Algebra Qual
Math 653/654 – Definitions, Theorems and Propositions

Kari Eifler

August 9, 2017

Contents

1 Groups

1 (group + 5 properties)

1. associativity $(ab)c = a(bc)$
2. identity element
3. inverses

A monoid satisfies (1) and (2).

A semigroup satisfies (1).

Properties:

- identity is unique
- inverse is unique
- $(a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1}$
- $a_1a_2...a_n$ is well-defined

A group is called abelian if $ab = ba$ for all $a, b \in G$.

ex. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^\star, \times)$, vector spaces wrt addition, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \text{ with } \det(A) \neq 0\}$

$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \text{ with } \det(A) = 1\}$

2 (S_n, A_n, D_n) S_n = group of permutations on $\{1, 2, ..., n\}$ ie. bijections from $\{1, 2, ..., n\}$ to itself

A_n = even permutations in S_n

D_n = group of symmetries on a regular n-gon

$|Sn| = n!|, An| = n!/2, |Dn| = 2n$

3 (subgroup) A non-empty subset H in G such that

1. $g, h \in H$ then $gh \in H$
2. $g \in H$ then $g^{-1} \in H$

Subgroup criterion: for $g, h \in H$ then $gh^{-1} \in H$

For S subset of G, the subgroup generated by S is denoted $\langle S \rangle$ and is the smallest subgroup containing S (ie. intersection of all subgroups containing S). It consists of all products $g_1^{a_1} ... g_m^{a_m}$ where $g_i \in S$ and $a_i \in \mathbb{Z}$.

4 (homomorphism) a map $f : G \to H$ between groups is a homomorphism if $f(ab) = f(a)f(b)$.

$f(g) = e$ is the trivial homomorphism.

A homomorphism is called

- a monomorphism if it is injective
- epimorphism if it is onto
- isomorphism if it is bijective (ie. it has an inverse). If $\exists f : G \to H$ isomorphism, we write $G \cong H$

5 (equivalence relation) $\sim$ is an equivalence relation if

1. $a \sim a$
2. if $a \sim b$ then $b \sim a$
3. if $a \sim b$ and $b \sim c$ then $a \sim c$

ex. for $H \leq G$ define $g \sim h$ if $gh^{-1} \in H$

6 (cosets) We call gH a left coset. The set of left cosets is denoted G/H.

Note: the map $aH \leftrightarrow Ha$ is not well-defined.

ex. $G = S_3$, $H = \langle (12) \rangle$, then $H(13) = H(132)$ but $(13)H \neq (123)H$.

7 (Lagrange's Theorem) If $H \leq G$ then $|H|$ divides $|G|$

Corollary 1: If $|G|$ is prime, the only subgroups are the trivial ones

Corollary 2: If $|G|$ is prime, then G is cyclic

8 (index) $|G/H| = [G : H]$

If G is finite, $[G : H] = |G|/|H|$

If $G > H > K$, then $[G : K] = [G : H][H : K]$

9 (completely classify $\langle g \rangle$) If all g^n are different, then $\langle g \rangle \cong \mathbb{Z}$. If not, then ker is a non-zero subgroup of $\mathbb{Z}$. Let $d = min(H \cap \mathbb{Z})$ so $dZ \cong ker(n \mapsto g^n)$. Then $\langle g \rangle \cong \mathbb{Z}/d\mathbb{Z}$.

10 (normal subgroup) We say $H \leq G$ is normal if $gH = Hg$.Equivalently, $g^{-1}Hg = g$.

We write $H \lhd G$.

Theorem: If $[G : H] = 2$ then $H \lhd G$

11 (conjugation) Conjugation by $g \in G$ is the map $x \mapsto g^{-1}xg$. This is an isomorphism (an isomorphism with itself is called an automorphism). We write it as $x^g = g^{-1}xg$

12 (simple) A group is simple if the only normal subgroups of G are G and $\{e\}$

ex. $\mathbb{Z}_p$ for prime p are simple

ex. A_n for $n \geq 5$ is simple

13 (coset representations) The multiplication $(gH)(hH) = (gh)H$ is well defined $\Leftrightarrow$ $H \lhd G$

G/H is then a group. Note: the map $g \mapsto gH$ is a homomorphism and is called the "canonical epimorphism"

14 (First Isomorphism Theorem) Let $\varphi : G \to H$ be a homomorphism. Then $\varphi(G) \cong G/\ker(\varphi)$. Moreover, the isomorphism is the map which sends $\varphi(g)$ to $g(\ker \varphi)$

Proof: well-defined, onto, one-to-one

15 (center) $Z(G) = \{h \in G \mid gh = hg \ \forall g \in G\}$.

This is normal in G

16 (propositions for normal) .

Proposition 1: If $H < G$ and $N \lhd G$ then $H \cap N \lhd N$

Proposition 2: If $H < G$ and $N \lhd G$ then $N \lhd \langle H \cup N \rangle = HN = NH$.

Proposition 3: If N and K are normal in G then $N \cap K \lhd G$

Proposition 4: $G/(N \cap K)$ is isomorphic to a subgroup of $G/N \times G/K$

17 (2nd and 3rd Isomorphism Theorems) **2nd Isomorphism Theorem:** For $H < G$, $N \lhd G$ then $HN/N \cong H/(N \cap H)$

3rd Isomorphism Theorem: If $N \lhd G$ and $K \lhd G$ and $K \leq N$ (so $K \lhd N$) then $N/K \lhd G/K$ and $(G/K)/(N/K) \cong G/N$

(should also probably know proofs of these two)

18 (direct product) Let G_i be a collection of groups. Then $\Pi_{i\in I}G_i = \{(g_i)_{i\in I} \mid g_i \in G_i\}$ is the direct product of the groups.

We have multiplication $(g_i)(h_i) = (g_ih_i)$

$\pi_j : \Pi G_i \to G_j$ is the projection (this is an epimorphism)

If H is a group and $\phi_i : H \to G_i$ are homomorphisms then we have a homomorphism $\Psi : H \to \Pi G_i$ which sends h to $(\phi_i(h))$. This is uniquely determined by $\pi_i \circ \Psi = \phi_i$

19 (free group, normal closure, free abelian group) The free group generated by S is the set of all products of $\{a_i\}$ and their inverses. Its elements are all products of $a_{i_1}^{\epsilon_1} \dots a_{i_k}^{\epsilon_k}$ where $\epsilon_i \in \{-1, 1\}$.

The normal closure of R is the smallest normal subgroup containing R, denoted $\langle\rangle$. Its elements are all products of the form $(g_1^{-1})(r_1^{\epsilon_1})(g_1)...(g_n^{-1})(r_n^{\epsilon_n})(g_n)$ where $\epsilon_i \in \{-1, 1\}$

The free abelian group generated by two elements is written $\langle a, b|ab = ba\rangle$.

20 (action) A (left) action of a group G on a set X is a map $G \times X \to X$, $(g, x) \mapsto gx$ satisfying:

1. $ex = x$
2. $(g_1g_2)x = g_1(g_2x)$

We call an action faithful if it is injective. The kernel of the action is the group of elements g acting identically ($gx = x$ for all $x \in X$). The stabilizer of x is the group $G_x = \{g \in G \mid gx = x\} < G$.

21 (equivalence classes of an orbit + transitive + free + Theorem) We say $x \sim y$ if there exists $g \in G$ such that $gx = y$

The equivalence classes are called the orbits of the action

An action is called transitive if it only has one orbit

An action is called free if every stabilizer is trivial

ex. every group acts on itself by multiplication on the left. Here, the action is free.

