contains S and is denoted $\langle S \rangle$.

finitely generated group

A group G is **finitely generated** if and only if there exists a subset $S \subseteq G$ such that $\langle S \rangle = G$.

cyclic group

A group G is **cyclic** if there exists $g \in G$ such that $G = \langle \{g\} \rangle$.

torsion element

Let $g \in G$. Then g is a **torsion element** if there exists $n \in \mathbb{N}$ such that $g^n = e$.

order of an element

The **order** of $g \in G$ is the minimum $n \in \mathbb{N}$ such that $g^n = e$. If there is no such n, then g has **infinite order**. The order of g is denoted:

$$o(g) \coloneqq \min \{n \in \mathbb{N} \mid g^n = e\}$$

torsion group

G is a **torsion group** if and only if every $g \in G$ is a torsion element. G is **torsion-free** if and only if G has no non-trivial torsion element.

symmetric group

The **symmetric group** S_n is the set of all bijective functions on the set $\{1, 2, \dots, n\}$. More generally, let X be a set. The **symmetric group** $\mathrm{Sym}(X)$ is the set of all bijective functions $f : X \to X$.

parity of a permutation

The parity of a permutation is the parity of the number (odd or even) of 2-cycles that the permutation can be broken up into.

group action

Let G be a group and X be a set. A **left action of** G **on** X is a map $\beta : G \times X \to X$ such that for all $a, b, \in G$ and $x \in X$,

1. $\beta(e, x) = x$
2. $\beta(a, \beta(b, x)) = \beta(ab, x)$

When β is clearly an action, we write $a \cdot x \coloneqq \beta(a, x)$. A **right action** is defined similarly. A left action is also denoted:

$$G \overset{\beta}{\curvearrowright} X$$

stabilizer

Let $G \curvearrowright X$ and $x \in X$. The **stabilizer** of x is the set $G_x \coloneqq \{g \in G \mid g \cdot x = x\}$.

kernel of a group action

Let $G \curvearrowright X$. The **kernel** of the action is the set $K \coloneqq \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}$. The elements of G which fix all the elements of X.

faithful action

Let $G \curvearrowright X$. The action is **faithful** if and only if the kernel is $\{e\}$. Distinct elements of G induce distinct permutations of X.

free action

Let $G \curvearrowright X$. The action is **free** if and only if $G_x = \{e\}$ for all $x \in X$. No non-trivial element of G fixes a point in G.

center

Let G be a group. The **center** of a group is $\mathrm{Z}(G) \coloneqq \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

centralizer

Let $S \subseteq G$. The **centralizer** of S in G is the set $\mathrm{C}_G(S) \coloneqq \{g \in G \mid gs = sg \text{ for all } s \in S\}$

orbit

Let $G \curvearrowright X$. Define the relation $x \sim_G y$ if and only if there exists $g \in G$ such that $g \cdot x = y$. This is an equivalence relation called the **orbit equivalence relation**. For every $x \in X$, the equivalence class $[x]$ is called the **orbit** of x and $\mathrm{Orb}(x) = [x] = \{g \cdot x \mid g \in G\}$.

conjugacy class

Consider the action of $G \curvearrowright G$ by $g \cdot x = gxg^{-1}$. The **conjugacy class** of $x \in G$ is $\mathrm{C}_x = \mathrm{Orb}\,(x) = [x]$.

index

Let $H \leq G$. The cardinality of the coset space G/H is called the index of H in G, denoted $[G : H]$.

symmetric set

Let $S \subseteq G$ be non-empty. S is a **symmetric set** if $S = S^{-1}$.

word length

Let G be a group generated by a non-empty symmetric set $S \subseteq G$. For every $g \in G, g \neq e$, define the **word legnth** of g with respect to S to be

$$|g|_S \coloneqq \min \{n \in \mathbb{N} \mid g = a_1 a_2 \cdots a_n, \text{ for some } a_1, a_2, \ldots, a_n \in S\}$$

Define $|e|_S \coloneqq 0$.

ball

Let G be a group generated by a non-empty symmetric set $S \subseteq G$. For every $n \in \mathbb{N}$, define the **ball** of radius n around the neutral element to be $B_n \coloneqq \{g \in G \mid |g|_S \leq n\}$. Define the **sphere** of radius n to be $S_n \coloneqq \{g \in G \mid |g|_S = n\}$.

word metric

The **word metric** on a group G generated by a non-empety symmetric subset S is

$$d : G \times G \to \mathbb{N}, \quad d(g, h) \coloneqq |g^{-1}h|_S$$

free group

Insert definition of free group.

1.2 Theorems

Theorem 1.1

Let H be a subgroup of G, and $a, b, \in G$. The following are equivalent:

1. $aH = bH$
2. $a \in bH$
3. $b \in aH$
4. $a^{-1}b \in H$
5. $b^{-1}a \in H$
6. $aH \cap bH \neq \emptyset$

Theorem 1.2

The left cosets of a subgroup give a partition of the group.

Theorem 1.3

The following are equivalent:

1. H is a normal subgroup of G.
2. The operation $\star$ on G/H defined by $aH \star bH \coloneqq (ab)H$ is well defined.
3. For all $a \in G$, $aH = Ha$.
4. For all $a \in G$, $aHa^{-1} \subseteq H$.

Theorem 1.4

Every subgroup of an abelian group is normal.

Theorem 1.5

Let $\phi : G \to H$ be group homomorphism.

1. $\ker(\phi)$ is a normal subgroup of G.
2. $\operatorname{Im}(\phi)$ is a subgroup of H

Theorem 1.6 (First isomorphism theorem)

Let $\phi : G \to H$ be group homomorphism and let $K = \ker(\phi)$. Then $G/\ker(\phi) \cong \operatorname{Im}(\phi)$ by the map $\psi : G/\ker(\phi) \to \operatorname{Im}(\phi), \psi(gK) \coloneqq \phi(g)$. If ϕ is surjective then $G/\ker(\phi) \cong H$.

