Intro Group Theory Cheat Sheet

Group Axioms

A group is an ordered pair (G, *) where G is a set and * is a binary operation on G satisfying the following axioms:
i. Closure: $\forall$ a, b $\in$ G, a * b, is also in G
ii. Associativity: (a * b) * c = a * (b * c), $\forall$ a, b, c $\in$ G
iii. Identity: $\exists$ e $\in$ G, called an identity of G, s.t. $\forall$ a $\in$ G we have a * e = e * a = a
iv. Inverse $\forall$ a $\in$ G $\exists$ a^{-1} $\in$ G, called an inverse of a, s.t. a * a^{-1} = a^{-1} * a = e.

Some Properties of Groups

i. Abelian group A group G is abelian if a * b = b * a $\forall$ a, b $\in$ G
ii. Finite group A group G is finite if the number of elements in G are finite
iii. Cancellation property suppose that a * b = a * c, $\forall$ a, b, c $\in$ G, $\Rightarrow$ b = c
iv. Uniqueness of Inverse and Identity
- The identity of G is unique
- $\forall$ a $\in$ G, a^{-1} is uniquely determined
- $(a^{-1})^{-1}$ = a $\forall$ a $\in$ G
- $(a * b)^{-1} = (b^{-1}) * (a^{-1})$
- for any $a_1, a_2, ..., a_n \in$ G the value of $a_1 * a_2 * * a_n$ is independent of how the expression is bracketed

Some Special Groups

i. Dihedral Group (D_n or D_{2n}) is a group of symmetries of a n-sided regular polygon. Order = 2n
ii. Symmetric Group (S_n) is the group whose elements are all the bijections from the set to itself.
Order = n!
iii. Klein-4 Group (K_4 or V) is a group with 4 elements in which each element is a self inverse.

Homomorphisms and Isomorphisms

i. Homomorphisms
Let (G , *) and (H, $\circ$) be groups.
A map $\varphi : G \to H,\ s.t.\ \varphi(x * y) = \varphi(x) \circ \varphi(y)\ \forall\, x, y \in G$ is called a **homomorphism.**
ii. Isomorphism
For φ : G $\to$ H is called an **isomorphism** if:
i. φ is a homomorphism
ii. φ is a bijection

Group Actions

A **group action** of a group G on a set A is a map from G $\times$ A to A satisfying the following properties
i. Identity: $e \cdot x = x$ and,
ii. Compatibility: $g \cdot (h \cdot x) = (gh) \cdot x$

Subgroups

For a Group G. The subset H of G, is a **Subgroup** of G, i.e. H $\leq$ G if
i. H is non-empty
ii. H is closed under products and inverses
- **A Normal subgroup** N of G, (i.e. $N \trianglelefteq G$) iff $gng^{-1} \in N\ \forall\, g \in G$ and $n \in N$.

The Subgroup Criterion
A subset H of group G is a subgroup of G iff
i. H $\neq \emptyset$
ii. $\forall\, x,\ y \in H\ xy^{-1} \in H$

Centralizers, Normalizers, Stabilizers and Kernels

- **Centralizer** of A in G is a subset of G defined as $C_G(A) = \{g \in G \mid gag^{-1} = a\ \forall\, a \in A\}$,
it is the set of all elements of G which commute with every element of A.
- **Center** of G is the subset of G defined as
$Z(G) = \{g \in G \mid gx = xg\ \forall\, x \in G\}$,
it is the set of elements commuting with all the elements of G. Note, this is case $Z(G) = C_G(G)$ so $Z(G) \leq G$.
- **Normalizer** of A in G is defined as the set
$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ where,
$gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Note that $C_G(A) \leq N_G(A)$.
- **Stabilizer** on a set S with element s in G is defined as the set
$G_s = \{g \in G \mid g \cdot s = s\}$. Note that $G_S \leq G$.
- **Kernel** of G on S is defined as the set
$Ker(f) = \{g \in G \mid g \cdot s = s\ \forall\, s \in S\}$

Cyclic Groups and Cycle Notation

A Group H is **Cyclic** if $\exists\, x \in H$ s.t. $H = \{x^n \mid n \in \boldsymbol{Z}\}$
For the above case we say $H\ \langle x \rangle$ and that H is generated by x.
- A cyclic group can have more than one generator.
- All cyclic groups are abelian.
- If $H = \langle x \rangle$ then $|H| = |x|$, if $|H| = n < \infty$ then $x^n = 1$
- Any two cyclic groups of the same order are isomorphic.

Two-Line to Cycle notation for permutations
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (125)(34) = (34)(125) = (34)(512) = (15)(25)(34)$$
Here, the last form is a case of 2-cycle (transposition).

Cosets and Quotient Groups

For any $N \leq G$ and any $g \in G$
- $gN = \{gn \mid n \in N\} = \{g, gh_1, gh_2 \ldots\}$ and,
- $Ng = \{ng \mid n \in N\} = \{g, h_1g, h_2g \ldots\}$ are called a left coset and a right coset respectively.

For a Group G and $N \trianglelefteq G$, the **quotient group** of N in G (i.e. G/N), is the set of cosets of N in G.

Lagrange's Theorem and some results

Lagrange's Theorem: For a finite group G and $H \leq G$,
- The order of H divides the order of G, and,
- The number of left cosets of H in G equals $\frac{|G|}{|H|}$

Some important results
- If G is a finite group and $x \in G$, then the order of x divides the order of G, and $x^{|G|} = e\ \forall\, x \in G$
- If G is a group of prime order, then G is cyclic

Cauchy's Theorem

Cauchy's Theorem: If G is a finite group and p is a prime dividing $|G|$ then G has an element of order p.

