1 Main Results From 593

prime/maximal/irreducible

- If $R$ is a field $R[x]$ is a Euclidian Domain $\Rightarrow$ a PID $\Rightarrow$ a UFD.
- If $I = (p)$ for some $p \in R$, $I$ is a prime ideal and $R$ is a domain, then $p$ is irreducible in $R$.
- $R$ domain, $(p)$ prime $\Rightarrow$ $p$ irreducible.
- If $R$ is a UFD, $p \in R$ irreducible, $\Rightarrow$ $(p)$ is prime in $R$.
- If $R$ is a PID, $I$ prime ideal $\Rightarrow$ $I$ is maximal ideal.
- $R/I$ is a domain $\iff I$ is prime.
- $R/I$ is a field $\iff I$ is maximal.
- **Conclusion:** For $k[x]$, $k$ a field, $I$ ideal in $k[x]$, we conclude $I = (g(x))$. And If $k[x]/(g(x))$ is a domain then $(g(x))$ is prime $\Rightarrow$ maximal $\Rightarrow k[x]/(g(x))$ is a field and $g(x)$ is irreducible.
- $I,J$ ideals, $I + J = (I,J)$=smallest ideal containing both.

Modules

- $A,B$ submodules of $M$, $A + B$ the smallest submodule containing both.
- **Chinese Reminder for modules.** $A_1,...,A_k$ ideals in $R$, $A_i + A_j = R$, then the map $M \to M/A_1M \times ... \times M/A_kM$ (with kernel $\cap A_iM$) is surjective and $M/(A_1...A_k)M \cong M/A_1M \times ... \times M/A_kM$.

Sequences

- In SES:
  
  $0 \longrightarrow A \overset{a}{\longrightarrow} B \overset{b}{\longrightarrow} C \overset{c}{\longrightarrow} 0$

  $0 \longrightarrow ker(b) \overset{a}{\longrightarrow} B \overset{b}{\longrightarrow} coker(a) \longrightarrow 0$

- the LES induces SES:

  $\begin{array}{ccccc}
  A & \overset{a}{\longrightarrow} & B & \overset{b}{\longrightarrow} & C \\
  & \overset{c}{\longrightarrow} & \overset{d}{\longrightarrow} & \overset{e}{\longrightarrow} & E \\
  \end{array}$

  $0 \overset{a}{\longrightarrow} Coker(a) \overset{b}{\longrightarrow} C \overset{c}{\longrightarrow} ker(d) \overset{d}{\longrightarrow} 0$
Tensors:

- \( M \otimes \mathbb{Z} N \simeq M \otimes \mathbb{Z} N \).
- The functor \( M \otimes - \) commutes with colimits, right exact, preserve surjectivity.
- \( M \otimes (N \oplus K) = M \otimes N \oplus M \otimes K \)
- \( M \otimes_A A \simeq M \).
- \( A^r \otimes_A A^s \simeq A^{rs} \)
- \( R \)-ring with module \( I, R/I \otimes_R N \simeq N/(IN) \).
- \( R/I \otimes_R R/J \simeq R/(I+J) \).
- **Rationalization of an abelian group** \( G \otimes \mathbb{Q} \).
- \( M \) torsion group, \( M \otimes \mathbb{Q} = 0 \)
- For \( M, N \in Ab \) Define \( \text{Tor}(M,N) \in Ab \) by applying \( N \times_i nts \) on any SES (resolution) \( 0 \to K \to P \to M \to 0 \) to get \( \text{Tor}(M,N) = \text{Ker}(K \times N \to P \times N) \).
- Independent of choice of SES and \( \text{Tor}(M,N) = \text{Tor}(N,M) \).
- For an \( N \) torsion free module \( \text{Tor}(M,N) = 0 \).
- **Flat** modules \( \iff \) preserves injections \( \iff \) preserve SES.
- Free modules and Projective modules are flat.
- Free modules are Projective.
- \( \mathbb{Q} \) is a flat \( \mathbb{Z} \)-module.
- Direct sum of flat is flat. \( \mathbb{Q} \oplus \mathbb{Z} \) is a flat abelian group which is neither injective or projective.
- Over a PID, flat \( \iff \) torsion free.
- \( \mathbb{Q} \times \mathbb{Z} \mathbb{Z}/n = 0 \).
- \( \mathbb{Z}/m \times \mathbb{Z} \mathbb{Z}/n = \mathbb{Z}/(m,n) \).
- \( \mathbb{Q}/\mathbb{Z} \times \mathbb{Q} = 0 \).
- \( \mathbb{Q} \times \mathbb{Z} \mathbb{Z}/n = 0 \).
- \( \mathbb{Q} \times \mathbb{Z} \mathbb{Z}/n = 0 \).