Theorem 1.7

The maps $\phi_1 : G_1 \to G_1 \times G_2$ and $\phi_2 : G_2 \to G_1 \times G_2$ defined by

- $\phi_1(g_1) = (g_1, e_{G_2})$
- $\phi_2(g_2) = (e_{G_1}, g_2)$

are injective homomorphisms.

Theorem 1.8

Let $\phi : G \to K$ be a group homormophism. ϕ is injective if and only if $\ker(\phi) = \{e\}$.

Theorem 1.9

Let G be a group and $S \subseteq G$ be a non-empty subset. Then

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H = \left\{ a_1 a_2 \dots a_n \mid n \in \mathbb{N}, a_i \in S \cup S^{-1} \right\}$$

where $S^{-1} = \left\{ a^{-1} : a \in S \right\}$.

Theorem 1.10

Every finitely generated group is countable.

Theorem 1.11 (Fundamental theorem of finitely generated abelian groups)

Let G be a finitely generated abelian group. Then there are $r, n_1, n_2, \dots, n_k \in \mathbb{N}$ such that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

Theorem 1.12 (Lagrange's theorem)

Let H be a subgroup of a finite group G. Then $|G| = |H||G/H|$.

Theorem 1.13

Let $a \in G$ be a torsion element and let $n \in \mathbb{N}$. Then $a^n = e$ if and only if $o(a)$ divides n.

Theorem 1.14

Let G be a finite group and p be a prime number that divides $|G|$. Then there exists $g \in G$ such that $o(g) = p$.

Theorem 1.15

If G is a finite group such that $|G| = p$ where p is a prime number, then $G \cong \mathbb{Z}_p$.

Theorem 1.16

Let $\beta : G \times X \to X$ be a left action of G on X. The map $\alpha_g : X \to X$ defined by $\alpha_g(x) \coloneqq g \cdot x$ is a bijection. The map $\alpha : G \to \mathrm{Sym}\,(X)$, $\alpha(g) \coloneqq \alpha_g$ is a group homomorphism.

Theorem 1.17

Let $\alpha : G \to \mathrm{Sym}\,(X)$ be a group homomorphism. Define $\beta : G \times X \to X$ be $\beta(g, x) = (\alpha(g))\,(x)$. Then β is a left action of G on X.

Theorem 1.18

Let $G \curvearrowright X$. Then

1. For all $x \in X$, $G_x \leq G$.
2. The action is faithful if and only if for all $g \neq e$, there exist $x \in X$ such that $g \cdot x \neq x$. Every group element moves at least 1 point except e.
3. The action is free if and only if for all $g \neq e, x \in X$, $g \cdot x \neq x$. Every group element moves all the points except e.
4. The kernel is a normal subgroup of G and $K = \bigcap_{x \in X} G_x$. The kernel of a group action is the intersection of all the stabilizers.

Theorem 1.19

Let X be a set and G a group acting on X. Then for every $g \in G$ and $x \in X$, the stabilizer $g \cdot x$ is $G_{g \cdot x} = \{h \in G : h \cdot (g \cdot x) = g \cdot x\}$ and

$$G_{g \cdot x} = g G_x g^{-1}$$

Theorem 1.20

A group action that is not faithful is also not free.

Theorem 1.21

For every non-empty $S \subseteq G$,

$$\mathrm{C}_G(S) = \mathrm{C}_G(\langle S \rangle) \leq G$$

Theorem 1.22 (Orbit-stabilizer theorem)

Let $G \curvearrowright X$ and $x \in X$. The map $\phi : \operatorname{Orb}(x) \to G/G_x$ defined by $g \cdot [x] \mapsto gG_x$ is a bijection.

Theorem 1.23 (Class equation)

Let G be a finite group and let $g_1, g_2, \ldots, g_n$ be representatives of the distinct conjugacy classes not included in $Z(G)$. Then

$$|G| = |\mathrm{Z}(G)| + \sum_{i}^{n} |\mathrm{C}_{g_i}|$$

Theorem 1.24

H is a finite subgroup if and only if $[G : H] < \infty$.

Theorem 1.25

Let p be a prime number and G be a group with $|G| = p^m$ for some m. Then $\mathrm{Z}(G) \neq \{e\}$.

Theorem 1.26

If $|G| = p^2$, then G is abelian.

Theorem 1.27

If $|G| = p^2$, either $G = \mathbb{Z}_{p^2}$ or $G = \mathrm{Z}_p \times \mathbb{Z}_p$.

Theorem 1.28

Let G be a group generated by a non-empty symmetric set $S \subseteq G$.

$$G = \bigcup_{n \in \mathbb{N}} B_n$$

Theorem 1.29

Let G be a group generated by a non-empty symmetric set $S \subseteq G$. If S is finite, then G is countable.

Theorem 1.30

If G is an infinite cyclic group, then $G \cong \mathbb{Z}$.

Theorem 1.31

If G is finite cyclic group, then $G \cong \mathbb{Z}_n$ and $|G| = n$.

Theorem 1.32

If G is an abelian group and is generated by $\{g_1, g_2, \ldots, g_n\}$, then the map $\phi : \mathbb{Z}^n \to G$ by $(k_1, k_2, \ldots k_n) \mapsto g_1^{k_1} g_2^{k_2} \cdots g_n^{k_n}$ is a surjective homomorphism. Thus by the first isomorphism theorem, $G \cong \mathbb{Z}^n / \ker(\phi)$.

Theorem 1.33

Let $n \in \mathbb{N}$ and $H \leq \mathbb{Z}^n$. Then there are $g_1, g_2, \ldots, g_n \in \mathbb{Z}^n$ and $h_1, h_2, \ldots, h_n \in H$ such that

- $\mathbb{Z}^n \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle$
- $H \cong \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_n \rangle$

where each $h_i \in \langle g_i \rangle$ for all $i = 1, 2, \ldots, n$.

Theorem 1.34 (universal property of the free group)

Let G be a group, S be a non-empty set, and $f : S \to G$ be any function. Then there exists a unique group homomorphism $\phi : \mathcal{F}_S \to G$ such that $\phi(s) = f(s)$ for all $s \in S$.