Theorem: Let G act on X freely and transitively. Then there exists a bijection $\phi : X \to G$ such that $\phi(gx) = g\phi(x)$

Theorem: If an action of G on X is transitive then $|X| = [G : G_x]$ for any x

ex. for every g, $x \mapsto x^g = g^{-1}xg$ is an automorphism of G on itself

22 (center + stabilizer + centralizer + normalizer) $Z(G) = \{g : gx = xg \ \forall x \in G\}$

this is the center of G.

For $h \in G$, the stabilizer of h is $\{g \mid gh = hg\}$, also called the centralizer of h

If $A \subseteq G$ then the centralizer of A is $Z_G(A) = \{g \in G \mid ga = ag \ \forall a \in A\}$

If $H \leq G$, then the normalizer of H is $\{g \in G \mid H = g^{-1}Hg\}$

23 (free abelian group generated by S) The free abelian group generated by S is $\{s_j \mid s_i s_j = s_j s_i \ \forall s_i \in S\}$

All other abelian groups generated by S are natural homomorphism images of that

24 (Fundamental Theorem on finitely generated abelian groups) If G is a finitely generated abelian group, then there exists unique $d_1|d_2|...|d_k$ and $r \geq 0$ such that

$$G = C_{d_1} \oplus C_{d_2} \oplus ... \oplus C_{d_k} \oplus \mathbb{Z}^r$$

where C_{d_i} is the cyclic group of order d_i and r=# zeros on the diagonal of the smith normal form

ALTERNATE FORM: If G is a finitely generated abelian group, then there exists unique $r \geq 0$ and $q_1, ..., q_n$ which are powers of (not necessarily distinct) prime numbers and $G = C_{q_1} \oplus ... \oplus C_{q_n} \oplus \mathbb{Z}^r$

25 (p-group + Theorem + Corollary + Proposition) A group is called a p-group if the order of every element is finite and is a power of p, where p is prime.

Theorem: If p divides $|G|$, then there exists an element g of order p

Corollary: A finite group G is a p-group if and only if $|G| = p^k$ for some k

Proposition: the center of a finite p-group is non-trivial

26 (1st Sylow Theorem) Suppose that p^k divides $|G|$. Then G contains a subgroup of order p^k

27 (Sylow p-subgroups) If p^k is the highest order of prime dividing $|G|$, then a subgroup of order p^k is called a Sylow p-subgroup

28 (2nd Sylow Theorem) Let P be a p-subgroup of G and let H be a Sylow p-subgroup. Then there exists some $g \in G$ such that $g^{-1}Pg < H$.

In particular, all Sylow subgroups are conjugate to one another.

29 (3rd Sylow Theorem) The number of Sylow p-subgroups divides $|G|$ and is congruent to 1 mod p

30 (groups of each order) 1: e

2: $\mathbb{Z}_2 = C_2$

3: C_3

4: $C_2 \times C_2$, C_4

5: C_5

6: $C_6 = C_2 \times C_3$, $S_3 = D_3$

7: C_7

8: C_8, $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, Q, D_4

2 Rings

31 (ring) A ring R is a set with two binary operators: $+$ and $\cdot$ s.t.

1. $(R, +)$ is an abelian group
2. $a(b + c) = ab + ac$
3. $a(bc) = (ab)c$

Also, may want it to have an identity or to be commutative

ex. $\mathbb{R}, \mathbb{C}, M_n(\mathbb{R}), C(X), \mathbb{Z}[G]$

32 ((left) zero divisor + left invertible) a is a left zero divisor if there exists some $b \neq 0$ such that $ab = 0$ (similar for right)

a is a zero divisor if it is simultaneously a left and right zero divisor

ex. $\mathbb{Z}/n\mathbb{Z}$ where n is not prime has zero divisors

ex. In $M_n(\mathbb{R})$, the zero divisors are the matrices which are not divisible

If R has identity, a is left invertible if there exists some b such that $ba = 1$.

33 (integral domain + division ring + field + homomorphism) A commutative ring with $0 \neq 1$ is called an integral domain if it has no zero divisors

If every non-zero element is invertible, then it is called a division ring

A commutative division ring is called a field

A homomorphism if a map f between rings R_1 and R_2 such that $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$

34 ((left) ideal) A left ideal of R is a non-empty subset I which is a subgroup of the additive group such that $ra \in I$ whenever $r \in R$, $a \in I$

Note: an ideal is a subring (without identity)

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

The smallest left ideal containing $a_1, a_2, ..., a_n$ is $\{x_1a_1 + x_2a_2 + ... + x_na_n + k_1a_1 + ... + k_na_n : x_i \in R, k_i \in \mathbb{Z}\}$

The smallest (two-sided) ideal is much more complicated: $\{x_{11}a_1y_{11} + a_{12}a_1y_{12} + ... + x_{nm}a_ny_{nm}\}$

If R is a ring and I a (two-sided) ideal then R/I is an additive group

35 (principal ideal + principal ring + PID) An ideal is called principal if it is generated by one element.

A ring is called a principal ring if all its ideals are principal.

A principal ideal domain (PID) is a domain in which all ideals are principal.

Recall: integral domain is commutative + no zero divisors

36 (Theorems about ideals) **Theorem 1:** If $f : R_1 \to R_2$ is a homomorphism, then $f(R_1) = R_1/\ker f$, $f(r)$ from $r + \ker f$

Theorem 2: If I, J are two ideals, then $I/(I \cap J) = (I + J)/J$

Theorem 3: If $I \subset J$ are two ideals then $R/J = (R/I)/(J/I)$

ex. if $R = \mathbb{Z}$ and (n) is the ideal generated by n, then

$(n) + (m) = (\gcd(n, m))$, $(n) \cap (m) = (lcm(n, m))$

37 (prime ideal) An ideal $P \neq R$ is said to be prime if it cannot be written as the product of two ideals

i.e. for all ideals A, B if $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$

Theorem: P is prime if and only if for every $a, b \in R$ if $ab \in P$ then $a \in P$ or $b \in P$

Theorem: If R is commutative with identity then an ideal P is prime if and only if R/P is an integral domain

38 (maximal) An ideal I is called maximal if $I \neq R$ and for every ideal J such that $I \subseteq J$ either $I = J$ or $J = R$

ex. In $\mathbb{Z}$, (n) subset of (m) IFF m divides n

Theorem: Let R be a ring with identity. Then every proper ideal is contained in a maximal ideal.

Theorem: Let R be a commutative ring with identity. Then every maximal ideal is prime.

Theorem: Let R be a commutative ring with identity. Then an ideal I is maximal if and only if R/I is a field.

39 (Theorem (direct product, ideals) + Corollary + Corollary) **Theorem:** If R is a ring and $A_1, ..., A_n$ are ideals and

1. $A_1 + A_2 + ... + A_n = R$
2. $A_i \cap (A_1 + ... + A_{i-1} + A_{i+1} + ... + A_n) = 0$

Then $R = A_1 \times ... \times A_n$

Corollary 1: Under the same conditions, $R/(A_1 \cap ... \cap A_n) \cong R/A_1 \times ... \times R/A_n$

Corollary 2: If $n = p_1^{k_1}...p_s^{k_s}$ for pairwise different primes p_i then $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_s^{ks}\mathbb{Z}$

40 (divides) For a commutative ring R, $a|b$ if there exists an x such that $b = ax$

We get an equivalence relation: $a \sim b$ if and only if $a|b$ and $b|a$. So $a = b$ times a unit.