2 Groups

2.1 Background

**Corollary 1.** All groups of order 4 are either \( \mathbb{Z}_4 \) or Klein, hence Abelian.

**Definition 1** (Centralizer, center, normalizer, normal subgroup). Let \( G \) be a groups, and \( A \) a subset.

- **Centralizer of** \( A \): \( C_G(A) = \{ g \in G | gag^{-1} = a, \forall a \in A \} \) (this is a subgroup, the biggest in which \( A \) is in the center).
• Center of G: \( Z(G) = C_G(G) \) (this is a subgroup).

• Normalizer of A: \( N_G(A) = \{ g \in G | gAg^{-1} = A \} \). Notice \( C_G(A) \leq N_G(A) \) (both subgroups, \( N_G \) is the biggest that fulfills the requirement)

• A subgroup. \( A \triangleleft G \iff N_G(A) = G \)

**Corollary 2.** \( Z(G) \triangleleft G \)

Proof. \( \forall g \in G : gZ(G)g^{-1} = Z(G) \implies N_G(Z(G)) = G \)

**Corollary 3.** Let \( G \) be a group, \( x \in G, a \in \mathbb{Z} - \{0\} \) \( \Rightarrow G = \langle x^a \rangle \iff \gcd(|x|, a) = 1 \)

**Corollary 5.** \( \phi : C_n = \langle a \rangle \rightarrow C_m, a \mapsto \Rightarrow \text{order}(x) \mid \gcd(n, m) \)

**Corollary 6.** Number of generators of a cyclic group of order \( n \) is (Euler’s \( \varphi \)-function).

\[ \varphi(p^{n_1} \cdots p^{n_r}) = \varphi(p^{n_1}) \cdots \varphi(p^{n_r}) \]

\[ \varphi(p^k) = p^{k-1}(p-1) \]. All \( p \)'s are prime.

**Theorem 1** (p-Sylow subgroup). Let \( G \) be a group of order \( p^a m, p \nmid m, p \)-prime. Then \( G \) has a subgroup of order \( p^a \), and \( G \) has an element of order \( p \).

**Corollary 7.** Let \( G \) be group, \( H, K \leq G \)

• \( |HK| = \frac{|H||K|}{|H \cap K|} \)

• \( KH \) is a subgroup \( \iff HK = KH \)

• if \( H \leq N_G(K) \Rightarrow HK \leq G \)

• if \( H \triangleleft G \Rightarrow HK \leq G \)

**Theorem 2** (Iso’s theorems 1-3). \( G \) Group, \( \varphi : G \rightarrow H \) homomorphism. \( A, B \) subgroups, \( A \leq N_G(B) \) (So \( AB \) is a subgroup as well). \( H, K \triangleleft G, H \leq K \)

1. \( \ker \varphi \triangleleft G, G/\ker \varphi \cong \varphi(G) \)

2. \( B \triangleleft AB, A \cap B \triangleleft A, AB/B \cong A/A \cap B \)

3. \( K/H \triangleleft G/H, (G/H)/(K/H) \cong G/K \)

**Theorem 3** (4th Iso’s theorem). \( G \) Group, \( N \triangleleft G \). There is a bijection from the set of subgroups \( A \) of \( G \) containing \( N \) to the subgroups \( \tilde{A} = A/N \). For \( A, B \leq G \) containing \( N \):

1. \( A \leq B \iff \tilde{A} \leq \tilde{B}, \text{ in that case } |B : A| = |\tilde{B} : \tilde{A}| \)