The Isomorphism Theorems

i. The First Isomorphism Theorem:
If $\varphi : G \to$ H is a homomorphism of groups. Then $ker\ \varphi \trianglelefteq G$ and, $G/ker\varphi \cong \varphi(G)$.
ii. The Second Isomoprhism Theorem:
For a group G with, $A, B \leq G$ and, $A \trianglelefteq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and, $AB/B \cong A/A \cap B$
iii. The Third Isomophism Theorem:
For a group G with, $H, K \trianglelefteq G$ and, $H \leq K$. Then $K/H \trianglelefteq G/H$ and, $\frac{G/H}{K/H} \cong G/K$

Parity of Permutations and Alternating Groups

The parity of any permutation σ is given by the parity of the number of its 2-cycles (transpositions).

Alternating Groups:
An alternating group is the group of even permutations of a finite set of length n. It is denoted by A_n it's order is $\frac{n!}{2}$

Equivalence Classes and Orbits

- If G is a group acting on the non-empty set A. Then $a \sim b \iff a = g \cdot b$ for some $g \in G$. Where $\sim$ is an equivalence relation.
- The **orbit** of G containing a is given as $\mathcal{O}_a = \{g \cdot a \mid g \in G\}$
- The action of G on A is called transitive if there is only one orbit.
- **Conjugacy classes** of G is the equivalence classes of G when it acts on itself with conjugation. i.e. $gag^{-1} \mid g \in G$

Class equations and Orbit-stabilizer Theorem

Class equation of a finite group G is written as:
$|G| = |Z(G)| + |\sum$(Conjugancy classes of G)$|$
Oribit-stabilizer Theorem:
For a group G acting on a set S, for any $s \in S$ we have, $|\mathcal{O}_s||G_s| = |G|$

Cayley's Theorem

Cayley's Theorem:
Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomoprhic to a subgroup of S_n

Automorphisms

Automorphism of G is defined as an isomorphism from G onto itself.
The set of all automorphisms of G is denoted by Aut(G)

p-groups and Sylow p-groups

- **p-group** is defined as a group of order p^a for some $a \geq 1$. Sub-groups of G which are p-groups are called p-subgroups.
- **Sylow p-group** is defined as a group of order $p^a m$, where $p \nmid m$, a subgroup of order p^a is called a Sylow p-subgroup of G. $Syl_p(G)$ is the set of Sylow p-subgroups of G.

The Sylow Theorems

i. The First Sylow Theorem:
If p divides $|G|$, then G has a Sylow p-subgroup.
ii. The Second Sylow Theorem:
All Sylow p-subgroups of G are conjugate to each other for a fixed p.
iii. The Third Sylow Theorem:
$n_p \equiv 1 (\text{mod } p)$, where n_p is the number of Sylow p-subgroups of G.

Intro Ring and Field Theory Cheat Sheet

Ring and Field Axioms

A ring R is a set with two binary operations $+$ and $\times$ satisfying the following axioms:
i. $(R, +)$ is an abelian group.
ii. Multiplicative associativity: $(a \times b) \times c = a \times (b \times c)\ \forall a, b, c \in R$.
iii. Left and right distributivity:
$(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$.
In addition to these rings may also have the following optional properties.
a. Multiplicative commutativity: $a \times b = b \times a,\ \forall\, a, b \in R$.
b. Multiplicative Identity: $\exists\, 1 \in R$ s.t. $\forall a \neq 0 \in R, 1 \times a = a \times 1 = a$.
c. Multiplicative Inverse: $\forall\, a \neq 0 \in R\ \exists\, a^{-1} \in R$ s.t. $a \times a^{-1} = a^{-1} \times a = 1$.
FOR THE PURPOSE OF THIS SHEET WE LOOK AT RINGS WITH MULTIPLICATIVE COMMUTATIVITY AND 1≠0.
A field F is a set with two binary operations $+$ and $\times$ satisfying the following axioms:
i. $(F, +)$ is an abelian group with identity 0.
ii. The non-zero elements of F form a abelian group under multiplication with identity 1.
iii. Left and right distributivity.

Polynomial Rings

For a ring R, $R[x]$ denotes the polynomial ring of a single variable x s.t.the elements of $R[x]$ are of the form
$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and $a_i \in R$
Polynomial rings can be generalized for multiple variables.

Zero Divisors, Units and Integral Domains

i. Zero Divisor: $a \neq 0 \in R$ is called a zero divisor of R if $\exists\, b \neq 0 \in R$ s.t. either $ab = 0$ or $ba = 0$.
ii. Unit: For a ring R with identity $1 \neq 0$, $u \in R$ is called a unit in R if $\exists v \in R$ s.t. $uv = vu = 1$.
iii. Integral Domain: A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.

- Any finite integral domain is a field.
- If R is an integral domain than the polynomial ring of one variable over R, i.e. $R[x]$, is also a integral domain.

Subrings

A subring of the ring R is defined as a subgroup of R that is closed under multiplication.

Ring Homomorphisms, Isomorphisms and Kernels

For rings R and S.
i. Ring Homomorphism is a map $\varphi : R \to S$ satisfying:

- $\varphi(a + b) = \varphi(a) + \varphi(b)\ \forall\, a, b \in R$
- $\varphi(ab) = \varphi(a)\varphi(b)\ \forall\, a, b \in R$

ii. Isomorphism is a bijective ring homomorphism.
iii. Kernel of the ring homomorphism φ is the set of elements of R that map to 0 in S.

- The image of φ is a subring of S.
- The kernel of φ is a subring of S. *(For Rings without 1)*

Ideals

Ideal: A subset I of ring R is called an ideal of R if

- It is a subring of R.
- It is closed under both left and right multiplication with elements from R.

Ideals are to rings what normal subgroups are to groups.