Proposition: $a|b$ if and only if (a) contains (b)

Corollary: $a \sim b$ if and only if $(a) = (b)$

Proposition: u is a unit (ie. an invertible element) if and only if $(u) = R$

41 (irreducible + prime) A non-unit element a is irreducible if whenever $b|a$ either b is a unit or $b \sim a$ (the latter, if R is a domain means $b = au$ for a unit u)

If R is a domain, this can be reformulated as: if whenever $a = a_1a_2$ either a_1 or a_2 is a unit.

Proposition: a is irreducible iff (a) is maximal among proper principal ideals

A non-unit element a is prime if $a|b_1b_2$ implies $a|b_1$ or $a|b_2$

Theorem: In a PID, every irreducible element is prime.

42 (Chinese Remainder Theorem) $A_1, ..., A_k$ are ideals in R with identity such that $A_i + A_j = R$ for $i \neq j$

If $b_1, ..., b_n \in R$ then $\exists b \in R$ s.t. $b - b_i \in A_i$. Moreover, b is unique modulo $A_1 \cap A_2 \cap ... \cap A_n$

43 (UFD, Noetherian) A domain R is a unique factorization domain (UFD) if every non-zero element can be written as a product $p_1 p_2 \dots p_n$ of irreducible elements in a unique way up to permutation of elements and units. Such a decomposition always exists.

A ring R is Noetherian if it does not have an infinite strictly increasing chain of ideals. Note that every element of a Noetherian domain can be decomposed into a product of irreducible elements.

44 (Euclidean) A commutative ring R is Euclidean if there exists a map $\varphi : R\backslash\{0\} \to \mathbb{N}$ such that

- $a, b \in R$ and $ab \neq 0$ then $\varphi(a) \leq \varphi(ab)$
- $\forall a, d \in R$ with $d \neq 0$ then $\exists q, r \in R$ such that $a = dq + r$ and either $r = 0$ or $\varphi(r) < \varphi(q)$

ex. $\mathbb{Z}$ with $\varphi(n) = |n|$, $\mathbb{Z}[\sqrt{2}]$ with $\varphi(a + b\sqrt{2}) = a^2 - 2b^2$

Proposition: Every Euclidean ring is PID

45 (ring of quotients, RS^{-1}) Let R be a commutative ring, $0 \notin S \subseteq R$ a multiplicative set. Define a/b for $a \in R$, $b \in S$ as the equivalence class of the pair (a, b) with the relation $(a_1, b_1) \sim (a_2, b_2)$ if there exists some $s \in S$ such that $sa_1b_2 = sb_1a_2$.

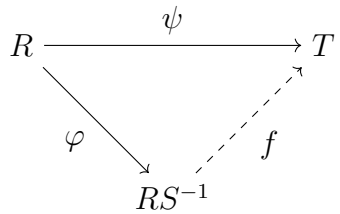
Then the ring of quotients RS^{-1} is the set $\{a/b \mid a \in R, b \in S\}$ with operations $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}$ and $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}$.

If R is a domain and we take $S = R\backslash\{0\}$ then RS^{-1} is called the quotient field of R.

If R is a domain, then the map $\varphi_s : R \to RS^{-1}$ defined via $r \mapsto \frac{rs}{s}$ is well-defined, and a monomorphism.

Let P be a prime ideal of R. Take $S = R\backslash P$ (this is multiplicative since P is prime). Then $S^{-1}R$ is called the localization of R at P.

46 ($S^{-1}R$) Theorem: Suppose T is commutative with identity, $\psi : R \to T$ is a homomorphism such that $\psi(s)$ is a unit in T for all $s \in S$. Then there exists a unique $f : RS^{-1} \to T$ making the following diagram commutative



Corollary: Let R be a domain. Then for any monomorphism ψ from R to a field $\mathbb{K}$, there exists a unique homomorphism f from the field of quotients of R to $\mathbb{K}$.

47 (local) A commutative ring with identity is local if it has a unique maximal ideal.

Equivalently, a commutative ring with identity is local if the set of non-invertible elements is an ideal.

48 (polynomials over R) $R[x] = \{r_0 + r_1x + \cdots + r_nx^n \mid r_i \in R\}$, where multiplication and addition are defined in the obvious way. We let $n = \deg(r_0 + r_1x + \cdots + r_nx^n)$.

1. $\deg(fg) \leq \deg(f) + \deg(g)$

   If R has no zero divisors and $f \neq 0 \neq g$ then $\deg(fg) = \deg(f) + \deg(g)$

2. $\deg(f + g) \leq \max(\deg(f), \deg(g))$

   If $\deg(f) \neq \deg(g)$ then $\deg(f + g) = \max(\deg(f), \deg(g))$

3. If the leading coefficient of $g(x)$ is a unit, then for every $f(x) \in R[x]$, there are unique $q(x), r(x) \in R[x]$ such that $f = gq + r$ and either $r = 0$ or $\deg(r) < \deg(g)$.

Theorem: Let R, S be commutative rings with identity, and let $\varphi : R \to S$ be a homomorphism such that $\varphi(1_R) = 1_S$. Then for any $s_1, s_2, \ldots, s_n \in S$ there exists a unique homomorphism $\overline{\varphi} : R[x_1, \ldots, x_n] \to S$ such that $\overline{\varphi}|_R = \varphi$ and $\overline{\varphi}(x_i) = s_i$.

49 (ring of formal power series) We can define a ring with infinitely many variables, and it is still a ring. We call it the ring of formal power series, denoted $R[[x]]$.

Proposition: $r_0 + r_1x + r_2x^2 + \ldots$ is a unit in the formal power series $\Leftrightarrow$ a_0 is a unit in R.

50 (Bezout) Bezout's Theorem: The remainder of division of $f(x)$ by $x - c$ is $f(c)$.

In particular, $(x - c)|f(x) \Leftrightarrow f(c) = 0$.

Proposition: If $c_1, c_2, \ldots, c_n$ are pairwise different roots of $f(x)$ and R has no zero divisors, then $(x - c_1) \ldots (x - c_n)|f(x)$. In particular, $n \leq \deg(f)$.

Proposition: $c \in R$ is a multiple root of $f(x)$ if and only if $f(c) = 0 = f'(c)$.

51 (content) If $f = a_0 + a_1x + \cdots + a_nx^n$ then $C(f) = \gcd(a_0, a_1, \ldots, a_n)$ is called the content.

Lemma: If D is a UFD then $C(fg) = C(f)C(g)$ up to a unit.

We say $f \in D[x]$ is primitive if $C(f) = 1$.

52 (Eisenstein's Criterion) Suppose $f(x) \in \mathbb{Z}[x]$ is primative, and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $\deg(f) \geq 1$ and for some prime p, p does not divide a_n, but $p|a_k$ for $k = 0, 1, \ldots, n-1$ but p^2 does not divide a_0, then $f(x)$ is irreducible

Corollary: Suppose $f = a_nx^n + \cdots + a_1x + a_0$. If there exists a prime p such that p does not divide a_n, if f is irreducible modulo p then f is irreducible over $\mathbb{Z}$ (hence also $\mathbb{Q}$)

53 (Irreducibility over $\mathbb{Z}$) Suppose $f \in \mathbb{Z}[x]$. Then f irreducible in $\mathbb{Z}[x]$ iff irr. in $\mathbb{Q}[x]$

3 Category Theory

54 (category, morphism, isomorphism) A category is a class $\mathcal{C}$ of objects together with morphisms such that for each pair (A, B) of objects in $\mathcal{C}$, there exists a set $\hom(A, B)$ with the property that if $(A, B) \neq (A', B')$ then $\hom(A, B) \cap \hom(A', B') = \emptyset$.