2. \( \triangleleft \tilde{A}, \tilde{B} \Rightarrow \triangleleft \tilde{A}, \tilde{B} \)

3. \( \tilde{A} \cap \tilde{B} = \tilde{A} \cap \tilde{B} \)

4. \( A \triangleleft G \iff \tilde{A} \triangleleft \tilde{G} \)

**Reminders**

• \( (\mathbb{Z}/(n))^x = (\mathbb{Z}/(p_1^{n_1})) \times \cdots \times (\mathbb{Z}/(p_r^{n_r})) \times = (\mathbb{Z}/(p_1^{n_1}))^x \times \cdots \times (\mathbb{Z}/(p_r^{n_r}))^x \)
2.2 Lectures

A few examples of groups:

- If $V$ is a vec.space, $GL(V) = Aut(V)$ is a group under composition. For finite dimension - $GL(V) \cong GL_n(V) = n \times n$ invertible matrices.

- If $V = \mathbb{R}^n$ is an inner product space, finite dimension, $Aut(V, \langle, \rangle) \cong O_n(\mathbb{R}) = n \times n$ orthogonal matrices.

**Corollary 8.** A subgroup of index 2 is normal.

**Definition 2** (group action, representation). A group acts on a set $X$ means $G \times X \to X$, where each $g \in G$ is in fact a member of $Aut X$. The action is a group homomorphism $G \to Aut X$. AKA representation of $G$ on $X$.

- Action is faithful id $G \to Aut X$ is injective.

- Orbit of $x \in X$ under $G$ is $\{gx | g \in G\} \subset X$. AKA $Gx$

- Stabilizer of $x \in X$ is $\{g \in G | gx = x\} \leq G$

**Theorem 4** (counting formula). If a finite group acting on $X$, then $|G| = |Stab(x)| \cdot |Orbit(x)|, \forall x \in X$

**Corollary 9.** Properties of actions:

- The orbits partition $X$ to equivalence classes

- The action is called **transitive** if there is only one orbit - all $X$.

2.3 From HW1

**Theorem 5** (Cayley’s Theorem). $G$ act on itself by left multiplication faithfully and iso to a subgroup of $Aut_{set} G$, and a subgroup of $S_n$

**Corollary 10** (Acting by conjugation). $G$ acts on itself by conjugation: $g \mapsto \gamma_g : (x \mapsto gxg^{-1})$. $\gamma_g$ is a group hom $G \to Aut_{group} G$, so in this case, the action is a group hom $G \to Aut_{group} G$.

The kernel is the center of $G$.

The image of $G$ under $G \to Aut_{group} G$ is called the **group of inner automorphism**

2.4 Back to lectures

**Theorem 6.** Under conjugation, the conjugacy classes of $S_n$ are determined by the cycle types and have 1-1 correspondence with partitions of $n$.

**Definition 3.** (Product = direct product of groups) For $N, H$ Groups, the Cartesian product $N \times H$ with the projections is the product of the group. I.e. denote $G = N \times H$ and let $G'$ be a group with maps to $N$ and $H$, so $\exists G' \to G$ s.t. the diagram commutes:
Corollary 11. Properties of $G = N \times H$

- $N, H \triangleleft G$
- $N \cap H = \{e\}$
- $N, H$ commute and each element in $G$ can be written uniquely as $n \cdot h$

Theorem 7. $N, H$ generate $G, N, H \triangleleft G, N \cap H = \{e\} \Rightarrow G \cong N \times H$

Theorem 8. $N, H$ generate $G, N \triangleleft G, N \cap H = \{e\} \Rightarrow$ if $g \in G$ then $g = x \cdot y, x \in N, y \in H$ and this composition is unique.