Quotient Rings

Let R be a ring with ideal I. R/I is called a quotient ring if
i. $(r + I) + (s + I) = (r + s) + I$
ii. $(r + I) \times (s + I) = (rs) + I$

First Isomorphism and Correspondence Theorem

i. First Isomorphism Theorem: Let $\varphi : R \to S$ be a ring homomorphism from ring R to S then:

- Kernel of φ is an ideal of R,
- Image of φ is a subring of S and,
- $R/\ker\varphi \cong \varphi(R)$.

ii. Correspondence Theorem: Let R be a ring, and I be an ideal of R.
The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I.
or
There exists an inclusion preserving biijection between ideals in R containing $\ker(\varphi)$ and ideals in $\varphi(R)$.

Principal, Prime and Maximal Ideals

i. Principal Ideals: An ideal generated by a single element is called a principal ideal.
ii. Prime Ideals: If $P \neq R$, then an ideal P is called a prime ideal if $ab \in P$, when $a, b \in R$ then at least one of a and b in an element of P. *This is analogous to the definition of prime numbers in number theory*
iii. Maximal Ideals: If $M \neq R$, then an ideal M is called a maximal ideal if the only ideals containing M are M and R itself.
• *Every maximal ideal of R is a prime ideal.*
• *The ideal P is a prime ideal in R iff R/P is an integral domain.*

Zorn's Lemma

If S is any nonempty partially ordered set in which every chain has an upper bound, then S has a maximal element.

Ring of Fractions of an Integral Domain

Let R be an integral domain. Let K be the ring of fractions of R s.t. $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$. K is also called a field of fractions since it always forms a field for any ring R.

- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, b, d \neq 0$
- $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, b, d \neq 0$

Chinese Remainder Theorem

The ideals I and J of a ring R are said to be **comaximal** if $I + J = R$.
Chinese Remainder Theorem: $\forall\, a, b \in R$, $\exists\, x \in R$ s.t. $x \equiv a (\mathrm{mod}\ I)$ and $x \equiv b (\mathrm{mod}\ J)$

Noetherian Rings

A commutative ring R is called **Noetherian** if there is no infinite increasing chain of ideals in R, i.e. when $I_1 \subseteq I_2 \subseteq I_3 \ldots$ is an ascending chain of ideals $\exists\, k \in \mathbb{Z}^+$ s.t. $I_k = I_m\ \forall k \geq m$.
It is equivalent to say that R is Noetherian if every ideal of R is finitely generated.

Hilbert Basis Theorem

If R is a noetherian ring then so is the polynomial ring $R[x]$.
$R[x_1, x_2, x_3, \ldots, x_n]$ for finite n is also noetherian.

Irreducible and Prime Elements

i. Irreducible Element An element a of ring R is called **irreducible** if it is non-zero, not a unit and, *only has trivial divisors (i.e. units and products of units).*
ii. Prime Element An element a of ring R is called **prime** if it is non-zero, not a unit and, if $a \mid bc$ then either $a \mid b$ or $a \mid c$ for some $b, c \in R$.
The concept of primes and irreducible is the same in integers, but they are distinct in general.
In an integral domain, every prime element is irreducible, but the converse holds only in UFDs.

Norm and Euclidean Domain

i. Norm: For a integral domain R, any function $N : R \to \mathbb{Z}^+ \cup 0$ with $N(0) = 0$ is called a *norm* on R.
ii. Euclidean Domain: An integral domain R is called an **Euclidean Domain** if there is a norm N on R s.t. for any two elements $a, b \in R$, where $b \neq 0\ \exists\, q, r \in R$ s.t. $\mathbf{a = qb + r}$ **where** $\mathbf{r = 0}$ **or** $\mathbf{N(r) < N(b)}$.
• Any field F is a trivial example of a Euclidean Domain.

Principal Ideal Domains (PIDs)

A **Principal Ideal Domain (PID)** is an integral domain in which every ideal is principal.
Every Euclidean Domain is a PID.
Examples:
•$\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not.
•$F[x]$ if F is a field, •$Z[i]$

Unique Factorisation Domains (UFDs)

Two elements $a, b \in R$ are said to be **associates** in R if they differ by a unit, i.e. $a = ub$ for some unit $u \in R$. A **Unique Factorisation Domain (UFD)** is an integral domain R in which every nonzero element $r \in R$ which is not a unit follows the properties:
i. r can we written as a finite product of irreducibles p_i of R.
ii. This decomposition is unique up to associates, i.e. if $r = p_1 p_2 \ldots p_n$ and $r = q_1 q_2 \ldots q_n$ then $m = n$ and for some renumbering of factors there is p_i associate to q_i
The above definition can be equivalently stated as:
A UID is any integral domain in which every non-zero, non-invertible element has a unique factorisation.
•Every PID is a UID.
• $Z[x]$ is a UID, but not a PID.
•In a UID every non-zero element is a prime iff it is irreducible.
• Fields $\subset$ Euclidean Domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains.

Primitive Polynomials and Gauss' Lemma

A polynomial $f(x) \in \mathbb{Z}[x]$ is called **primitive** if $n = deg(f) > 0$, $a_n > 0$ and, $gcd(a_0, a_1, \dots, a_n) = 1$ for $a_i \in \mathbb{Z}$

Gauss' Lemma: If $f(x), g(x) \in \mathbb{Z}$ are primitive $\implies fg$ is also primitive.

Eisenstein's Criterion

The Eisenstein's Criterion is a test for irreducibility of polynomials.

Let P be a prime ideal of the integral domain R amd, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$.

Eisenstein's Criterion states that $f(x)$ is irreducible in R[x] if

• $a_{n-1}, \dots a_1, a_0$ are elements of P and,

• a_0 is **not** an element of P^2.

If Eisenstein's Criterion doesn't directly apply to f(x) try on f(x+1), if f(x+1) is irreducible it implies f(x) is also irreducible.

Characteristics of Fields

Let 1_F denote the identity of F.

The **characteristic** of a field F, denoted as $ch(F)$ is defined as the smallest integer p such that $p \cdot 1_f = 0$ if such a p exists and is defined as 0 otherwise.