Theorem 1.35

If S_1, S_2 are non-empty sets with the same cardinality, then $\mathcal{F}_{S_1} \cong \mathcal{F}_{S_2}$.

Theorem 1.36

$\mathcal{F}_2 \ncong \mathcal{F}_3$

Theorem 1.37

Every group is a quotient of a free group.

Theorem 1.38

Let $H \trianglelefteq G$. Define $\pi : G \to G/H$ by $\pi(g) = gH$. π is a surjective homomorphism and $\ker(\pi) = H$.

2 Rings

2.1 Definitions

ring

A **ring** R is a set together with two binary operations, $+$ and $\cdot$ such that

1. $(R, +)$ is an abelian group
2. $\cdot$ is associative: for all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. for all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

commutative

Let $(R, +, \cdot)$ be a ring. R is **commutative** if and only if for all $a, b \in R$, $a \cdot b = b \cdot a$.

unital

Let $(R, +, \cdot)$ be a ring. R is **unital** if and only if there exists $\mathbf{1} \in R$, $\mathbf{0} \neq \mathbf{1}$ such that for all $a \in R$, $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$.

zero divisor

Let R be a ring. A non-zero element $a \in R$ is a **zero divisor** if and only if there exists $b \in R$ such that $b \neq 0$ and $ab = 0$.

unit

Let R be a unital ring. A non-zero element $a \in R$ is a **unit** if and only if there exists $b \in R$ such that $ab = ba = 1$. The set of all units of R is denoted $R^\times$.

integral domain

An **integral domain** is a commutative unital ring R that has no zero divisors.

division ring

A **division ring** is a unital ring R such that $R^\times = R \setminus \{0\}$.

field

A **field** is a commutative division ring.

ring homomorphism

let R, S be rings. A map $\phi : R \to S$ is a **ring homormophism** if and only if for all $a, b \in R$,

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

A bijective ring homomorphism is a **ring isomorphism**. The **kernel** of ϕ is $\ker(\phi) := \{a \in R \mid \phi(a) = 0\}$.

subring

Let R be a ring and S be a non-empty subset of R. S is a subring of R if and only if it is a subgroup of $(R, +)$ that is closed under multiplication. This is denoted $S \leq R$.

ideal

Let R be a ring and $I \subseteq R$ be non-empty. I is a **left ideal** of R if and only if for all $a, b \in I, r \in R$,

1. $a - b \in I$
2. $ra \in I$

A **right ideal** is defined similarly, with $ra \in I$. A **two-sided ideal** has $ra, ar \in I$. In commutative rings, the three are the same.

quotient ring

Let I be an ideal of R. The **quotient ring** is the coset space $R/I := \{r + I \mid r \in R\}$ with the operations

1. $(r_1 + I) + (r_2 + I) := (r_1 + r_2) + I$
2. $(r_1 + I) \cdot (r_2 + I) := (r_1 \cdot r_2) + I$.

trivial ideal

The trivial ideals are $\{0\}$ and R.

ideal generated by a set

Let R be a ring and let E be a non-empty subset of R. The **ideal generated by** E, denoted $\langle E\rangle$, is the smallest ideal of R that contains E.

$$\langle E\rangle \coloneqq \bigcap_{E\subseteq I\trianglelefteq R} I$$

principal ideal

Let I be an ideal of R. If I is generated by a single element, then I is a **principal ideal**.

prime ideal

Let R be a ring and I be an ideal of R. I is a **prime ideal** if and only if for all $a, b \in I$, if $ab \in I$, then either $a \in I$ or $b \in I$.

maximal ideal

Let I be an ideal of R. I is a **maximal ideal** if and only if $I \neq R$ and if $I \subseteq J \trianglelefteq R$, then either $I = J$ or $J = R$.

principal ideal domain

An integral domain R is a **principal ideal domain** (PID) if and only if every ideal in R is principal.

Euclidean domain

An integral domain R is a **Euclidean domain** (ED) if and only if there exists $d : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ where for all $a, b \in R$ and $a \neq 0$, there exists $q, r \in R$ such that $b = aq + r$ with either $r = 0$ or $d(r) < d(a)$.

irreducible element

Let R be an integral domain, $a \in R$ be non-zero, and $a \notin R^\times$. a is **irreducible** if and only if whenever $a = bc$ for some $b, c \in R$, then either $b \in R^\times$ or $c \in R^\times$. Otherwise, a is **reducible**

prime element

Let R be an integral domain, $a \in R$ be non-zero, and $a \notin R^\times$. a is **prime** if and only if $\langle a\rangle$ is a prime ideal.

unique factorization domain

Let R be an integral domain. R is a **unique factorization domain** (UFD) if and only if

- For every non-zero $r \in R \setminus R^\times$, there exists not necessarily distinct irreducible elements $p_1, p_2, \ldots p_n \in R$ such that $r = p_1p_2\cdots p_n$.
- The factorization of r is unique up to re-ordering and multiplying by invertible elements.

field of fractions

Let R be an integral domain. Let $\mathcal{D}$ be the set of all pairs (a,b) where $b \neq 0$ and $a,b \in R$.

$$\mathcal{D} = \{(a,b) \mid a,b, \in R, b \neq 0\} = R \times R \setminus \{0\}$$

Define the following relation on $\mathcal{D}$ by $(a,b) \sim (c,d)$ if and only if $ad = bc$. This is an equivalence relation. Finally, let $\mathbb{F} = \mathcal{D}/\sim$. Define the operations $+$ and $\cdot$ on $\mathbb{F}$ as follows:

1. $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$
2. $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

Then $(\mathbb{F}, +, \cdot)$ is the **field of fractions of** R.

polynomial ring

Let R be a commutative ring. The **polynomial ring** over R is the set

$$R[x] := \left\{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_0, a_1, \ldots, a_n \in R, a_n \neq 0\right\}$$

with operations blah blah blah R can be considered a subring of $R[x]$ by considering all the constant polynomials. If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ and $a_n \neq 0$, the **degree** of f is $\deg(f(x)) := n$.

evaluation map

Let R be a commutative ring. Given $\alpha \in R$, define $e_\alpha : R[x] \to R$ by $e_\alpha(f(x)) = f(\alpha)$. This is the **evaluation map** of α and e_α is a ring homomorphism. α is a **root** of $f(x)$ if and only if $f(\alpha) = 0$.