Theorem 9. $N, H$ groups, $H$ acts on $N$ by group hom $(H \rightarrow \text{Aut}_{\text{Grp}} N)$ So the binary op define on:

$$(N \times H) \times (N \times H) \rightarrow (N \times H)$$

$$(x, a)(y, b) \mapsto (x(a \cdot y), ab)$$

Gives a group structure denoted as $N \rtimes_{\phi} H$ - the semi product

Corollary 12. Properties of the above semi product

- $(x, a)^{-1} = (a^{-1} \cdot x^{-1}, a^{-1})$
- $N \triangleleft N \rtimes H, H \leq N \rtimes H$
- $\phi$ is trivial $\iff$ the semi-product=product $\iff$ $N$ and $H$ are commutative $\iff H \triangleleft N \rtimes H$
- If $H, N \leq G$ and $G = \langle H, K \rangle$ and intersection is trivial and $N$ is normal then $G = N \rtimes H$ and the action must be conjugation.
- $C_4 = \langle r \rangle \rtimes_{\phi} C_2 = \langle x \rangle$ where $x \cdot r = x^{-1}$. Then the semi product is $D_4$.
- $Q$ is never semi product.

quiz2,q5 Just send the generator of $C_{12}$ to $(1, 2) \in S_5$.

3 From HW2

Definition 4. (Split) The short exact sequence $1 \rightarrow A \rightarrow G \xrightarrow{\pi} B \rightarrow 1$ is split if exists $\phi : B \rightarrow G$ s.t. $\pi \phi = \text{id}_B$

Definition 5. The Alternating group $A_N \leq S_N$ is the even permutations. If recognized as subgroup of $\text{GL}_n(k)$ so we have the exact seq: $\{1\} \rightarrow A_N \hookrightarrow S_n \twoheadrightarrow \{\pm 1\} \rightarrow \{1\}$, where $\det : S_N \rightarrow \{\pm 1\}$

4 Back to Lectures

Definition 6. A group $G$ is simple if it has no non-trivial normal subgroups.

- Equivalent: if $\exists G \rightarrow H \Rightarrow G \cong H$.
- The alternating group - even permutations - $A_N$ is simple for $N \geq 5$. 
• $A_4$ is not simple, $\cong$ tetrahedral group = semi direct product of the (normal) 4-sylow and a 3-sylow.

**Theorem 10.** (Sylow’s) $G$ a group, $p$ prime, $|G| = p^N m, p \nmid m$ so
1. $\exists H \leq G, |H| = p^N, H$ – called the $p$-sylow subgroup
2. all the $p$-sylows are conjugate to each other. (one orbit under conjugation).
3. Let $s_p$ be the number of $p$-sylows. so $s_p \equiv 1(\text{mod} p)$ and $s_p|m$.
4. (Sylow 1’) In fact, $\exists H \leq G$ s.t. $|H| = p^a$ for all $a = 0...N$

**Properties of p-Sylow**
• Every two $p$-Sylow groups are conjugate.
• $|G| = p^m p \nmid m$ Then the number of $p$-Sylow group $n_p$ is the index of the normalizer of $P$.
• If there is only one $p$-sylow so, $P$ is normal.

**Definition 7.** A **composite series** for a group $G$ is a finite sequence of subgroups: 
\[
\{e\} = G_0 \triangleleft G_1 \triangleleft ... \triangleleft G_r = G, \text{ where all } G_{i+1}/G_i \text{ are non-trivial and simple. These are called the factor groups.}
\]

**Theorem 11.** **Jordan-Holder:**
• Every finite group has a composite series
• If $G$ has two composite series, they have the same factor groups up to rearrangement. (Also valid for infinite groups).

**Corollary 13.** $A_4$ has one normal Klein subgroup $K$ gen by all 2+2 cycles $(ab)(cd)$, and 4 subgroup of order 3 $< (abc) >$. Also, it is $K \rtimes C_3$, where the conjugation correspond to $(a,b,ab)$ or $(a,ab,b)$.

**Solvability**
• A group is **solvable** if it has a normal series in which all the quotients are abelian.
• If $G$ is finite, solvable $\iff$ the factors group is the Jordan-Holder Thm are abelian.
• For a SES $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1, B$ solvable $\iff$ both $A$ and $C$ are solvable. In such case, $B$ will have the same Jordan-Holder factors as $A$ and $C$ together.
• Every subgroup of a solvable is solvable.
• Semi direct product of ”solvable”’s is solvable.
• The **Derived series** of $G$ is a normal sequence where each group is the commutator of the previous one.
• Solvable $\iff$ the derives series terminates with the trivial group.
• $p$-groups are solvable.