If $f \in \hom(A, B)$ then we write $f : A \to B$.

Morphisms can be composed: for any triple (A, B, C) of objects in $\mathcal{C}$, there is a function

$$\begin{aligned} \hom_{\mathcal{C}}(B, C) \times \hom_{\mathcal{C}}(A, B) &\to \hom_{\mathcal{C}}(A, C) \\ (g, f) &\mapsto g \circ f \end{aligned}$$

which satisfy

1. associativity

   if $f : A \to B$, $g : B \to C$, $h : C \to D$ then $h \circ (g \circ f) = (h \circ g) \circ f$

2. identity

   for every object B of $\mathcal{C}$, there exists a morphism $1_B : B \to B$ so that for any $f : A \to B$ or $g : B \to C$, $1_B \circ f = f$ and $g \circ 1_B = g$.

A morphism $f : A \to B$ in $\mathcal{C}$ is called an isomorphism if there exists a morphism $g : B \to A$ in $\mathcal{C}$ so that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.

55 (covariant / contravariant functor) Let $\mathcal{A}$ and $\mathcal{B}$ be categories. A covariant functor $F : \mathcal{A} \to \mathcal{B}$ is an assignment such that

1. $\forall A \in \mathrm{Ob}(\mathcal{A})$ we have $F(A) \in \mathrm{Ob}(\mathcal{B})$
2. $\forall f : A \to A'$ in $\mathrm{Mor}(\mathcal{A})$, we have $F(f) : F(A) \to F(A')$ in $\mathrm{Mor}(\mathcal{B})$

It must satisfy

(a) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for all $A \in \mathrm{Ob}(\mathcal{A})$

(b) $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : A \to B$ and $g : B \to C$ in $\mathrm{Mor}(\mathcal{A})$

We call such a functor a contravariant functor if requirement 2. is changed to: $\forall f : A \to A'$ in $\mathrm{Mor}(\mathcal{A})$, we have $F(f) : F(A') \to F(A)$ in $\mathrm{Mor}(\mathcal{B})$

4 Modules

56 (module) Let R be a ring (with identity). We say M is a left R-module if

1. M is an abelian group (wrt addition)
2. there exists scalar multiplication by R on M

$$\begin{aligned} \cdot : R \times M &\to M \\ (r, m) &\mapsto r \cdot m =: rm \end{aligned}$$

satisfying

(a) $(r_1 + r_2)m = r_1 m + r_2 m$
(b) $(r_1 r_2)m = r_1(r_2 m)$
(c) $1_R m = m$
(d) $r(m_1 + m_2) = rm_1 + rm_2$

ex. Abelian groups $\leftrightarrow$ $\mathbb{Z}$-modules

Let ${}_R\mathcal{M}$ be the category of left R-modules.

57 (quotient modules) Given $N \subseteq M$ as R-modules and as groups $N \lhd M$. We can then form the quotient group $M/N = \{m + N \mid m \in M\}$ has an induced structure of an R-module: $r(m + N) := rm + N$.

58 (R-module homomorphism) Given R-modules M and M', a function $f : M \to M'$ is an R-module homomorphism if

$$f(m_1 + m_2) = f(m_1) + f(m_2) \qquad f(r \cdot m) = r \cdot f(m).$$

Theorem: TFAE:

1. $f : M \to M'$ is an isomorphism
2. f is invertible wrt composition

   i.e. there exists an R-module homomorphism $g : M' \to M$ such that $g \circ f = \mathrm{id}_M$ and $f \circ g = \mathrm{id}_{M'}$
3. f is an isomorphism of abelian groups
4. f is one-to-one and onto

59 (First Isomorphism Theorem) Given $f : M \to M'$ an R-module homomorphism, the function

$$\begin{aligned} \overline{f} : M/\ker(f) &\to f(M) \\ m + \ker(f) &\mapsto f(m) \end{aligned}$$

is an isomorphism of R-modules

60 (direct product, (external/internal) direct sum) Given R-modules M_i,

$$\Pi_{i \in I} M_i = \{(m_i)_{i \in I}\}$$

is called the direct product. This is an R-module where scalar multiplication is entrywise: $r \cdot (m_i)_{i \in I} = (r \cdot m_i)_{i \in I}$.

Define the (external) direct sum to be

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \in \Pi_{i \in I} M_i \mid \text{ for all but finitely many } i \in I, m_i = 0\}$$

This is an R-submodule of the direct product.

Suppose $M_i \subseteq M$ are R-submodules of M. Then define the internal sum to be

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in I} m_i \mid m_i \in M_i, m_i = 0 \text{ for almost all } i \right\}.$$

If $M_i \subseteq M$, we have an R-module homomorphism

$$\phi : \bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i \subseteq M$$
$$(m_i)_{i\in I} \mapsto \sum_{i\in I} m_i$$

This is always surjective.

61 ((short) exact sequenes) Given R-module homomorphisms $f : N \to M$ and $g : M \to P$, we call the diagram

$$N \xrightarrow{f} M \xrightarrow{g} P$$

a sequence of R-module homomorphisms. We say the sequence is exact at M if $\operatorname{Im} f = \ker g$.

Proposition: The sequence $0 \to N \xrightarrow{f} M$ is exact IFF f is injective.

Proposition: The sequence $M \xrightarrow{g} P \to 0$ is exact IFF g is surjective.

An exact sequence of the form

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$$

is called a short exact sequence (so f is injective, g is surjective, $\operatorname{Im}(f) = \ker(g)$.

62 (Hom-Groups) Fix a ring R and let A, B be left R-modules. Let

$$\operatorname{Hom}_R(A, B) = \{f : A \to B \mid f \text{ is an } R\text{-module homomorphism}\}$$

This is an abelian group under addition of functions.

Proposition: If R is commmutative, then $\operatorname{Hom}_R(A, B)$ is an R-module by setting $(rf)(a) = r \cdot f(a) = f(ra)$.

Suppose $\varphi : A \to B$ is a fixed R-module homomorphism and let $f \in \operatorname{Hom}_R(M, A)$. Then define $\varphi_*(f) = \varphi \circ f \in \operatorname{Hom}_R(M, B)$. So the assignment $\varphi_* : \operatorname{Hom}_R(M, A) \to \operatorname{Hom}_R(M, B)$ is a group homomorphism.

For M an R-module, we have a functor

$$\begin{aligned}\mathrm{Hom}_R(M,-) :_R \mathcal{M} &\to \mathrm{Ab} \\ A &\mapsto \mathrm{Hom}_R(M,A) \\ \left(A \xrightarrow{\varphi} B\right) &\mapsto \left(\mathrm{Hom}_R(M,A) \xrightarrow{\varphi_*} \mathrm{Hom}_R(M,B)\right)\end{aligned}$$

Proposition: For a fixed M, $\mathrm{Hom}_R(M,-)$ is a covariant additive functor. It is also a left exact covariant functor.

Proposition: For a fixed R-module N, $\mathrm{Hom}_R(-,N)$ is a left exact contravariant functor.

Theorem: For a ring R and a free R-module F, the functor $\mathrm{Hom}_R(F,-) :_R \mathcal{M} \to \mathrm{Ab}$ is exact.

63 (additive functor / exact) Let R and S be rings. Then $F :_R \mathcal{M} \to_S \mathcal{M}$ is additive if for all $A, B \in_R \mathcal{M}$ the induced map

$$\begin{aligned}F_{AB} : \mathrm{Hom}_R(A,B) &\to \mathrm{Hom}_R(F(A),F(B)) \\ \left(A \xrightarrow{f} B\right) &\mapsto \left(F(A) \xrightarrow{F(f)} F(B)\right)\end{aligned}$$

is a group homomorphism.