2.2 Theorems

Theorem 2.1

Let R be a ring, $a, b \in R$. Then

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -ab$
3. $(-a)(-b) = ab$

Theorem 2.2

Let R be a ring and $a, b, c \in R$. If a is not a zero divisor and $ab = ac$, then either $a = 0$ or $b = c$.

Theorem 2.3

Cancellation laws hold in any integral domain.

Theorem 2.4

All fields are integral domains.

Theorem 2.5

If a ring is a subset of a field, then the ring is an integral domain.

Theorem 2.6

Every finite integral domain is a field.

Theorem 2.7

Let R be a ring and S be a non-empty subset of R. The following are equivalent:

1. $S \leq R$
2. $(S, +) \leq (R, +)$ and S is closed under multiplication.
3. For all $a, b, \in S$, $a - b \in S$ and $ab \in S$.

Theorem 2.8

Let R, S be rings and let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi)$ is a subring of R.

Theorem 2.9

The intersection of subrings is a subring. The intersection of ideals is an ideal.

Theorem 2.10

Let S_1, S_2 be subrings of R. $S_1 \cup S_2$ is a subring of R if and only if $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. Analogous for ideals.

Theorem 2.11

Let R be a unital ring and let I be an ideal of R. Then $I = R$ if and only if $1 \in I$.

Theorem 2.12

Let R be a ring and E be a non-empty subset of R. The left ideal generated by E is

$$\langle E \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R, a_i \in E, n \in \mathbb{N} \text{ for all } i = 1, 2, \ldots, n \right\}$$

Theorem 2.13

If $I = \langle a \rangle$, then it is the smallest ideal containing a.

Theorem 2.14

Let R be a commutative unital ring. Then R is a field if and only if $\{0\}$ and R are the only ideals of R.

Theorem 2.15

Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \trianglelefteq R$.

Theorem 2.16

Let $\phi : R \to S$ be a ring homomorphism. Then ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Theorem 2.17

Let $\mathbb{F}$ be a field. Any non-zero ring homomorphism from $\mathbb{F}$ into any ring is injective.

Theorem 2.18

Let I be an ideal of $C([0,1])$. I is maximal if and only if there exists $c \in [0,1]$ such that $I = I_c = \{f \in C([0,1]) \mid f(c) = 0\}$.

Theorem 2.19

Let R be a unital ring. Every proper ideal is contained in a maximal ideal.

Theorem 2.20

Let R be a commutative unital ring and let I be an ideal of R. Then I is a prime ideal if and only if R/I is an integral domain.

Theorem 2.21

Let R be a commutative unital ring and let I be an ideal of R. Then I is a maximal ideal if and only if R/I is a field.

Theorem 2.22

Let R be a commutative unital ring. Every maximal ideal is a prime ideal.

Theorem 2.23

Let $I \trianglelefteq R$. If $I \trianglelefteq J \trianglelefteq R$, then $J/I \trianglelefteq R/I$. Conversely, if $\tilde{J} \trianglelefteq R/I$, there exists $J \trianglelefteq R$ such that $I \trianglelefteq J$ and $\tilde{J} = J/I$

Theorem 2.24

Every ideal of $\mathbb{R}[x]$ is principal.

Theorem 2.25

Every Euclidean domain is a principal ideal domain.

Theorem 2.26

Let R be an integral domain and let $a, b \in R$. Then $\langle a \rangle = \langle b \rangle$ if and only if $b = au$ for some $u \in R^{\times}$.

Theorem 2.27

In any integral domain, every prime element is irreducible.

Theorem 2.28

In any principal ideal domain, every irreducible element is prime.

Theorem 2.29

Every principal ideal domain is a unique factorization domain.

Theorem 2.30

$\mathbb{R}[X]$ is a unique factorization domain.

Theorem 2.31 (Fundeamental theorem of arithmetic)

$\mathbb{Z}$ is a unique factorization domain.

Theorem 2.32

Let R be a principal ideal domain and $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ be an increasing sequnce of ideals of R. Then there exists $N \in \mathbb{N}$ such that for all $n \geq N, I_n = I_N$.

Theorem 2.33

Let R be a principal ideal domain and let $a \in R \setminus R^{\times}$. Then there are $b, q \in R$ such that $a = bq$ and b is irreducible.

Theorem 2.34

Let R be an integral domain, $a \in R$, $u \in R^{\times}$. Then au is irreducible if and only if a is irreducible and au is prime if and only if a is prime.

Theorem 2.35

The operations on the field of fractions are well defined.

Theorem 2.36

Let R be an integral domain and $\mathbb{F}$ its field of fractions. The map $\phi : R \to \mathbb{F}$ by $\phi(r) := [(r, 1)]$ is an injective ring homomorphism. Furthermore, $(R, 1)$ is a subring of $\mathbb{F}$.

Theorem 2.37

Let R be an integral domain.

1. If $p(x), q(x) \in R[x]$ are both non-zero, then $\deg\left(p(x)q(x)\right) = \deg\left(p(x)\right) + \deg\left(q(x)\right)$.
2. $\left(R[X]\right)^{\times} = R^{\times}$.
3. $R[X]$ is an integral domain.

Theorem 2.38

If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a Euclidean domain with respect to degree. Moreover, it is a principal ideal domain, and thus also a unique factorization domain.

Theorem 2.39

Let R be an integral domain. If $I \triangleleft R$ then $I[x] \triangleleft R[x]$.

Theorem 2.40

Let R, S be integral domains. If $\phi : R \to S$ is a ring homomorphism, then the map $\tilde{\phi} : R[x] \to S[x]$ defined by

$$\tilde{\phi}\left(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0\right) = \phi(a_n)x^n + \phi(a_{n-1})x^{n-1} + \cdots + \phi(a_1)x + \phi(a_0)$$

is a ring homomorphism and $\ker(\tilde{\phi}) = \ker(\phi)[x]$.