• $ch(F)$ is either 0 or a prime p, • $\mathbb{Q}$ and $\mathbb{R}$ have characteristic 0

• $F_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p,

Field Extensions and Degree

If K is a field containing the subfield F, then K is said to be an **extension field** of F. It is denoted as K/F.

The **degree** of a field extension K/F denoted by $[K : F]$ is the dimension of K as a vector space over F.

Irreducible Polynomials in Fields

• For a irreducible polynomial $p(x) \in F$, there exists a field K containing a isomorphic copy of F in which $p(x)$ has a root, i.e. there exists a field extension K of F in which $p(x)$ has a root. A simple way to find this extension is to consider the quotient $K = F[x]/(p(x))$.

• For the above case, let $\theta = x \mod (p(x)) \in K$. Then the elements $1, \theta, \theta^2 \dots \theta^{n-1}$ are a basis for K as a vector space over F, with $[K : F] = n$.

• For the above case, let α be the root of $p(x)$ s.t. $p(\alpha) = 0$. Then, $F(\alpha) \cong F[x]/(p(x))$.

Algebraic and Transcendental Elements

i. Algebraic Element: If K is a field extension over F, then $\alpha \in K$ is called **algebraic** over F, if there exists some non-zero polynomial $f(x)$ with coefficients, in F, s.t. $f(\alpha) = 0$.

ii. Transcendental Element: Elements $\alpha \in K$ which are not algebraic over F are called **transcendental**.

• If α is algebraic over F, then $F[\alpha] = F(\alpha)$, if α is transcendental over F, then $F[\alpha] \neq F(\alpha)$.

Algebraic Extensions

• Let α be algebraic over F. There there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root.

• If L/F is an extension of fields and α is algebraic over both F and L then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

• If $F(\alpha)$ is the field generated by α over F then, $F(\alpha) \cong F[x]/(m_\alpha(x))$.

• Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$ • Similarly, $[K : F]$ divides $[L : F]$.

• Let K_1, K_2 be two finite extensions of field F contained in K. Then, $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$, but if $[K_1 : F] = n, [K_2 : F] = m$ and if gcd $(m, n) = 1$. Then, $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

Splitting Fields

Splitting Fields: The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ but not over any proper subfield of K containing F.

• For any field F, if $f(x) \in F[x]$. Then, there exists an extension K of F which is a splitting field for $f(x)$.

• A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

• Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic. • The polynomial $x^n - 1$ over $\mathbb{Q}$ has in general a splitting field contained in $\mathbb{C}$.

• Let $\mathbb{Q}(\zeta_n)$ be the cyclotomic field of n^{th} roots of unity. $[\mathbb{Q}\zeta_n : \mathbb{Q}] = \varphi(n)$ where $\varphi(n)$ is Euler's totient function.

Algebraic Closure of Fields

• The field $\bar{F}$ is called an **algebraic closure** of F if $\bar{F}$ is algebraic over F and, if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$.

• A field K is said to be **algebraically closed** if every polynomial with coefficients in K has a root n K. $\bar{F}$ as defined above is algebraically closed.

• For every field F there exists an algebraically closed field K containing F.

Fundamental Theorem of Algebra

The field $\mathbb{C}$ is algebraically closed.

Finite Fields

• For every prime $p \in \mathbb{N}$ there exists a field $\mathbb{F}_p$ of order p, e.g.$\mathbb{Z}/p\mathbb{Z}$.

• For any finite field F, the order of F is $q = p^r$ for some prime p and positive integer r.

Structure Theorem for Finite Fields

Let p be a prime integer and let $q = p^r$ for some positive integer r. Then the following statements hold.

- There exists a field of order q.
- Any two fields of order q are isomorphic.
- Let K be a field of order q. The multiplicative group K^x of non-zero elements of K is a cyclic group of order $q - 1$.
- Let K be a field of order q. The elements of K are the roots of $x^q - x \in \mathbb{F}_p[x]$.
- A field of order p^r contains a field of order $p^k \iff k|r$
- The irreducible factors of $x^q - x$ over $\mathbb{F}$ are the irreducible polynomials in $\mathbb{F}[x]$ whose degree divides r.

Introductory Galois Theory Cheat Sheet

Definition of a Field

A field F is a set with two binary operators $(+, \times)$ satisfying the following axioms,

- (F,+) is an abelian group with identity 0.
- The non zero elements of F form an abelian group under multiplication with identity $1 \neq 0$.
- Left and right distributivity

Characteristic of Fields

A characteristic of a field F, denoted by $\mathrm{ch}(F)$ is defined as is the smallest integer p such that $\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0$. If such a p does not, exist $\mathrm{ch}(F) = 0$.

K-algebra

A K-algebra (or algebra over a field) is a ring A which is a module over field K with multiplication being K-bilinear, (i.e., $k_1a_1 \cdot k_2a_2 = k_1k_2a_1a_2$).

Field Extensions

For fields K, L. We say L is a field extension of K if K is a subfield of L. Alternatively, L is a field extension of K, if L is a K-algebra.

Algebraic elements and Algebraic extensions

For a field extension $K \subset L$.
Algebraic element: $\alpha \in L$ is called algebraic if $\exists P \not\equiv 0 \in K[x]$ s.t. $P(\alpha) = 0$.
Transcendental element: If such a P does not exist then α is transcendental.
Consider the following definitions,

- Denote the smallest subfield of L containing K and α to be $K(\alpha)$.
- Denote the smallest sub ring of L containing K and α to be $K[\alpha]$.

The following statements are equivalent,

- α is algebraic over K.
- $K[\alpha]$ is finite dimensional algebra over K.
- $K[\alpha] = K(\alpha)$.

Algebraic extension: L is called algebraic over K if all $\alpha \in L$ are algebraic over K.