An additive covariant functor $F :_R \mathcal{M} \to_S \mathcal{M}$ is exact if for any R-modules A, B, C if $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence of R-modules, then $0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \to 0$ is an exact sequence of S-modules.

64 (left / right exact) We say $F :_R \mathcal{M} \to_S \mathcal{M}$ is left exact if we have a short exact sequence of R-modules $0 \to A \to B \to C \to 0$, then $0 \to F(A) \to F(B) \to F(C)$ is an exact sequence of S-modules.

Similar for right exact.

65 (generating sets) Let R be a ring, M an R-module, and $S \subseteq M$ be a subset. Then we define the sub-R-module of M generated by S, to be

$$\left\{r_1x_1 + \cdots + r_nx_n \mid r_i \in R, x_i \in S, n \geq 1\right\} = \sum_{x \in S} Rx = (x : x \in S)_R$$

We say M is finitely generated over R if there exists a finite set $\{x_1, \ldots, x_n\} \subseteq M$ so that $M = Rx_1 + \cdots + Rx_m = (x_1, \ldots, x_m)_R$.

A set S is linearly independent over R if whenever $r_1x_1 + \cdots + r_mx_m = 0$ with $r_i \in R$,

$x_i \in S \subseteq M$, we must have $r_k = 0$. Otherwise, S is linearly dependent over R.

If $B \subseteq M$ is linearly independent over R and B generates M over R, then we call B a basis of M as an R-module.

An R-module M that has a basis is called a free R-module.

Proposition: If M is free with $B \subseteq M$ then

$$\begin{aligned} f : \bigoplus_{x \in B} R &\to M \\ (r_x)_{x \in B} &\mapsto \sum_{x \in B} r_x \cdot x \in M \end{aligned}$$

is an isomorphism of R-modules IFF B is a basis.

Corollary: An R-module M is free IFF $M \cong \oplus_{i \in I} R$ as an R-module.

Theorem: Let R be a PID, let F be a free R-module. If $M \subseteq F$ is a submodule then M is free and $\text{rank}_R(M) \leq \text{rank}_R(F)$.

66 (torsion) For an R-module M, we say $x \in M$ is torsion of there exists some $r \in R$, $r \neq 0$ such that $r \cdot x = 0$.

Take $M_{\text{tor}} = \{m \in M \mid m \text{ is } R\text{-torsion}\}$. This is a submodule of M.

We say M is torsion-free as an R-module if $M_{\text{tor}} = \{0\}$.

67 (Splitting Lemma) Let $0 \to N_1 \xrightarrow{f} M \xrightarrow{g} N_2 \to 0$ be an exact sequence of R-modules. TFAE:

1. there exists an R-module homomorphism $\psi : N_2 \to M$ such that $g \circ \psi = \text{id}_{N_2}$
2. there exists an R-module homomorphism $\varphi : M \to N_1$ such that $\varphi \circ f = \text{id}_{N_1}$

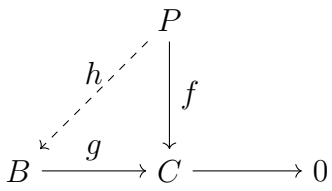
If these conditions are satisfies, then

$$M = \text{Im}(f) \oplus \ker(\varphi) = \ker(g) \oplus \text{Im}(\psi) \cong N_1 \oplus N_2.$$

In this case, we say that the exact sequence is split and that φ and ψ are splittings.

Proposition 1: Let F be a free R-module. Any short exact sequence of R-modules of the form $0 \to A \xrightarrow{f} B \xrightarrow{g} F \to 0$ is split.

68 (Projective) An R-module P is projective if whenever $f : P \to C$ is an R-module homomorphism and $g : B \to C$ is a surjective R-module homomorphism, then there exists an R-module homomorphism $h : P \to B$ such that $g \circ h = f$.

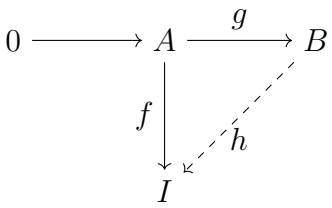


Theorem: Let R be a ring and P an R-module. TFAE:

1. P is projective
2. Every exact sequence $0 \to A \to B \to P \to 0$ of R-modules splits
3. There is an R-module M such that $M \oplus P$ is free
4. The functor $\mathrm{Hom}_R(P, -) :_R \mathcal{M} \to \mathrm{Ab}$ is exact

Corollary: Free modules are projective modules

69 (injective) An R-module I is injective if whenever $f : A \to I$ is an R-module homomorphism and $g : A \to B$ is an injective R-module homomorphism, then there exists an R-module homomorphism $h : B \to I$ such that $h \circ g = f$.



Theorem: Let R be a ring and I an R-module. TFAE:

1. I is injective
2. Every exact sequence $0 \to I \to B \to C \to 0$ of R-modules splits
3. If $I \subseteq B$ as a submodule, then there exists a submodule $C \subseteq B$ such that $B \cong I \oplus C$.
4. The functor $\mathrm{Hom}_R(-, I) :_R \mathcal{M} \to \mathrm{Ab}$ is exact

70 (divisible abelian group) D is a divisible abelian group if $\forall n \in \mathbb{Z}\ n \neq 0$ the homomorphism

$$\begin{aligned}[n] : D &\to D \\ x &\mapsto nx\end{aligned}$$

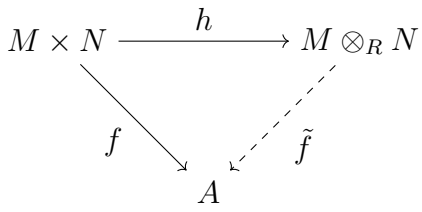
is surjective.

Proposition: Let D be an abelian group. Then D is divisible $\Leftrightarrow$ D is an injective $\mathbb{Z}$-module.

5 Tensor Products

71 ($M \otimes_R N$) Let R be a ring, M a right R-module, N a left R-module. Then $M \otimes_R N$ is an abelian group together with an R-biadditive map $h : M \times N \to M \otimes_R N$ which satisfies:

For all abelian groups A and R-biadditive maps $f : M \times N \to A$ there exists a unique group homomorphism $\tilde{f} : M \otimes_R N \to A$ such that $f = \tilde{f} \circ h$



Theorem: Let R be a ring, M a left R-module, N a right R-module. Then $M \otimes_R N$ exists and is unique up to unique isomorphism.

That is, if there exists another possible group $(M \otimes_R N)'$ then the isomorphism between the two groups is unique.

An element of $M \otimes_R N$ looks like $\sum_{i=1}^{n} m_i \otimes n_i$ where $m_i \in M$, $n_i \in N$. We say $m \otimes n$ is a pure tensor in $M \otimes_R N$. For any $m \in M$ and $n \in N$, $m \otimes 0 = 0 \otimes n = \mathbf{0}$.

Note: If R is commutative and M and N are R-modules, then $M \otimes_R N$ is an R-module with $r \cdot (m \otimes n) = mr \otimes n = m \otimes rn$.

72 (tensor product examples) **ex 1.** If T is a torsion abelian group (i.e. every element of T has finite order) then $\mathbb{Q} \otimes_{\mathbb{Z}} T = \{0\}$

ex 2. If D is a divisible abelian group and T is a torsion abelian group then $D \otimes_{\mathbb{Z}} T = \{0\}$.

ex 3. $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/t\mathbb{Z}$ where $t = \gcd(m, n)$

Ex 4. For a general R and left R-module N, $R \otimes_R N \cong N$ (isomorphic as R-modules). Similarly, $M \otimes_R R \cong M$.