Theorem 2.41

If R is an integral domain and I is a prime ideal of R, then $I[X]$ is a prime ideal of $R[X]$.

Theorem 2.42

Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in $\mathbb{F}$.

Theorem 2.43

Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ have degree two or three. Then $p(x)$ is reducible if and only if it has a root in $\mathbb{F}$.

Theorem 2.44

Let R be a unique factorization domain and $\mathbb{F}$ its field of fractions. If $p(x)$ is reducible in $\mathbb{F}[X]$ then it is reducible in $R[x]$.

Theorem 2.45

In a unique factorization domain, a nonzero element is prime if and only if it is irreducible.

Theorem 2.46

Let $f(x) \in \mathbb{F}[x]$ with $\deg(f(x)) = n$. Then f has at most n roots in $\mathbb{F}$.

3 Fields

3.1 Definitions

characteristic

Let $\mathbb{F}$ be a field. The **characteristic** of $\mathbb{F}$ denoted $\mathrm{ch}(\mathbb{F})$, is the smallest natural number $n \in \mathbb{N}$ such that $n \cdot 1 := 1 + 1 + \cdots + 1 = 0$. If no such n exists, then $\mathrm{ch}(\mathbb{F}) = 0$.

prime subfield

Let $\mathbb{F}$ be a field. The **prime subfield** of $\mathbb{F}$ is the smallest subfield containing 1.

field extension

Let $\mathbb{K}$ be a field and let $\mathbb{F}$ be a subfield of $\mathbb{K}$. Then $\mathbb{K}$ is an **extension field** of $\mathbb{F}$ and $\mathbb{K} \backslash \mathbb{F}$ is called a **field extension**.

index of a field extension

Let $\mathbb{K} \backslash \mathbb{F}$. The **index of $\mathbb{K}$ over $\mathbb{F}$**, denoted $[\mathbb{K} : \mathbb{F}]$, is the dimension of $\mathbb{K}$ as a vector space over $\mathbb{F}$.

finite extension

$\mathbb{K}$ is a **finite extension** of $\mathbb{F}$ if $[\mathbb{K} : \mathbb{F}] < \infty$.

subfield generated by a subset

Let $\mathbb{K}$ be an extension of $\mathbb{F}$ and let $\alpha_1, \alpha_2, \dots \in \mathbb{K}$ be a collection of elements of $\mathbb{K}$. Then the smallest subfield of $\mathbb{K}$ containing both $\mathbb{F}$ and the elements $\alpha_1, \alpha_2, \dots$ is the **field generated by $\alpha_1, \alpha_2, \dots$ over $\mathbb{F}$**. It is denoted $\mathbb{F}(\alpha_1, \alpha_2, \dots)$.

algebraic element

Let $\mathbb{K}$ be a field extension of $\mathbb{F}$. An element $\alpha \in \mathbb{K}$ is **algebraic over $\mathbb{F}$** if and only if there exists $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$. If α is not algebraic over $\mathbb{F}$, then α is **transcendental over $\mathbb{F}$**.

algebraic extension

An extension $\mathbb{K}\backslash\mathbb{F}$ is an **algebraic extension** if and only if every $\alpha \in \mathbb{K}$ is algebraic over $\mathbb{F}$.

splitting field

Let $f(x) \in \mathbb{F}[x]$. A field extension $\mathbb{K}\backslash\mathbb{F}$ is a **splitting field** for $f(x)$ if and only if $f(x)$ is completely split into the product of linear factors in $\mathbb{K}[x]$. In other words, there are $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{K}$ such that

1. $f(x) = \alpha_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$
2. $f(x)$ does not completely split over any proper subfield of $\mathbb{K}$ that contains $\mathbb{F}$.

In other other words,

$$\mathbb{K} = \mathbb{F}\left(\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n\right)$$

algebraic closure

Let $\mathbb{K}\backslash\mathbb{F}$ be a field extension. $\mathbb{K}$ is the **algebraic closure** of $\mathbb{F}$ if and only if $\mathbb{K}\backslash\mathbb{F}$ is an algebraic extension and every polynomial $f(x) \in \mathbb{F}[x]$ splits completely into linear factors in $\mathbb{K}[x]$.

algebriacally closed

A field $\mathbb{K}$ is **algebraically closed** if and only every every polynomial $f(x) \in \mathbb{K}[x]$ has a root in $\mathbb{K}$.

field automorphism

Let $\mathbb{K}\backslash\mathbb{F}$ be a field extension. A field isomorphism $\phi : \mathbb{K} \to \mathbb{K}$ is an **automorphism** of $\mathbb{K}$. The set of all automorphisms is denoted $\mathrm{Aut}(\mathbb{K})$. In particular, let

$$\mathrm{Aut}(\mathbb{K}\backslash\mathbb{F}) \coloneqq \{\phi \in \mathrm{Aut}(\mathbb{K}) \mid \phi(a) = a \text{ for all } a \in \mathbb{F}\}$$

This the set of all automorphisms of $\mathbb{K}$ that fix $\mathbb{F}$.

fixed field

Let $H \leq \mathrm{Aut}(\mathbb{K})$. The set $\mathrm{Fix}(H) \coloneqq \{\alpha \in \mathbb{K} \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$ is a subfield of $\mathbb{K}$ called the **fixed field of H**.

separable

Let $f(x) \in \mathbb{F}[x]$ and let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}$. Then for some $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{K}$, $f(x) = \alpha_0(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2} \cdots (x-\alpha_k)^{n_k}$. A root α_i is a **multiple root** if $n_i > 1$. $f(x)$ is **separable** if it has no multiple roots.

character of a group

A **character of a group** G with values in a field $\mathbb{F}$ is a homomorphism χ from G to the multiplicative group of $\mathbb{F}$.

$$\chi : G \to \mathbb{F}^{\times}$$

Galois extension

Let $\mathbb{K}\backslash\mathbb{F}$ be a field extension. $\mathbb{K}\backslash\mathbb{F}$ is a **Galois extension** if and only if $|\mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$. In this case $\mathrm{Gal}(\mathbb{K}\backslash\mathbb{F}) = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})$ is the **Galois group**.

