Chapter 1 : Galois Theory

References: Serge Lang, *Algebra*; Swayam's Algebra; Michael Artin, *Algebra*

1.1 Group Theory

1.1.1 Basics

Group axioms - closure, associativity, identity, inverses. Subgroups = subsets + groups.
Direct product of groups with component-wise operations also forms a group
Cyclic groups are singly generated; primitive roots are generators of n^{th} roots of unity

Homomorphism of G into itself is endomorphism; isomorphism of G into itself is automorphism.
Latter forms a group too, even for monoids
A homomorphism is determined by the image of its domain's generators
A homomorphism which yields an isomorphism between G & $\text{Im}(G)$ is an **embedding**

Trivial kernel $\iff$ injective homomorphism $f : G \hookrightarrow G' \implies$ embedding
Product of commuting subgroups with trivial intersection is isomorphic with G

1.1.2 Cosets

If $H \leq G, a \in G$ then aH is the left coset of H. Note that $aH = H \iff a \in H$
The mapping $x \to ax$ is bijective, implying the equal cardinality of all cosets

Turns out belonging to a coset is an equivalence relation, so they equipartition G
The number of left cosets of H in G is index $(G : H)$. Note that $(G : 1) = |G|$
This yields **Lagrange's Theorem**: $\forall H \leq G, |G| = (G : H) \cdot |H|$

This generalises for $G \geq H \geq K$ as $(G : K) = (G : H) \cdot (H : K)$ and in fact, the RHS coset representatives' products yield the LHS coset representatives
A corollary of this is the cyclicity of any group with prime order
Transpositions generate the permutation group S_n, whose size is $n!$

1.1.3 Normal subgroups

A normal subgroup H is one that satisfies $\forall x \in G : xH = Hx$ (conjugation by x)
The set of cosets of H, denoted by G/H, is a group iff H is normal

For $f : G \to G/H$, we have a homomorphism $f(x) = xH$ of which H is the kernel
Above map is the **canonical map**, and $\mathbf{G/H}$ is the factor group of G by H

For $S \subset G$, the set N_S of G-elements which preserve S under conjugation is its **normaliser** and the set Z_S of G-elements which preserve *every element* of S under conjugation is its **centraliser**. Centraliser of G is the **center** - a normal subgroup of G

1.1.4 Class equation

Number of elements in the center of a p-group is more than one (beyond just identity)
Any subgroup having index = smallest prime dividing $|G|$, is normal
If G/Z(G) is cyclic then G = Z(G) because every element of G is of the form $g^m z$ for g generator

1.1.5 Existence proof: induction

Base case of $|G| = 1$ or p is cyclic hence trivial. Assume existence of property (element of order p) holds for all groups H, $|H| < |G|$
Case: G is abelian Pick an element g of order q (else we done), and consider the group $\frac{G}{<g>}$ (normal coz G abelian). By induction hypothesis, $G/ < g >$ has an element h of order p coz p divides it coz $| < g > | = q$
Lift h to G, *i.e.* find the pre-image a of h in G such that $h < g >= a < g >$. Then the element ah has order as multiple of p (coz order of h is p and abelian)
If it's p we done else if it's pq, consider element a^q and we're done
Case: G is not abelian Just make use of the class equation - if p divides the order of the stabiliser of any element not in the center then we have a subgroup of order $< |G|$ satisfying the hypothesis and we're done
If p doesn't divide $|stab(g)|$ for any g not in Z(G), then it means $p|\frac{|G|}{|stab(g)|}$ and thus their sum. So by divisibility, p must divide the $|Z(G)|$ too, as p divides the rest. And center isn't the group itself coz we took it ain't abelian, hence we have a subgroup satisfying hypothesis

1.2 Ring Theory

Rings are sets of elements R with two operations + and * satisfying:

- (R,+) is an abelian group
- (R,*) is a closed, commutative and associative set
- * distributes over +

Ring with multiplicative inverses is a field
R is a ring of elements, with identity denoted as 1 and its multiples denoted by n
R[x] is the ring of all polynomials with coefficients in ring R, where x is any variable
Subring of R is a subset of R which is a ring in itself

Ring homomorphism: A map $\phi : R \to S$ such that
$\phi(a) + \phi(b) = \phi(a + b)$; $\phi(a) \cdot \phi(b) = \phi(ab)$; $\phi(1_R) = 1_S$.