Proposition: Given (S, R)-bimodule M and a left R-module N, then the tensor product $M \otimes_R N$ is also a left S-module with $s(m \otimes n) = (sm) \otimes n$.

Proposition: Let R be a commutative ring. Then $R^m \otimes_R R^n \cong R^{mn}$ as left R-modules.

Proposition: $\left(\bigoplus_{i \in I} M_i\right) \otimes_R N \cong \bigoplus_{i \in I} M_i \otimes_R N$.

73 **($F_M :_R \mathcal{M} \to \mathbf{Ab}$)** Given a right R-module M, there is a covariant additive functor

$$F_M :_R \mathcal{M} \to \text{Ab}$$

such that

$$F_M(N) = M \otimes_R N \qquad F_M(\phi) = \text{id}_M \otimes \phi$$

where $\phi : N \to N'$ is a homomorphism of left R-modules.

Theorem: Given

$$\begin{aligned} f &: M \to M' && \text{right } R\text{-modules} \\ g &: N \to N' && \text{left } R\text{-modules} \end{aligned}$$

Then there exists a unique homomorphism of abelain groups

$$f \otimes g : M \otimes_R N \to M' \otimes_R N'$$

such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. If R is commutative, then $f \otimes g$ is an R-module homomorphism.

Corollary: If $f_1 : M' \to M''$ and $g_1 : N' \to N''$ then $(f_1 \otimes g_1) \circ (f \otimes g) = (f_1 \circ f) \otimes (g_1 \circ g)$.

Corollary: If f, g are isomorphisms, then $f \otimes g$ is an isomorphism.

74 **((S, R)-bimodule)** Let R and S be rings and let M be an abelian group. Then M is (S, R)-bimodule (denoted ${}_SM_R$) if M is a left S-module and a right R-module and if

$$s(mr) = (sm)r \qquad \forall s \in S, r \in R, m \in M$$

6 Invariant Dimension Property

75 (invariant dimension property) A ring R has the invariant dimension property if for any free R-module F, any two bases of F have the same cardinality.

Theorem: If R is commutative, then R satisfies the invariant dimension property.

Proposition: There exists rings R such that $\exists m \neq n$ with $R^m \cong R^n$ as left R-modules.

76 (flat) We say that M is flat if $M \otimes_R -$ is exact.

Proposition: Let R be a ring

1. As a $(\mathbb{Z}, R)$-bimodule, R is a flat module
2. Let $\{M_i\}$ be (S, R)-bimodules. Then $\oplus_i M_i$ is flat $\Leftrightarrow$ each M_i is flat
3. If M is an (S, R)-bimodule and is projective as a right R-module then M is flat

77 (Noetherian) Let R be a ring and M be a left R-module. We say M is Noetherian if it satisfies one of the following equivalent conditions:

1. every submodule of M is finitely generated
2. ascending chain condition

   i.e. every ascending sequence $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ of submodules of M stabilizes (that is, there exists some N such that $\forall n \geq N$, $M_n = M_N$)
3. every non-empty subset of submodules of M contains a maximal element with respect to inclusion

A ring R is a Noetherian ring if it is Noetherian as a left R-module

Proposition: Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence of left R-modules. Then M is Noetherian $\Leftrightarrow$ M' and M'' are Noetherian.

Corollary: In particular, submodules, quotient modules, and direct sums of Noetherian modules are Noetherian.

Proposition: Let R be a Noetherian ring. Then every finitely generated left R-module is Noetherian.

78 (Hilbert's Basis Theorem:) If R is a commutative Noetherian ring, then $R[x]$ is Noetherian.

7 Modules over a PID

79 (torsion-free) Let R be a PID, M an R-module, $M_{\text{tors}} = \{m \in M \mid \exists 0 \neq a \in R \text{ such that } am = 0\} \subseteq M$ is a submodule. If $M_{\text{tors}} = \{0\}$ then M is torsion-free.

Lemma: M/M_{tors} is always torsion-free.

Theorem 1: Over a PID, torsion free and finitely generated $\Rightarrow$ free and finitely generated.

Theorem 2: Let R be a PID and M a finitely generated R-module. Then

1. M/M_{tors} is free and finitely generated
2. $\exists F \subseteq M$ submodule that is free and finitely generated so that $M = M_{\text{tors}} \oplus F$
3. $\text{rank}_R(F) = \text{rank}_R(M/M_{\text{tors}}) < \infty$

We say M is torsion if $M_{\text{tors}} = M$.

80 (Elementary Divisors Theorem) Let R be a PID. Let F be a free finitely generated R-module. Let $0 \neq E \subseteq F$ be a submodule. Then there exists a basis $z_1, \ldots, z_n$ of F and elements $\lambda_1, \ldots, \lambda_t$ of R $(1 \leq t \leq n)$ such that

1. $\lambda_1 | \lambda_2$ and $\lambda_2 | \lambda_3$ and etc... $\lambda_i \neq 0$
2. $\lambda_1 z_1, \ldots, \lambda_t z_t$ is a basis for E
3. $F/E \cong R/(\lambda_1 R) \oplus R/(\lambda_2 R) \oplus \cdots \oplus R/(\lambda_t R) \oplus \underbrace{R \oplus \cdots \oplus R}_{r=n-t \text{ times}}$

Moreover, $\lambda_1, \ldots, \lambda_t$ are unique up to units in R^x and r is uniquely determined by F/E.

$$0 \to E i \Rightarrow F \to M \to 0 \qquad n = \text{rank}_R(F),\ t = \text{rank}_R(E),\ r = n - t$$

where E is free + finitely generated, F is free + finitely generated, M is finitely generated.

81 ($K[x]$) Let K be a field. Then $K[x]$ is the polynomial ring in x with coefficients in K.

We know that $K[x]$ is a PID, UFD and a Euclidean Domain.

For $f, g \in K[x]$, then $\deg(fg) \leq \deg(f) + \deg(g)$, and $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

Division algorithm: Let $f, g \in K[x]$ with $\deg(f), \deg(g) \geq 0$. Then there exists unique polynomials $q, r \in K[x]$ so that $f = gq + r$ and $\deg(r) < \deg(g)$.

Corollary: Let $f \in K[x]$, $\deg(f) = n \geq 0$. Then

1. f has at most n roots in K
2. If $c \in K$ is a root of f then $(x - c)$ divides f in $K[x]$.

82 (extension) If $K \subseteq L$ are fields, we say that L is an extension of K and write L/K is an extension of fields.

Given fields L/K and $\alpha \in L$, we say that α is algebraic over K if there exists some non-zero polynomial $f \in K[x]$ with $f(\alpha) = 0$. Otherwise, α is transcendental over K.

If every $\alpha \in L$ is algebraic over K then we say L/K is an algebraic extension.

Given an extension L/K of fields, L is a K-vector space. We set $[L : K] = \dim_K(L)$ to be the degree of L over K. If $[L : K] = n < \infty$ then L/K is a finite extension, otherwise, it's an infinite extension.

Given $\alpha_1, \ldots, \alpha_m \in L$, then $K(\alpha_1, \ldots, \alpha_m)$ is the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_m$.