3.2 Theorems

Theorem 3.1

$\mathrm{ch}(\mathbb{F})$ is either 0 or a prime number.

Theorem 3.2

- If $\mathrm{ch}(\mathbb{F}) = 0$, the prime subfield of $\mathbb{F}$ is isomorphic to $\mathbb{Q}$.
- If $\mathrm{ch}(\mathbb{F}) = p$, where p is prime, the prime subfield of $\mathbb{F}$ is isomorphic to $\mathbb{Z}_p$.

Theorem 3.3

Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. Then there exists and extension field $\mathbb{K}$ over $\mathbb{F}$ such that f has a root in $\mathbb{K}$.

Theorem 3.4

Let $p(x) \in \mathbb{F}[x]$ be irreducible. Then $[\mathbb{F}[x]/\langle p(x)\rangle : \mathbb{F}] = \deg(p(x))$.

Theorem 3.5

Let $p(x) \in \mathbb{F}[X]$ be irreducible and α be a root in some extension field $\mathbb{K}$ of $\mathbb{F}$. Then $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle p(x)\rangle$.

Theorem 3.6

Let $\phi : \mathbb{F}_1 \to \mathbb{F}_2$ be an isomorphism of fields. Let $p(x) \in \mathbb{F}_1[x]$ be an irreducible polynomial and let $q(x) \in \mathbb{F}_2[x]$ be the polynomial obtained by applying ϕ to the coefficients of $p(x)$. Let α be a root of $p(x)$ in some field extension $\mathbb{K}_1\backslash\mathbb{F}_1$ and let β be a root of $q(x)$ in some field extension $\mathbb{K}_2\backslash\mathbb{F}_2$. Then the isomorphism ϕ extends to an isomorphism of fields $\tilde{\phi} : \mathbb{F}_1(\alpha) \to \mathbb{F}_2(\beta)$ such that $\tilde{\phi}(\alpha) = \beta$.

Theorem 3.7

Every finite extension is an algebraic extension.

Theorem 3.8

Let $\mathbb{K}\backslash\mathbb{F}$ and $\alpha \in \mathbb{K}$. Then α is algebraic over $\mathbb{F}$ if and only if $[\mathbb{F}(\alpha) : \mathbb{F}] < \infty$.

Theorem 3.9

Let $\mathbb{K}\backslash\mathbb{F}$. The set of all elements $\alpha \in \mathbb{K}$ that are algebraic over $\mathbb{F}$ is a subfield of $\mathbb{K}$ containing $\mathbb{F}$.

Theorem 3.10

Let $\mathbb{K}\backslash\mathbb{L}$ and $\mathbb{L}\backslash\mathbb{F}$ be field extensions. If $[\mathbb{K} : \mathbb{L}] < \infty$ and $[\mathbb{L} : \mathbb{F}] < \infty$, then $[\mathbb{K} : \mathbb{F}] < \infty$.

Theorem 3.11

If the powers of α are linearly independent, then the field extension $[\mathbb{F}(\alpha) : \mathbb{F}]$ has infinite index. If the powers of α are linearly dependent, then α is algebraic over $\mathbb{F}$.

Theorem 3.12

Let $f(x) \in \mathbb{F}[x]$. Then there exists a field extension $\mathbb{K}\backslash\mathbb{F}$ such that $\mathbb{K}$ is a splitting field for $f(x)$.

Theorem 3.13

If $\mathbb{K}\backslash\mathbb{L}$ and $\mathbb{L}\backslash\mathbb{F}$ are algebraic extensions, then $\mathbb{K}\backslash\mathbb{F}$ is an algebraic extension.

Theorem 3.14

Let $\mathbb{L}\backslash\mathbb{F}$ be a field extension and let $b_1, b_2, \ldots, b_k \in \mathbb{L}$ be algebraic over $\mathbb{F}$. Then

$$[\mathbb{F}(b_1, b_2, \ldots, b_k) : \mathbb{F}] < \infty$$

Theorem 3.15

Let $\phi : \mathbb{F}_1 \to \mathbb{F}_2$ be an isomorphism of fields. Let $p(x) \in \mathbb{F}_1[x]$ and let $q(x) \in \mathbb{F}_2[x]$ be the polynomial obtained by applying ϕ to the coefficients of $p(x)$. Let $\mathbb{E}_1$ be the splitting field of $p(x)$ over $\mathbb{F}_1$ and let $\mathbb{E}_2$ be the splitting field of $q(x)$ over $\mathbb{F}_2$. Then the isomorphism ϕ extends to an isomorphism of splitting fields $\tilde{\phi} : \mathbb{E}_1 \to \mathbb{E}_2$.

Theorem 3.16

Splitting fields are unique.

Theorem 3.17

Let $\mathbb{K}_1 \cong \mathbb{K}_2$. Then $\mathbb{K}_1$ is algebraically closed if and only if $\mathbb{K}_2$ is algebraically closed.

Theorem 3.18

Let $\mathbb{K}_1\backslash\mathbb{F}_1$ and $\mathbb{K}_2\backslash\mathbb{F}_2$ be field extensions. Suppose there exists an isomorphism of fields $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ such that $\phi(\mathbb{F}_1) = \mathbb{F}_2$. Then

1. $\mathbb{K}_1\backslash\mathbb{F}_1$ is algebraic if and only if $\mathbb{K}_2\backslash\mathbb{F}_2$ is algebraic.
2. $\mathbb{K}_1\backslash\mathbb{F}_1$ is finite if and only if $\mathbb{K}_2\backslash\mathbb{F}_2$ is finite.
3. $\mathbb{K}_1$ is the algebraic closure of $\mathbb{F}_1$ if and only if $\mathbb{K}_2$ is the algebraic closure of $\mathbb{F}_2$

Theorem 3.19

Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}$. Then $\mathbb{K}$ is algebraically closed.