1.2.1 Ideal

$I \leq R$ is an ideal if:

- $(I, +) \leq (R, +)$: subgroups
- $r \in R, s \in I \Rightarrow rs \in I$

Ideals are basically subrings without the identity (unless zero ring)
Ideal $(a_1, a_2, \ldots, a_n)$ is the smallest ideal containing all a_i: ideal generated by $\{a_1, a_2, \ldots, a_n\}$

First Isomorphism Theorem: ring homomorphism $\phi : R \to S \Rightarrow R/I \cong S$
Third IsoTheorem: Ideal J of $R/I \Rightarrow J = K/I$ for some K, $K \leq R$ and $I \subset K$

An ideal P of R is a **prime ideal** iff:

- $P \neq R$
- $ab \in P \Rightarrow a \in P \text{ or } b \in P$

P is prime ideal $\iff R/P$ is an (integral) domain

An ideal M of R is a **maximal ideal** iff:

- $M \neq R$
- $M \leq I \leq R \Rightarrow I = M \text{ or } I = R$

M is a maximal ideal $\iff R/M$ is a field
Zorn's Lemma $\Rightarrow$ every commutative ring R has a maximal ideal

1.2.2 Domain

A domain R is a ring with no zero divisors $\therefore$ in R: $a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0$
Any subring of a field is a domain
S is a multiplicatively closed (m.c.) set iff:

- $0 \notin S, 1 \in S$
- $s, t \in S \Rightarrow s \cdot t \in S$

$R \times S = \{(r, s) | r \in R, s \in S\}$ We can define an equivalence relation $\sim$ on $R \times S$: $(r, s) \sim (r', s')$ if $r \cdot s' = r' \cdot s$ This gives us equivalence classes $[r/s]$ of $R \times S/\sim$, which are fractions
Examples of multiplicatively closed sets:

1. $R* = R\backslash\{0\}$
2. $S = R/P$ where P is a prime ideal in R
3. $S = \{1, f, f^2, f^3, \ldots\}$ where $0 \neq f \in R$

I, J are ideals in R:

- $I + J = \{i + j \mid i \in I, j \in J\}$
- I and J are comaximal iff $I + J = R$

I and J are comaximal $\Rightarrow I \cap J = I \cdot J$ and $R/I \cap J = R/I \times R/J$

1.2.3 Polynomial Ring K[x]

Elements are $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid a_n \neq 0$ degree of f is defined as the largest integer power with a non-zero coefficient
$\forall\ f, g \neq 0 :\ deg(fg) = deg(f) + deg(g)$ Division algorithm: $\forall f(x) \neq 0, g(x) \in R\ \exists\ q(x), r(x) : g = f \cdot q + r$ where $q(x) = 0\ or\ deg(q) < deg(f)$
All ideals in K[x] are principal ideals: $\forall$ ideals $I\ \exists\ f(x) \in I$ such that $deg(f) = min\{\deg(g) | g(x) \in I\}$ Then $I = (f(x))$
f(x) is prime iff:

- f(x) is not unit
- $f(x)|g(x)h(x) \Rightarrow f(x)|g(x)\ or\ f(x)|h(x)$

f(x) is prime $\iff R/f(x)$ is a prime ideal
f(x) is irreducible iff:

- f(x) is not unit
- $f(x) = g(x)h(x) \Rightarrow g(x)\ unit\ or\ h(x)\ unit$

f(x) is prime $\iff R/f(x)$ is a maximal ideal
Eisenstein Criterion: If R is a domain and P is a prime ideal, and $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ and $\forall\ i :\ a_i \in P$ and $a_0 \notin P^2$ then f(x) is irreducible