Lemma: Let L/K be a field extension and let $\alpha \in L$. Define a ring homomorphism

$$\begin{aligned} \rho : K[x] &\to L \\ f &\mapsto f(\alpha) \end{aligned}$$

Then

1. α is algebraic over $K \Leftrightarrow \ker(\rho) \neq \{0\}$

   α is transcendental over $K \Leftrightarrow \ker(\rho) = \{0\}$
2. If α is algebraic over K then $\mathrm{Im}(\rho) = K(\alpha)$ is the smallest subfield of L containing K and α

   If α is transendental over K, then $\mathrm{Im}(\rho) = K[\alpha]$ and is isomorphic to a polynomial ring over K

83 (quotient by function) Let K be a field and $0 \neq f \in K[x]$. Then $K[x]/(f)$ is a K-vector space (since it's a K-module) and $\dim_K(K[x]/(f)) = \deg f$. And

$$K[x]/(f) \cong \{c_0 + c_1 x + \cdots + c_{d-1}x^{d-1}(\mod f) \mid c_i \in K\}$$

84 (irreducible polynomial of an algebraic element) Given L/K a field extension and $\alpha \in L$ algebraic over K,

$$\begin{aligned} \rho : K[x] &\to L \\ g &\mapsto g(\alpha) \end{aligned}$$

is a K-algebra homomorphism (a homomorphism of rings that's also a linear transformation) and $\mathrm{Im}(\rho) = K(\alpha)$.

We define $\mathrm{Irr}(\alpha, K, x)$ to be the unique monic polynomial in $K[x]$ of least degree having α as a root.

Proposition: Let L/K be fields and let $\alpha \in L$ be algebraic over K. Let $\varphi = \mathrm{Irr}(\alpha, K, x)$. Then $K(\alpha) \cong K[x]/(\varphi)$. Moreover, $[K(\alpha) : K] = \dim_K(K(\alpha)) = \deg(\varphi) = \deg(\mathrm{Irr}(\alpha, K, x))$.

Corollary: If $\alpha \in L$ is algebraic over K then $[K(\alpha) : K] < \infty$. Moreover, $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ where $d = \deg(\mathrm{Irr}(\alpha, K, x))$ is a K-basis for $K(\alpha)$.

Proposition: Let L/K be a finite extension. Then L/K is algebraic.

Proposition: Let $H \subseteq K \subseteq L$ be fields. Then $[L : H] = [L : K][K : H]$.

Even stronger, if $\{x_i\}_{i \in I}$ is a basis for L/K and if $\{y_j\}_{j \in J}$ is a basis for K/H then $\{x_i y_j\}_{i \in I, j \in J}$ is a basis for L/H.

85 (compositum of fields) Let K, L be extensions of some field. If K and L are both subfields of some other field F then we define the compositum of K and L, KL, to be the smallest subfield of F that contains both K and L.

86 (prime field) Given a field K, there exists a unique ring homomorphism

$$\begin{aligned} \psi : \mathbb{Z} &\to K \\ 1 &\mapsto 1 \\ 2 &\mapsto 1 + 1 \end{aligned}$$

Then $\ker(\psi)$ is an ideal in $\mathbb{Z}$, so $\ker \psi = (0)$ or (p) for some prime p. If $\ker(\psi) = (0)$ then K contains a copy of $\mathbb{Q}$, so K has characteristic 0 and $\mathbb{Q}$ is the prime field of K since $\mathbb{Q}$ is contained in every subfield of K. If $\ker \psi = (p)$ then K has characteristic p and $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is the prime field of K

8 Distinguished Classes of Fields

87 (Great Theorem) Let K/L be a field extension. We say that K is finitely generated over L if $K = L(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$.

Proposition: Suppose all fields below are contained in the same larger field

1. Let $F \subseteq K \subseteq L$ be fields.
   Then L/F is finite $\Leftrightarrow$ L/K is finite and K/F is finite
2. Suppose K/F is finite and L/F is any extension. Then KL/L is finite
3. If K/F and L/F are finite, then KL/F is finite
4. Let $F \subseteq K \subseteq L$ be fields.
   Then L/F is algebraic $\Leftrightarrow$ L/K is algebraic and K/F is algebraic
5. Suppose K/F is algebraic and L/F is any extension. Then KL/L is algebraic
6. If K/F and L/F are algebraic, then KL/F is algebraic

88 (algebraically closed) A field F is algebraically closed if every polynomial in $F[x]$ has a root in F.

ex. $\mathbb{C}$ is algebraically closed.

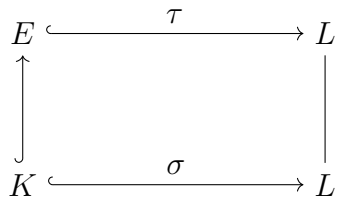
ex. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ = field of algebraic numbers. This is the smallest algebraically closed field in $\mathbb{C}$ containing $\mathbb{Q}$.

Theorem: Let K be a field. Then there is an algebraically closed field $\overline{K}$ which is also algebraic over K.

Proposition: Suppose $K \subseteq F \subseteq E$, where E is algebraically closed. Then $\overline{K} \subseteq \overline{F}$. Moreover, $\overline{K} = \overline{F}$ if and only if F is algebraic over K.

89 (embeddings) Let L and K be fields. A ring homomorphism $\sigma : K \hookrightarrow L$, $1 \mapsto 1$ is called an embedding.

Suppose E/K is an extension of fields. An embedding $\tau : E \hookrightarrow L$ extends σ if $\tau|_K = \sigma$



Special Case: If $K \subseteq L$ and $\sigma : K \hookrightarrow L$ is the inclusion map, then τ is called an embedding of E over K

$$\begin{array}{ccc} E & \xhookrightarrow{\tau} & L \\ | & & | \\ K & \xhookrightarrow{\mathrm{id}_K} & L \end{array}$$

Key Fact: Suppose $K \subseteq E \subset L$ are fields and say $f \in K[x]$ has a root $\alpha \in E$. Then for any embedding $\tau : E \hookrightarrow L$ over K (i.e. embedding that fixes K), the element $\tau(\alpha) \in \tau(E) \subseteq L$ is also a root of f.

Fix an embedding $\sigma : K \hookrightarrow L$ where K is a field and L is algebraically closed. Suppose E/K is algebraic. Define $\mathrm{Emb}(E/K, \sigma) = \{\tau : E \hookrightarrow L \mid \tau|_K = \sigma\}$.

If $K \subseteq L$ is a subfield, $\mathrm{id}_K : K \hookrightarrow L$ inclusion, then $\mathrm{Emb}(E/K) = \{\tau : E \hookrightarrow L \mid \tau|_K = \mathrm{id}_K\} = \mathrm{Emb}(E/K, \mathrm{id}_K\}$.

If $\sigma : K \hookrightarrow L$, let $K^\sigma = \sigma(K)$. For $f(x) \in K[x]$, we take $f^\sigma(x)$ to be $\sigma(a_m)x^m + \cdots = \sigma(a_1)x + \sigma(a_0)$. Then $\phi : K[x] \to L[x], f \mapsto f^\sigma$ is a ring homomorphism.

9 Splitting Field of a Polynomial

90 (splitting field of f) Let K be a field and let $\overline{K}/K$ be an algebraic closure of K. For a polynomial $f \in K[x]$, write $f = c(x - \alpha_1)\dots(x - \alpha_n)$ for $c \in K^x$, $\alpha_i \in \overline{K}$. The field $E = K(\alpha_1, \dots, \alpha_n)$ is called the splitting field of f over K.

Theorem: Let E be a splitting field of $f \in K[x]$.

1. If F is another splitting field (say in some other algebraically closed field containing K), then there exists an isomorphism $\sigma : F \to E$ such that $\sigma|_K = \mathrm{id}_K$
2. If $K \subseteq E \subseteq \overline{K}$, then any embedding $\sigma : E \hookrightarrow \overline{K}$ over K must have image E (i.e. $\sigma(E) = E$).