Theorem 3.20

The set $\text{Aut}(\mathbb{K})$ is a group under composition and for any subfield $\mathbb{F} \leq \mathbb{K}$, the set $\text{Aut}(\mathbb{K}\backslash\mathbb{F})$ is a subgroup of $\text{Aut}(\mathbb{K})$.

Theorem 3.21

For any $\phi \in \text{Aut}(\mathbb{K}), \phi(1) = 1$. Thus if $\mathbb{F}$ is the prime subfield of $\mathbb{K}$, then $\phi|_{\mathbb{F}} = \text{id}$ for all $\phi \in \text{Aut}(\mathbb{K})$. So $\text{Aut}(\mathbb{K}\backslash\mathbb{F}) = \text{Aut}(\mathbb{K})$.

Theorem 3.22

If $H_1 \leq H_2 \leq \text{Aut}(\mathbb{K})$ are subgroups, then $\text{Fix}(H_2) \leq \text{Fix}(H_1)$.

Theorem 3.23

If $\mathbb{L}$ is a subfield of $\mathbb{K}$ and $\mathbb{F}$ is a subfield of $\mathbb{L}$, then $\text{Aut}(\mathbb{K}\backslash\mathbb{L}) \leq \text{Aut}(\mathbb{K}\backslash\mathbb{F})$.

Theorem 3.24 (Fundamental theorem of algebra)

$\mathbb{C}$ is algebraically closed.

Theorem 3.25

Let $f(x) \in \mathbb{F}[x]$ and let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}$. Then $|\text{Aut}(\mathbb{K}\backslash\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}]$, with equality if and only if f is separable.

Theorem 3.26

Let $\mathbb{K}$ be a field and G be a finite subgroup of $\text{Aut}(\mathbb{K})$. Let $\mathbb{F}$ be the fixed field of G. Then $|G| = [\mathbb{K} : \mathbb{F}]$.

Theorem 3.27

Let $\mathbb{K}\backslash\mathbb{L}$ and $\mathbb{L}\backslash\mathbb{F}$ be field extensions. Then

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{F}]$$

Theorem 3.28

Let $\mathbb{K}\backslash\mathbb{F}$ be a finite field extension. Then $|\text{Aut}(\mathbb{K}\backslash\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}]$, with equality if and only if $\text{Fix}(\text{Aut}(\mathbb{K}\backslash\mathbb{F})) = \mathbb{F}$.

Theorem 3.29

Let $\phi : \mathbb{F}_1 \to \mathbb{F}_2$ be an isomorphism of fields. Let $p(x) \in \mathbb{F}_1[x]$ and let $q(x) \in \mathbb{F}_2[x]$ be the polynomial obtained by applying ϕ to the coefficients of $p(x)$. Let $\mathbb{K}_1$ be the splitting field of $p(x)$ over $\mathbb{F}_1$ and let $\mathbb{K}_2$ be the splitting field of $q(x)$ over $\mathbb{F}_2$. Then

$$|\{\psi : \mathbb{K}_1 \to \mathbb{K}_2 \mid \psi \text{ is an isomorphism that extends } \phi\}| \leq [\mathbb{K} : \mathbb{F}]$$

with equality if $f(x)$ is separable.

Theorem 3.30

Let $\mathbb{K}$ and $\mathbb{L}$ be fields and $\chi_i : \mathbb{K} \to \mathbb{L}$ be distinct non-zero ring homomorphisms for $i = 1, 2, \ldots, \mathbb{N}$. If there exist $c_1, c_2, \ldots, c_n \in \mathbb{L}$ such that for all $a \in \mathbb{K}$,

$$c_1\chi_1(a) + c_2\chi_2(a) + \cdots + c_n\chi_n(a) = 0$$

then $c_1 = c_2 = \cdots = c_n = 0$.

Theorem 3.31

Let $\mathbb{K}$ be a field and G, H subgroups of $\mathrm{Aut}(\mathbb{K})$. Then $\mathrm{Fix}(G) = \mathrm{Fix}(H)$ if and only if $G = H$.

Theorem 3.32

If $\mathbb{K}$ is the splitting field of a separable $f(x) \in \mathbb{F}[x]$, then $\mathbb{K}\backslash\mathbb{F}$ is a Galois extension.

Theorem 3.33

Let $\mathbb{K}\backslash\mathbb{F}$ be a Galois extension and $p(x) \in \mathbb{F}[x]$ be irreducible. If $p(x)$ has a root in $\mathbb{K}$, then $p(x)$ is separable and completely splits over $\mathbb{K}$.

Theorem 3.34

A finite extension $\mathbb{K}\backslash\mathbb{F}$ is Galois if and only if $\mathbb{K}$ is the splitting field of a separable $f(x) \in \mathbb{F}[x]$.

Theorem 3.35

Let $\mathbb{K}\backslash\mathbb{F}$ be a Galois extension and let $\mathbb{E}$ be a subfield of $\mathbb{K}$ containing $\mathbb{F}$. Then $\mathbb{K}\backslash\mathbb{E}$ is also Galois.

Theorem 3.36

Let $\mathbb{K}\backslash\mathbb{F}$ be a Galois extension and let $\mathbb{E}$ be a subfield of $\mathbb{K}$ containing $\mathbb{F}$. Let $G = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})$ and $H = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{E})$. Then $H \leq G$ and $[G : H] = [\mathbb{E} : \mathbb{F}]$.

Theorem 3.37

Let $\mathbb{K}\backslash\mathbb{F}$ be a Galois extension and let $\mathbb{E}$ be a subfield of $\mathbb{K}$ containing $\mathbb{F}$. Let $G = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})$ and $H = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{E})$. Then $H \leq G$, $H = \{\sigma \in G : \sigma|_{\mathbb{E}} = \mathrm{id}\}$. $\mathbb{E}\backslash\mathbb{F}$ is Galois if and only if H is normal in G.