1.2.4 Special Domains

Principle Ideal Domain Domain R is a P.I.D. if every ideal in R is principal *e.g.* $\mathbb{Z}[i], \mathbb{Z}[\omega]$. In a PID, prime elements are irreducible and vice-versa
Norm N is defined as a function from ring R to $\mathbb{N}_0$ satisfying N(0) = 0 Every ring in which a norm is defined and that enables us to follow Euclid' Division Algorithm is an ED All euclidean domains are PIDs
Unique Factorisation Domain Domain R is a U.F.D. if every element has a unique terminating factorisation into irreducible elements R is a UFD $\Rightarrow$ R[x] is a UFD
Gauss Lemma: $f(x) \in R[x]$ is a non-constant polynomial Let $K[x] = Qt(R)$ (quotient ring of R) and $g(x), h(x) \in K[x]$ So if $f(x) = g(x)h(x)$ for non-constant g, h, then $\exists\ g'(x), h'(x) \in R[x]$ such that $f(x) = g'(x)h'(x)$
Localisation Noetherian Rings Module Theory

1.3 Field Extensions

Here we attempt to find the solutions of algebraic equations in one or more variables.
Given a subring A of a ring B, and a finite number of polynomials, $f_1, \ldots, f_n$ in $A[X_1, \ldots, X_n]$, we want the n-tuples $(b_l, \ldots, b_n) \in B^{(n)}$ such that $f_i(b_1, \ldots, b_n) = 0$

1.3.1 Algebraic Extensions

Let F be a field. If F is a subfield of a field E, then we also say that E is an extension field of F.
$\alpha \in E$ is algebraic iff there are coefficients $a_i \in F$ such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$

Saying that α is algebraic over F is equivalent to stating that the evaluation homomorphism $F[X] \to E$ has a nonzero kernel, which is a principal ideal generated by a unique monic polynomial $p(X)$. The fact that $F[\alpha]$ is an integral domain forces $p(X)$ to be irreducible.

An extension E is "finite" if it is of **finite dimension**. If this is the case then E is also algebraic over F.
For fields $K \subset E \subset F$ we have: $[K : F] = [K : E][E : F]$ where $[E : F]$ denotes the dimension of E as a vector space over F.
For a field k, extension E and $\alpha \in E$, $k(\alpha)$ denotes the smallest field containing k and α. It contains $f(\alpha)/g(\alpha)$ for all polynomials $f, g \in k[X]; g(\alpha) \neq 0$.
For algebraic α over k, $k(\alpha) = k[\alpha]$ with $[k(\alpha) : k] = \deg\{Irr(\alpha, k, X)\}$

Given field extensions $E, F \subset L$ of a field k, their compositum EF is the smallest subfield of a common containing field that includes both E and F, provided L exists.
Given a subfield k of E and elements $\alpha_1, \ldots, \alpha_n$ in E, the field $k(\alpha_1, \ldots, \alpha_n)$ consists of all rational functions of $\alpha_1, \ldots, \alpha_n$ with coefficients in $k, i.e.\ \frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\cdots:\alpha_n)}, f, g \in k[X]$
A field E is finitely generated over k if there exist finitely many elements $\alpha_1, \ldots, \alpha_n$ such that $E = k(\alpha_1, \ldots, \alpha_n)$. It is the compositum of all its finitely generated subfields.

Every finite field extension is finitely generated (just include the bases).
If α_i are algebraic over k and n is finite then $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is **finite algebraic** over k. This is coz we can append an α_i at each step of finite tower.