Proposition: Let F be a field and suppose $f(x) \in F[x]$. Then $f(x)$ has no repeated roots if and only if $\gcd(f(x), f'(x)) = 1$.

10 Embeddings

91 (nada!)

92 (Lifting Lemma) Let K be a field, $\sigma : K \hookrightarrow L$ embedding, L algebraically closed. Suppose E/K is algebraic. Then there exists an embedding $\tau : E \hookrightarrow L$ extending σ.

Corollary: Let K be a field. Then any two algebraic closures of K are isomorphic over K.

ex. Consider

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}, i) & \xrightarrow{\rho} & \mathbb{C} \\ | & & | \\ \mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\tau} & \mathbb{C} \\ | & \overset{\mathrm{id}_{\mathbb{Q}}}{} & | \\ \mathbb{Q} & \hookrightarrow & \mathbb{C} \end{array}$$

The options for τ are sending $\sqrt[4]{2}$ to one of $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$.. What ρ is depends on the choice of τ. Let ρ send $\sqrt[4]{2}$ to $\tau(\sqrt[4]{2})$ and then it may send i to either i or $-i$.

11 Splitting Fields

93 (freebee)

94 (normal extensions) We say E/K is a normal extension if it satisfies any of the following equivalent conditions

1. every embedding $\sigma : E \hookrightarrow \overline{K}$ over K induces an automorphism of E (i.e. $\sigma(E) = E$)
2. E is the splitting field over K of some set of polynomials in $K[x]$
3. every irreducible polynomial of $K[x]$ which has a root in E must split in E (i.e. all its roots are in E)

Theorem: Suppose E/K is normal.

1. If H/K is any extension, then EH/H is normal
2. If $E \supseteq F \supseteq K$ are fields, then E/F is normal (note: F/K need not be normal)
3. If E'/K is also normal, then EE'/K is normal

4. If F/K is algebraic, then there exists a normal extension E/K such that $F \subseteq E$.

95 (separable extensions) Let $\sigma : K \hookrightarrow L$, where L is algebraically closed. If E/K is algebraic, we set the separable degree of E/K to be $[E : K]_s = \#\operatorname{Emb}(E/K, \sigma)$.

Lemma: If K is a field and $\sigma : K \hookrightarrow L$ an embedding, L algebraically closed and E/K is algebraic, then $\#\operatorname{Emb}(E/K, \sigma)$ is independent of σ and L.

Theorem: If $E \supseteq F \supseteq K$ is a tower of algebraic extensions, then $[E : K]_s = [E : F]_s[F : K]_s$. If E/K is finite, then $[E : K]_s \leq [E : K]$.

If E/K is finite and $[E : K]_s = [E : K]$ then E/K is called a separable extension.

An element $\alpha \in E$ is separable over K if $K(\alpha)/K$ is separable (i.e. $[K(\alpha) : K]_s = [K(\alpha) : K]$)

Lemma: $K(\alpha)/K$ is separable $\Leftrightarrow \operatorname{Irr}(\alpha, K, x)$ has no repeated roots in $\overline{K} \Leftrightarrow \gcd(f(x), f'(x)) = 1$ where $f = \operatorname{Irr}(\alpha, K, x)$.

If every element of E is separable over K then we say E/K is a separable extension.

Theorem: The compositum of separable extensions is separable.

Proposition: Suppose $\operatorname{char}(K) = 0$. Then every irreducible polynomial in $K[x]$ is separable. In particular, every algebraic extension E/K is separable.

12 Inseparable Extensions

96 (inseparable) Suppose E/K is algebraic. Then TFAE:

1. E/K is inseparable
2. E/K is not separable
3. $\exists \alpha \in E$ that is not separable over K
4. $\exists \alpha \in E$ so that $\operatorname{Irr}(\alpha, K, x)$ has repeated roots

Propostion: Let K be a field of characteristic p. Let $\alpha \in \overline{K}$ and $f = \operatorname{Irr}(\alpha, K, x) \in K[x]$. Then there exists some $\mu \geq 0$ so that

1. every root of f in $\overline{K}$ has multiplicity p^μ
2. $[K(\alpha) : K] = p^\mu[K(\alpha) : K]_s$
3. α^{p^μ} is separable over K

If $\mu \geq 1$ then α is inseparable over K and $K(\alpha)/K$ is inseparable.

Corollary:

1. For any finite extension E/K, $[E:K]_s | [E:K]$
2. If $\text{char}(K) = 0$ then $[E:K]_s = [E:K]$
3. If $\text{char}(K) = p > 0$ then $[E:K]_i = \frac{[E:K]}{[E:K]_s}$ is a power of p (called the inseparable degree of E/K)

97 (perfect) A field K is perfect if every algebraic extension of K is separable.

Suppose $\text{char}(K) = p > 0$. Then the p^{th} power Frobenus map is $\phi : K \to K$, $x \mapsto x^p$ is a field embedding.

Proposition: Let K be a field of characteristic $p > 0$. Then K is perfect $\Leftrightarrow$ ϕ is an automorphism

98 (Galois group) If E/K is normal and separable, we say E/K is a Galois extension. If E/K is any extension, then

$$\text{Aut}(E/K) = \{\sigma : E \xrightarrow{\sim} E \text{ field automorphism } \mid \sigma|_K = \text{id}_K\}$$

If E/K is Galois, then we write $\text{Gal}(E/K) = \text{Aut}(E/K)$.

If $f \in K[x]$ is separable, then the Galois group of f over K is $\text{Gal}(E/K)$ where E is the splitting field of f over K.

Proposition 1: If E/K is finite and Galois, then $\text{Gal}(E/K) = \text{Emb}(E/K)$ and $|\text{Gal}(E/K)| = [E:K]$

Propositon 2: Suppose E/K is Galois and suppose $K \subseteq F \subseteq E$ where F is a field. Then E/F is Galois and $\text{Gal}(E/F) \leq \text{Gal}(E/K)$

Proposition 3: Let E/K be a finite, Galois group. If $E = K(\alpha)$ and $f = \text{Irr}(\alpha, K, x) \in K[x]$ then each element of $\text{Gal}(E/K)$ permutes the roots of f which induces a homomorphism $\text{Gal}(E/K) \hookrightarrow S_n$ where $n = \deg(f) = [E:K] = \#\,\text{Gal}(E/K)$.

99 (positive element theorem) If E/K is finite and separable, then $\exists \alpha \in E$ so that $E = K(\alpha)$.

100 (Fundamental Theorem of Galois Theory) Let E/K be an extension and $H \subseteq \text{Aut}(E/K)$ a subgroup. Define $E^H := \{\alpha \in E \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}$ to be the fixed field, so $K \subseteq E^H \subseteq E$.

Let E/K be a finite Galois extension and let $G = \mathrm{Gal}(E/K)$. Then there is an inclusion reversing bijection

$$\begin{array}{rcr} \text{intermediate fields} & \leftrightarrow & \text{subgroups of } G \\ E^H & \leftarrow & H \\ F & \mapsto & \mathrm{Gal}(E/F) \end{array}$$

Given an intermediate field $K \subseteq F \subseteq E$, F/K is Galois $\Leftrightarrow \mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/K)$. In this case, the map $\mathrm{Gal}(E/K) \to \mathrm{Gal}(E/K)$, $\sigma \mapsto \sigma|_F$ yields

$$\mathrm{Gal}(F/K) \cong \frac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/K)}$$