- If L is algebraic over K then any K-subalgebra of L is a field.
- Consider $K \subset L \subset M$. If $\alpha \in M$ is algebraic over K, then it is algebraic over L, also its minimal polynomial over L divides its minimal polynomial over K.
- If $K \subset L \subset M$ then M is an algebraic extension over $K \iff M$ is algebraic over L and L is algebraic over K.

Algebraic closure of L **over** K**:** A subfield L' of L s.t. $L' = \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$

Minimal Polynomial

If α is an algebraic element then $\exists!$ monic polynomial P of minimal degree such that $P(\alpha) = 0$ such a polynomial is called the **minimal polynomial**.

- The minimal polynomial is irreducible
- Any other polynomial Q s.t. $Q(\alpha) = 0$ will be divisible by P.

Pritmitive polynomials and Gauss' lemma

Primitive polynomial: A polynomial $P \in \mathbb{Z}[X]$ is called primitive if if has a positive degree and the gcd of its coefficients is 1.
Gauss' lemma: A non-constant polynomial $P \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}[X] \iff$ it is primitive and irreducible over $\mathbb{Q}[x]$

Eisenstein criterion for irreducibility

A polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is irreducible if $\exists p$ prime s.t. p divides all coefficients except a_n and p^2 does not divide a_0.

Finite extensions

For a field extension $K \subset L$. L is called a **finite extension** of K if the vector space of L over K has a finite dimension.
Degree of finite extension: Denoted as $[L : K] = \dim_K L$

- $K \subset L \subset M$. Then M is finite over $K \iff M$ is finite over L and L is finite over K. Also in this case, $[M : K] = [M : L][L : K]$.
- Let $K(\alpha_1, \ldots, \alpha_n) \subset L$ denote the smallest subfield of L containing K and $\alpha_i \in L$. This $K(\alpha_1, \ldots, \alpha_n)$ is generated by $\alpha_1, \ldots, \alpha_n$.
- L is finite over $K \iff L$ is generated by a finite number of algebraic elements over K .
- $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$

Stem field

Let $P \in K[X]$ be an irreducible monic polynomial. A field extension E is called a **stem field** of P if $\exists \alpha \in E$, s.t. α is a root of P and $E = K[\alpha]$

- If E, E' are two stem fields for $P \in K[x]$, s.t. $E = K[\alpha], E' = K[\alpha']$ where α, α' are roots of P. Then $\exists!$ isomorphism $E \cong E'$ of K-algebras which maps α to α'.
- If a stem field contains two roots of P, then $\exists!$ automorphism that maps one root to another.
- If E is a stem field, $[E : K] = \deg P$
- If $[E : K] = \deg P$ and E contains a root of P then E is a stem field.

Some irreducibility criteria,

- $P \in K[X]$ is irreducible over $K \iff$ it does not have roots in L/K of degree $\leq \deg P/2$.
- $P \in K[X]$ is irreducible over K with $\deg P = n$. If L/K with $[L : K] = m$ if $\gcd(m, n) = 1$ then P is irreducible over L.

Splitting field

Let $P \in K[X]$. The **splitting field** of P over K is an extension of L where P is split into linear factors and the roots of P generate L (alternatively if P cannot be factored into any intermediate field smaller than L).

- Splitting field L exists and its degree is $\leq d!$, where $d = \deg P$. And it is unique up to isomorphism as $K-$algebras.
- Degree of the splitting field divides $d!$.

Algebraic closure

- A field K is algebraically closed if any non-constant polynomial $P \in K[X]$ has a root in K.
- L is called an **algebraic closure** of K if it is algebraically closed and an algebraic extension over K.
- Every field has an algebraic closure.
- Algebraic closures of K are unique up to isomorphism as $K-$algebras.

Properties of finite fields

Let p be a prime integer and let $q = p^r$ for some positive integer r. Then the following statements hold.

- There exists a field of order q.
- Any two fields of order q are isomorphic.
- Let K be a field of order q. The multiplicative group $K^\times$ of non-zero elements of K is a cyclic group of order $q - 1$.
- Let K be a field of order q. The elements of K are the roots of $x^q - x \in \mathbb{F}_p[x]$.
- A field of order p^r contains a field of order $p^k \iff k|r$
- The irreducible factors of $x^q - x$ over $\mathbb{F}_p$ are the irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divides r.
- The splitting field of $x^q - x$ has q elements.
- $\mathbb{F}_q$ is a stem field and a splitting field of any irreducible polynomial $P \in \mathbb{F}_p$ of degree r.

Frobenius homomorphism

Let K be a field, $\mathrm{ch}(K) = p > 0$. There exists a homomorphism $\varphi : K \to K$, s.t. $\varphi(x) = x^p$. This is the Frobenius homomorphism.

- The group of automorphisms over $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$ is cyclic and is generated by the Frobenius map.

Separability

- **Separable polynomial:** An irreducible polynomial $P \in K[X]$ is called separable if $\gcd(P, P') = 1$, i.e. it has distinct roots.
- **Degree of separability:** $\deg_{\text{sep}} P = \deg Q$ for some $P(X) = Q\left(X^{p^r}\right)$
- **Degree of inseparability:** $\deg_i P = \frac{\deg P}{\deg Q}$
- **Purely inseparable polynomial:** P is purely inseparable if $\deg_i P = \deg P$. Also if P is purely inseparable $P = X^{p^r} - a$
- **Separable element:** If L/K is an algebraic extension, then $\alpha \in L$ is called separable if its minimal polynomial over K is separable. And vice versa.
- If $\alpha \in K$ is separable then $|\mathrm{Hom}(K(\alpha), \overline{K})| = \deg P_{\min}(\alpha, K))$
- **Separable degree:** For L/K, we have $[L : K]_{\text{sep}} = |\mathrm{Hom}_K(K(\alpha), \overline{K})|$. Inseparable degree is degree of extension divided by separable degree.
- **Separable extension:** L is separable over K if $[L : K]_{\text{sep}} = [L : K]$.
  - If $\mathrm{ch}(K) = 0$ then any extension of K is separable.
  - If $\mathrm{ch}(K) = p$ then pure inseparable extension has degree p^r with degree of inseparability p^r
- Separable degrees obey the multiplicative property.
- TFAE for finite L/K
  - L is separable over K
  - Any element of L is separable over K
  - $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where each α_i is separable over K.
  - $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, then α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$.
- **Separable closure:** $L^{\text{sep}} = \{x \mid x \text{ separable over } K\}$ for $x \in \overline{K}$

Multilinear map

For a module M over ring A. A function L from $M^r = \underbrace{M \times M \times \cdots \times M}_{r \text{ times}}$ into A is called multilinear if $L(\alpha_1, \ldots, \alpha_r)$ is linear as a function of each α_i when the other α_j are fixed.