Finite field extensions of $\mathbb{Q}$ are called algebraic number fields.
The commutative ring $k((x))$ of infinite power series in $k[x]$ forms a field
$[\mathbb{C} : \mathbb{R}] = 2$ as $(1, i)$ forms a basis of $\mathbb{C}$ over $\mathbb{R}$
$[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ but $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$
$[E : F]$ can also be understood as the dimension of quotient field E/F as a vector space

1.3.2 Algebraic Closures

An embedding is an injective homomorphism denoted by $\hookrightarrow$
For $E \supset F$, embedding $\tau : E \to L$ extends $\sigma : F \to L$ if $\tau|_F = \sigma$
If α is a root of $f(x) \in F[X]$ then $\tau(\alpha)$ is a root of $f^\sigma = \sigma(f)$
For algebraic $E \supset k$, any embedding from E to itself over k is an automorphism

The image ξ of X under the canonical homomorphism $\sigma : k[X] \to k[X]/(p(X))$ is a root of p^σ, which means $\forall f \in k[X], \exists E \supset k$ such that f has a root in E
L is algebraically closed if every polynomial in $L[X]$ has roots in L
For any field k we have the existence of an algebraically closed extension field $L \supset k$

1.3.3 Splitting Field-Extensions

Field k, polynomial $f(X) \in k[X]$. Splitting Field of K of f is the extension K of k consisting of all roots of f, thus making it "split" into linear factors over K.
Splitting field of $f_1(X), \ldots, f_n(X)$ is the same as that of a combined polynomial $f(X) = f_1(X)f_2(X)\ldots f_n(X)$

For splitting field K of $f(X) \in k[X]$, if E is another splitting field then there is an isomorphism $\sigma : E \to K$ which is identity over k.
For splitting field K of $\{f_i(X)\} \in k[X]$, if E is another splitting field then any embedding of E into K^a inducing identity over k is an isomorphism $\sigma : E \to K$.

$K \subset k^a$ is a **normal extension** of k if every irreducible polynomial in $k[X]$ with a root in K splits into linear factors in K.
In other words, K is the splitting field of a family of polynomials in $k[X]$.
Every embedding σ of K into k^a induces an automorphism on $K, i.e.\ \sigma(K) = K$

1.3.4 Inseparable Extensions

An irreducible polynomial $f(x) \in F[x]$ is **separable** if it has distinct roots in its splitting field. An algebraic extension K/F is separable if so is minimal polynomial of every element of K over F.

An extension that is not separable is **inseparable**. This can only occur in fields of prime characteristic $p > 0$. A polynomial $f(x)$ is inseparable if and only if its formal derivative $f'(x)$ is zero. This happens if $f(x)$ is a polynomial in x^p.
A field F is called **perfect** if all its finite extensions are separable (e.g., fields of characteristic 0 or finite fields). $\alpha \in K$ is separable over $k \subset K$ if its minimal polynomial over k has distinct roots

$K \supset k$ is a **separable extension** if all its elements are separable over k
In characteristic 0, all algebraic extensions are separable (not characteristic p)
Separable degree $[K : k]_s$ is the number of distinct k-embeddings of K into k^a
For separable extensions $K \supset k : [K : k]_s = [K : k]$

1.3.5 Primitive Element Theorem

The **Primitive Element Theorem** is a foundational result in field theory that establishes a condition for when a complex field extension can be simplified. It states that a finite field extension E/F is a **simple extension** (meaning it can be generated by a single element) if and only if there are only a finite number of intermediate fields between E and F.

A direct, powerful corollary is that every **finite separable extension** is a simple extension.

$$E = F(\alpha_1, \ldots, \alpha_n) \implies E = F(\gamma) \text{ for some } \gamma \in E$$

The element γ that generates the entire field is called a **primitive element**.

Key Idea

Imagine building a structure. An extension like $F(\sqrt{2}, \sqrt{3})$ is like building with two different types of special blocks, $\sqrt{2}$ and $\sqrt{3}$. The theorem tells us that if the conditions are right (separability), we can always find a single, more complex "master block" (like $\gamma = \sqrt{2} + \sqrt{3}$) from which we can construct all the same parts as the original two blocks combined. This simplifies the description of the entire structure down to just the base materials (F) and one special component (γ).