Theorem 3.38 (Fundamental theorem of Galois theory)

Let $\mathbb{K}\backslash\mathbb{F}$ be a Galois extension and let $G = \mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})$. Then there is a bijection between the subgroups H of G and the subfields $\mathbb{E}$ of $\mathbb{K}$ containing $\mathbb{F}$ ($\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$). This is given by the correspondences:

- $H \mapsto \mathrm{Fix}(H) := \{x \in \mathbb{K} \mid \sigma(x) = x \text{ for all } \sigma \in H\}$
- $\mathbb{E} \mapsto \{\sigma \in G \mid \sigma|_{\mathbb{E}} = \mathrm{id}\}$.

Under this correpondence:

1. If $\mathbb{E}_1, \mathbb{E}_2$ correspond to H_1 and H_2 respectively, then $\mathbb{E}_1 \subseteq \mathbb{E}_2$ if and only if $H_2 \leq H_1$.
2. $[\mathbb{K} : \mathbb{E}] = |H|$ and $[\mathbb{E} : \mathbb{F}] = [G : H]$
3. $\mathbb{K}\backslash\mathbb{E}$ is a Galois extension with Galois group $\mathrm{Aut}(\mathbb{K}\backslash\mathbb{E}) = H$
4. $\mathbb{E}\backslash\mathbb{F}$ is Galois if and only if H is normal in G. In this case,

$$\mathrm{Aut}(\mathbb{E}\backslash\mathbb{F}) \cong \mathrm{Aut}(\mathbb{K}\backslash\mathbb{F})/\mathrm{Aut}(\mathbb{K}\backslash\mathbb{E}) \cong G/H$$

4 Modules

4.1 Definitions

module

Let R be a unital ring and let M be an abelian group. M is a **left R-module** if there exists an operation $\star : R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$,

1. $1 \star x = x$
2. $r \star (s \star x) = rs \star x$
3. $r \star (x + y) = r \star x + r \star y$
4. $(r + s) \star x = r \star x + s \star x$

group representation

Let G be a group and V be a vector space over $\mathbb{F}$. A **representation** of G on V is a group homomorphism $\rho : G \to \mathrm{GL}(V)$. ($\mathrm{GL}(V) \coloneqq \mathrm{Aut}(V)$, the set of all bijective linear transformations $T : V \to V$.)

group ring

The **group ring** $\mathbb{F}[G]$ is defined as

$$\mathbb{F}[G] \coloneqq \{f : G \to \mathbb{F} \mid f \text{ is finitely supported}\}$$

with pointwise addition and product defined by

$$f(x) \star g(y) = \left(\sum_{x \in G} f(x)\delta_x\right) \star \left(\sum_{y \in G} g(y)\delta_y\right) = \sum_{x,y \in G} f(x)g(y)\delta_{xy}$$

bimodule

Let R and S be unital rings. An **(R, S)-bimodule** is a left R-module M that is also a right S-module such that for all $r \in R, s \in S, x \in M$,

$$(r \cdot x) \cdot s = r \cdot (x \cdot s)$$

If R is commutative and M is a left R-module, then M is also a right R-module by defining $(x \cdot r) \coloneqq r \cdot x$. M turns into an (R, R)-bimodule (or R-bimodule).

module homomorphism

Let M and N be left R-modules. A map $\phi : M \to N$ is an **R-module homomorphism** if and only if for all $x, y \in M$ and $r \in R$,

1. $\phi(x + y) = \phi(x) + \phi(y)$
2. $\phi(rx) = r\phi(x)$

free abelian group

Let S be a nonempty set. Let H be the normal subgroup of $\mathcal{F}_S$ generated by the set

$$\left\{s_1 s_2 s_1^{-1} s_2^{-1} \mid s_1, s_2 \in S\right\}$$

The quotient group $\mathcal{A}_S = \mathcal{F}_S / H$ is the **free abelian group generated by** S.

tensor product

Let R be a unital ring, M be a right R-module, and N be a left R-module. Let H be the subgroup of $\mathcal{A}_{M\times N}$ generated by the sets

1. $\{(m_1+m_2,n)-(m_1,n)-(m_2,n) \mid m_1,m_2 \in M, n\in N\}$
2. $\{(m,n_1+n_2)-(m,n_1)-(m,n_2) \mid m\in M, n_1,n_2 \in N\}$
3. $\{(m\cdot r,n)-(m,r\cdot n) \mid m\in M, n\in N\}$

The quotient group $\mathcal{A}_{M\times N}/H$ is called the **tensor product** of M and N and is denoted $M\otimes_R N$. It is an abelian group.
For all $m\in M, n\in N, r\in R$, the elements of the tensor product (H-coset of (m,n)) is denoted $m\otimes n$. By definition,

$$\begin{aligned}(m_1+m_2)\otimes n &= (m_1\otimes n)+(m_2\otimes n)\\ m\otimes(n_1+n_2) &= (m\otimes n_1)+(m\otimes n_2)\\ (m\cdot r)\otimes n &= m\otimes(r\cdot n)\end{aligned}$$

4.2 Theorems

Theorem 4.1

If $\rho : G\to \mathrm{GL}(V)$ is a representation, then V is a left $\mathbb{F}[G]$-module.

Theorem 4.2

If M is an (S,R)-bimodule, then $M\otimes_R N$ turns into a left S-module via

$$s\cdot(m\otimes n) \coloneqq (s\cdot m)\otimes n$$

Theorem 4.3

Every element in $M\otimes_R N$ can be wrritten as a finite sum of cosets.

$$M\otimes_R N = \left\{\sum_{\text{finite}} (m_i\otimes n_i)\right\}$$

Theorem 4.4 (universal property of the tensor product)

Let V,W,Z be vector spaces over $\mathbb{F}$ ($\mathbb{F}$-bimodules). If $T: V\times W\to Z$ is bilinear (when you fix a coordinate, then it is linear), then there exists a unique $\tilde{T} : V\otimes_{\mathbb{F}} W\to Z$ such that $T(v,w)=\tilde{T}(v\otimes w)$.

4.3 Examples

modules

- Let R be a field. Then M as a vector space over R is a left R-module.
- $\mathbb{Z}$-modules are just abelian groups.

$$\begin{aligned}1\cdot x &= x\\ 2\cdot x &= x+x\end{aligned}$$