Tensor product

Consider a ring A and two $A-$modules, M, N. The tensor product is denoted as $M \otimes_A N$ and is an $A-$module along with a $A-$bilinear map, $\varphi : M \times N \to M \otimes_A N$ which satisfies a "universal property".

Universal property of tensor product:

For a $A-$module P, if for an $A-$bilinear map, $f : M \times N \to P$, then $\exists!$ homomorphism $\tilde{f}$ of $A-$modules s.t. $f = \tilde{f} \circ \varphi$

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[dr, "f"'] & M \otimes_A N \arrow[d, dashed, "\tilde{f}"] \\ & P \end{tikzcd}$$

- Commutativity of tensor product $M \otimes_A N \cong N \otimes_A M$
- $A \otimes_A M \cong M$
- The basis for the tensor product of free modules is the tensor product of their individual basis elements.
- The tensor product is associative.

Base change theorem: For a ring A, B an $A-$algebra, M an $A-$module and N a $B-$module. Then we have the following bijection

$$\mathrm{Hom}_A(M, N) \leftrightarrow \mathrm{Hom}_B(B \otimes_A M, N)$$

- For I an ideal of a ring A and M an $A-$module we have, $A/I \otimes_A M \cong M/IM$

Chinese remainder theorem

Comaximal ideals: Two ideals of a ring are called comaximal (or coprime) if their sum gives the ring itself.

- If I, J are comaximal then $IJ = I \bigcap J$
- If $I_1, \ldots, I_k$ comaximal w.r.t J then $\prod_{i=1}^{k} I_i$ is also comaximal with J.
- If I, J are comaximal then so are I^m, J^n for any m, n.

Chinese remainder theorem: For a ring A, consider two comaximal ideals I, J, then $\forall a, b \in R, \exists! x \in A$ s.t. $x \equiv a (\mathrm{mod} I)$ and $x \equiv b (\mathrm{mod} J)$

Generalized Chinese remainder theorem: For a ring A, let $I_1, \ldots, I_n$ be ideals of the ring A. Consider the map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as $\pi(a) = (a \mod I_1, \ldots, a \mod I_n)$. Then $\ker \pi = I_1 \bigcap \cdots \bigcap I_n$, i.e. it is surjective iff $I_1, \cdots I_n$ are pairwise comaximal. If π is a surjection we have,

$$A/\bigcap I_k = A/\prod I_k \cong \prod (A/I_k)$$

Structure of finite algebras

Let A be a finite $K-$algebra then,

- There are only finitely many maximal ideals in A.
- For finitely many maximal ideals m_i. Let $J = m_1 \bigcap \cdots \bigcap m_r$. Then $J^n = 0$ for some n.
- $A \cong A/m_1^{n_1} \times \cdots \times A/m_r^{n_r}$ for some (not necessarily unique) $n_1, \ldots, n_r$.

Reduced K-Algebra: If it has no nilpotent elements.

Local ring: If it has only one maximal ideal. A non zero ring in which every element is either a unit or nilpotent is local.

Further results on separability

Let L be a finite extension over K then the following hold,

- L is separable $\iff$ $L \otimes_K \overline{K}$ is reduced.
- L is purely inseparable $\iff$ $L \otimes_K \overline{K}$ is local.
- L is separable $\iff$ $\forall$ algebraic extensions Ω, $L \otimes_K \Omega$ is reduced.
- L is purely separable $\iff$ $\forall$ algebraic extensions Ω, $L \otimes_K \Omega$ is local.
- If L is separable then the map $\varphi : L \otimes_K \overline{K} \to \overline{K}^n$ defined as $\varphi(l \otimes k) = (k\varphi_1(l), \ldots, k\varphi_n(l))$ (where φ_i are distinct homomorphisms from L to $\overline{K}$), is an isomorphism.
- Let L be a finite separable extension of K then it has only finitely many intermediate extensions.

Primitive element theorem

There exists $\alpha \in L$ s.t. $L = K(\alpha)$ whenever L is finite and separable.

Normal extensions

A **normal extension** of K is an algebraic extension which is a splitting field of a family of polynomials in $K[X]$.

TFAE for an extension L of K,

- $\forall x \in L, P_{\min}(x, K)$ splits in L.
- L is a normal extension.
- All homomorphisms from L to $\overline{K}$ have the same image.
- The group of automorphisms, $\mathrm{Aut}(L/K)$ acts transitively on $\mathrm{Hom}_K(L, \overline{K})$.

Some properties of normal extensions,

- $K \subset L \subset M$, if M is normal over K then it is normal over L, but L need not be normal over K.
- Extensions with degree 2 are normal.

Galois extensions

An algebraic extension that is both normal and separable is called a **Galois extension.**

- For a finite extension L over K the number of automorphisms $|\mathrm{Aut}(L/K)| \leq [L : K]$. Equality holds iff L is a Galois' extension.

If L is normal over K then,

- Isomorphism of sub extensions extend to automorphisms of L.
- $\mathrm{Aut}(L/K)$ acts transitively on the roots of any irreducible polynomial in $K[X]$.
- If $\mathrm{Aut}(L/K)$ fixes $x \notin K$. Then x is purely inseparable.