Conditions and Implications

- **Finite Extension**: The theorem applies to extensions of finite degree, $[E : F] < \infty$.
- **Separability**: This is the most crucial condition for the common statement of the theorem. An extension is separable if the minimal polynomial of every element has distinct roots. This is always true for fields of characteristic 0 (like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) and for all finite fields.

The theorem can fail for inseparable extensions, which occur in characteristic $p > 0$. For example, the extension $\mathbb{F}_p(t^{1/p}, u^{1/p})$ over $\mathbb{F}_p(t, u)$ is inseparable and requires two generators.

1.4 Galois Theory

Galois group of a polynomial acts transitively on the roots iff polynomial is irreducible
Artin's character theorem (multiplicative monoids) shows they're linearly independent
By Artin theorem on characters, all Galois permutations are linearly independent

Norm and trace belong to the base field itself
For $k \subset E, T : E \times E \to k$ given by $T(x, y) = Tr(xy)$ is a non-degenerate, symmetric, bilinear map.
Same with an inner product space.
$T(x, y) = 0 \ \forall y \in E \implies Tr(xE) = 0 \implies xE = E, Tr(E) = 0$

For K Galois over k, all subfields of K containing k are Galois over k
Field k is perfect if $k = k^p$ or k is characteristic 0
Every algebraic extension of a perfect field k is separable and perfect

1.4.1 Solvability

$[x, y] = x^{-1}y^{-1}xy, [G, G] = \langle [x, y] \mid x, y \in G \rangle$
Then $[G, G] \lhd G$ and $G/[G, G]$ is abelian and $[G, G]$ is minimal

For a finite solvable group G, any subgroup H is solvable
For a normal subgroup N of finite solvable G even G/N is solvable

1.4.2 Kummer Extensions

Kummer theory describes certain abelian extensions of a field. An extension K/F is a **Kummer extension** if it is a finite Galois extension whose Galois group $\mathrm{Gal}(K/F)$ is abelian of exponent n, and the base field F contains a primitive n-th root of unity ($\zeta_n \in F$).
The core theorem states that such extensions are precisely of the form $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ for some elements $a_i \in F$. There is a correspondence between subgroups of the multiplicative group $F^\times/(F^\times)^n$ and Kummer extensions of exponent n.

1.4.3 Constructible Numbers

A complex number is **constructible** if its corresponding point in the plane can be constructed from a given unit length using only a straightedge and compass.

Algebraically, a number α is constructible if and only if it is contained in a field extension $K \subset \mathbb{C}$ which is the top of a tower of quadratic extensions:

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n = K$$

where $\alpha \in K$ and $[F_i : F_{i-1}] = 2$ for all i. This implies that the degree of the minimal polynomial of a constructible number over $\mathbb{Q}$ must be a power of 2. This criterion proves the impossibility of classical problems like doubling the cube ($[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$) and trisecting an arbitrary angle.

1.4.4 Cyclotomic Polynomials

The **n-th cyclotomic polynomial**, $\Phi_n(x)$, is the unique irreducible monic polynomial over $\mathbb{Q}$ whose roots are the primitive n-th roots of unity. Its degree is given by Euler's totient function, $\phi(n)$.
It is defined as:

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_k)$$

where ζ_k are the primitive n-th roots of unity. The polynomial $x^n - 1$ factors into cyclotomic polynomials:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

The field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is called the n-th cyclotomic field. Its Galois group is abelian and isomorphic to the multiplicative group of integers modulo n, $(\mathbb{Z}/n\mathbb{Z})^\times$.

1.4.5 Transcendental Extensions

An element α is **transcendental** over a field F if it is not the root of any non-zero polynomial in $F[x]$. An extension K/F is transcendental if it is not algebraic.
A **transcendence basis** of K/F is a subset $S \subset K$ that is algebraically independent over F and is maximal with respect to this property (meaning K is an algebraic extension of $F(S)$). Any two transcendence bases of an extension have the same cardinality, which is called the **transcendence degree** of the extension, denoted $\mathrm{tr.deg}_F(K)$.