Galois groups

If L is a Galois extension, $G = \mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ is called the **Galois group** of the extension.

- $L^{\mathrm{Gal}(L/K)} = K$, (i.e. the set of invariants in L with the action of the Galois group is equal to K).
- Let L be a field and G a subgroup of $\mathrm{Aut}(L)$, then
  - If all orbits of G are finite, then L is a Galois extension of L^G.
  - If order of G is finite then, $[L : L^G] = |G|$ and G is a Galois group.

The Fundamental theorem of Galois theory

Let L/K be a Galois extension, and $\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ is its Galois group.

- If L is finite over K, then for a intermediate field F and a subgroup $H \subset \mathrm{Gal}(L/K)$ we have the following correspondence,
  - $F \to \mathrm{Gal}(L/F)$
  - $H \to L^H$
- F is Galois over K $\iff$ $g(F) = F, \forall g \in \mathrm{Gal}(L/K)$ $\iff$ $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K)$

Discriminant

For a polynomial P with roots x_i, the **discriminant** is $\Delta = \prod_{i<j}(x_i - x_j)^2$.

For $\mathrm{Gal}(P) \subset S_n$. For a separable polynomial,

- Δ is preserved by any permutation.
- $\sqrt{\Delta}$ is preserved only by even permutations
- $G \subset A_n \iff \sqrt{\Delta} \in K$

Cyclotomic polynomials and extensions

Let $P_n = X^n - 1$ where $p \nmid n$ if $\mathrm{ch}(K) = p > 0$.

P_n has n distinct roots which form a cyclic multiplicative subgroup $\mu_n \subset \overline{K}^{\times}$.

Let μ_n* denote the set of **primitive $\mathbf{n^{th}}$ roots of unity** (no roots of degree $< n$).

- $|\mu_n *| = \varphi(n)$

Cyclotomic polynomials: $\Phi_n = \prod_{\alpha \in \mu_n *}(X - \alpha) \in \overline{K}[X]$.

- $P_n = \prod_{d|n} \Phi_d$.
- Φ_n has coefficients in prime fields.
- If $\mathrm{ch}(K) = 0$ then $\Phi_n \in \mathbb{Z}[X]$, else if $\mathrm{ch}(K) = p$, we have Φ_n is the reduction mod p of the n^{th} cyclotomic polynomial over $\mathbb{Z}$.
- If $\mathrm{ch}(K) = 0$, then Φ_n is irreducible over $\mathbb{Z}[X]$.

Consider L, splitting field of K

- The splitting field of P_n over K is $K(\zeta)$ where ζ is a root of Φ_n.
- All $g \in \mathrm{Gal}(L/K)$ acts as $\zeta \to \zeta^{a^g}, (a^g, n) = 1$.
- $\mathrm{Gal}(L/K)$ injects into $\mathbb{Z}/n\mathbb{Z}^{\times}$ and this is an isomorphism when Φ_n is irreducible over K.

Kummer extensions

A field extension L/K is called a **Kummer extension** if for some integer $n > 1$

- K contains n distinct n^{th} roots of unity.
- $\mathrm{Gal}(L/K)$ is abelian group with lcm of the orders of group elements (exponent) equal to n.

Consider K s.t. for some n, $(\mathrm{ch}(K), n) = 1$ and $X^n - 1$ splits in K, for any $a \in K$ take $d = \min\{i \mid a^{i/n} \in K\}$ then we have,

- $d \mid n$ and $P_{\min}(a^{1/n}) = X^d - a^{d/n}$
- $K(a^{1/n})$ is Galois extension with cyclic Galois group of order d.

The converse is also true.

Artin-Schreier extensions

Let L/K be a field extension s.t. $\mathrm{ch}(K) = p$ for prime p. It is called **Artin-Schreier extension** if degree of extension L is p.

Artin-Schreier theorem: Let $\mathrm{ch}(K) - p$ and let $P = X^p - X - a \in K[X]$. Then P is either irreducible or splits in K. Let α be a root of P.

- If P is irreducible, then $K(\alpha)$ is a cyclic extension (i.e. Galois group is cyclic) of K of degree p.
- Any cyclic extension of degree p is obtained in the same way.

Composite extensions

Let L_1, L_2 be two intermediate extensions of K and some L/K that contains them both. Then $L_1L_2 = L_2L_1 = K(L_1 \bigcup L_2)$ the smallest extension that contains both L_1, L_2 is called **composite extension.**

- If L_1 and L_2 are separable/purely inseparable/normal/finite over K then its composite field also possess that property.

Linearly disjoint extensions

TFAE for algebraic extensions,

- $L_1 \otimes_K L_2$ is a field.
- $L_1 \otimes_K L_2 \to L$ is an injection.
- A linearly independent set in L_1 is also linearly independent in L_2.
- For linearly independent sets (over K) $A \in L_1, B \in L_2$ we have $A \times B$ is linearly independent over K

L_1, L_2 satisfying these properties are called **linearly disjoint extensions.**

- If $\deg L_1$ is finite then $[L_1L_2 : L_2] = [L_1 : K]$ equivalently $[L_1L_2 : K] = [L_1 : K][L_2 : K]$
- Extensions which are relatively prime degrees are linearly disjoint.

For $\overline{K}$ the algebraic closure of K,

- Let $L_1, L_2 \subset \overline{K}$, if L_1 is Galois over K and let $K' = L_1 \bigcap L_2$. Then L_1L_2 is Galois over L_2. The map $\phi : g \to g|_{L_1}$ of $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/K)$ is injective with image $\mathrm{Gal}(L_1/K')$ and L_1, L_2 linearly disjoint over K'.

Solvable extensions and polynomials

Solvable extension: A finite extension E of K is solvable by radicals if $\exists \alpha_1, \cdots, \alpha_r$ generating E such that $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ for some n_i.
Solvable polynomials: $P \in K[X]$ is solvable by radicals if $\exists$ a solvable extension E/K containing its roots.

- A composite of solvable extensions is solvable.
- For finite L/K solvable $\implies$ $\exists$ finite Galois extension also solvable when $\mathrm{ch}(K) = 0$.

Solvable groups

A group G is called **solvable** if it has a finite sequence of normal subgroups, $(I = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G)$ and also G_{i+1}/G_i is abelian.

- Subgroups of solvable groups are solvable.
- If G is solvable and $H \trianglelefteq G$ then G/H is solvable.
- If G if a finite abelian group then G is solvable
- S_n is not solvable for $n \geq 5$.

Solvability by radicals

Let $P \in K[X], \mathrm{ch}(K) = 0$. P is a polynomial solvable by radicals iff $\mathrm{Gal}(P)$ is solvable. Here $\mathrm{Gal}(P) = \mathrm{Gal}(F/K)$, where F is a splitting field of P over K.

Abel-Ruffini theorem

General polynomials of degree $n \geq 5$ are not solvable by radicals since S_n for $n \geq 5$ is not solvable.

Group representations

For vector space V, a **representation** of a finite group G is a homomorphism $\varphi : G \to GL(V)$, where $GL(V)$ is the group of automorphisms of V.
Regular representation: For vector space V generated by elements of group G. A homomorphism involving permuting this basis is called regular.

- For L/K as a vector space over K we have a representation of the Galois group $\varphi : \mathrm{Gal}(L/K) \to GL_K(L)$. This is a regular representation.

Normal basis theorem

For L/K a finite Galois extension, $\exists x \in L/K$ s.t. $\{gx \mid g \in G\}$ is a $K-$basis of L.

Integral elements

Integral elements: For a integral domain A and B an extension ring of A. An element $\alpha \in B$ is said to be integral over A if α is the root of a monic polynomial in $A[X]$.
TFAE,

- α is integral over A.
- $A[\alpha]$ is a finitely generated $A-$module.
- $A[\alpha] \subset C \subset B$ where C is a finitely generated A module.

Field Norm and Trace

Let $K \hookrightarrow E$ be a separable field extension, for $\alpha \in K$ its field norm is defined as $N_{E/K}(\alpha) = \prod_{\sigma_i : E \hookrightarrow \overline{K}} \sigma_i(\alpha)$. The trace (Tr) is the same with sum instead.

- Norm is multiplicative, trace is additive and $k-$linear.
- If $E = K(\alpha)$, $N_{E/K} = (-1)^{[E:K]}(\text{Constant coeff of } P_{\min}(\alpha, K))$, $\mathrm{Tr}_{E/K}(\alpha) = -(\text{Coefficient of } X^{[E:K]-1})$.
- For a tower $K \subset F \subset E$, $N_{E/K} = N_{F/K} \circ N_{E/F}$, $\mathrm{Tr}_{E/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{E/F}$.
- $T : E \times E \to K$ as $(x, y) \to \mathrm{Tr}(x, y)$ is a non-degenerate $K-$bilinear.
- If α is integral over $\mathbb{Z}$. Then $N_{E/\mathbb{Q}}(\alpha), \mathrm{Tr}_{E/\mathbb{Q}}(\alpha)$ are integers.

Integral extensions, closures

Integral extension: For $A \subset B$, B is said to be an integral extension of A if every element of B is an integral element over A.

- $A \subset B \subset C$ if B is integral over A and C integral over $B \implies C$ is integral over A.
- B is finitely generated over A as a module $\iff$ $B = A[\alpha_1, \ldots, \alpha_r]$ where each α_i is integral over A.
- Elements of B integral over A forms a subring of B. This is the integral closure of A in B.

Integrally closed: A is integrally closed in B if the integral closure of A in B is same as A. In general A is integrally closed if A is integrally closed in its field of fractions.

- $\mathbb{Z}$ is integrally closed.
- Any UFD is integrally closed.

Let K be a Number field, the integral closure of $\mathbb{Z}$ in K is O_K the ring of integers.

- $\forall \alpha \in K$, there exists $d \in \mathbb{Z}^*$ such that $d\alpha \in O_K$.
- $\alpha \in O_K \implies P_{\min}(\alpha, \mathbb{Q}) \in Z[X]$.
- O_K is a finitely generated, free $\mathbb{Z}-$module of rank $n = [K, \mathbb{Q}]$.

Reduction modulo prime

Let $P \in \mathbb{Z}[X]$ be an irreducible polynomial, and K its splitting field over $\mathbb{Q}$. With $[K : \mathbb{Q}] = n$. Let $G = \mathrm{Gal}(P)$. Let $\alpha_1, \ldots, \alpha_n$ be roots of P. Consider $A = O_K$ and let $J_1, \ldots, J_r$ be all the maximal ideals of A containing some prime p. Consider $D_i \subset G, D_i = \{g \in G \mid gJ_i = J_i\}$ and let $k_i = A/J_i$. There exists a natural homomorphism $D_i \to \mathrm{Gal}(k_i, \mathbb{F}_p)$
We then have the following,

- G acts transitively on $\{J_1, \ldots, J_r\}$ and D_i maps surjectively into $\mathrm{Gal}(k_i/\mathbb{F}_p)$.
- If reduction $\overline{P} = P \mod p$ does not have multiple roots then the map $D_i \leftrightarrow \mathrm{Gal}(k_i/\mathbb{F}_p)$ is a bijection and k_i is a splitting field of $\overline{P}$ for some i.

Example: If for $P \in \mathbb{Z}[X]$ is irreducible and $\exists$ prime p such that $\overline{P} = P \mod p$ is also irreducible. Then we have that $\mathrm{Gal}(P)$ contains an $n-$cycle permutation.