**Corollary 14.** **Consequences of Sylow:**
• $G$ of order $pq$, $(p,q \text{ - primes})$ is never simple)
• There are 5 groups of order 12: $C_12, C_6 \times e_2, A_4, D_6, < x, z | x^4 = 1, z^3 = 1, xzx^{-1} = z^2 >$
5  From HW3

Corollary 15. the Class Equation $|G| = |Z(G)| + \sum_{g_i} |G : C(g_i)|$

6  Back to lectures

Definition 8. A (Linear) Representation of a group $G$ is an action of $G$ on a vector space $V \to GL(V)$.

- Tautological rep: $GL(n(k)) \hookrightarrow GL(k^n)$.
- $D_4, 2$dim : $r \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $x \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- $D_4, 4$dim : $r \mapsto \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $x \mapsto \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Definition 9. A sub-representation of rep of $G$ on $V$ is a sub space $W \subset V$ s.t. $g(W) \subset W$.

- Called irreducible if there are no proper sub-reps.
- $D_4, 4$-dim-rep, has 3 sub-reps, $W = \langle \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \rangle$, $W' = \langle \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \rangle$, $T = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Definition 10. The Category of representation of a group $G$ over $K$:

- objects: VectSpaces $V$ over $k$, with group map $G \to GL(V)$.
- morphism: linear map $\phi : V \to W$ with $\phi \circ g(x) = g \circ \phi(x)$
  - Equivalent to the category of $k[G]$-modules.

Corollary 16. Given map of reps of $G$, $V \to W$ then $\text{Ker}\phi, \text{Im}\phi, \text{coKer}\phi$ are sub reps.

Corollary 17. Building reps by:

- $V \times W, g(v, w) = (gv, gw)$.
- $V \otimes W, g(v \otimes w) = gv \otimes gw$.
- $V \cap W$.

Corollary 18 (Schur's). $V \to W$ map of irreducible reps, so it is either an iso or the zero map.

Corollary 19. $V$ is irreducible $\iff \forall x \in V - \{0\}$, the orbit of $x$ spans $V$.

Theorem 12. Maschke's $G$ - group, $|G| < \infty$ invertible in $k$ (char=0 or when char = a prime $p$, $p \nmid |G|$, then every subarep $W$ of a $G$-rep $V$ has a $G$-rep complement. i.e $V = W \oplus U$ as $G$-reps. Under these condition, and if in addition $V$ is finite dimension, then
• it decomposes to irreducible sub-reps.

• It decomposes uniquely to \( V_1 \oplus ... \oplus V_t \) where each \( V_i \) is a direct some of \( a_i \) irreducible sub-reps isomorphic to each other \( V_i \cong W_i^{a_i} \).

**Schur part 2** For an algebraically closed field \( k = \overline{k} \), the only \( G \)-rep automorphism of irreducible reps is given by scalar multiplication.

• if \( G \) is a finite abelian group, the only irreducible maps are 1-dim.

**Corollary 20.** If \( N \triangleleft G \), then a rep of \( G/N \) is a rep of \( G \) by \( G \rightarrow G/N \rightarrow GL(V) \).

**Examples**

• For \( S_n \rightarrow GL_n(\mathbb{C}) \) the permutation rep. \( \langle \begin{bmatrix} 1 & \cdots & 1 \\ 1 & \cdots & 1 \\ \vdots & \cdots & \ddots \\ 1 & \cdots & 1 \end{bmatrix} \rangle \) is a sub rep and the complement \( \langle \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \rangle, \sum x_i = 0 \rangle \) is called the **standard rep** which is irreducible.

• \( S_3 \) has 3 irreducible maps over \( \mathbb{C} \): 1-dim trivial, 1-dim alternating, 2-dim standard.

**Definition 11.** A **Group character** of \( G \) id a 1-dim rep of \( G \) \( \chi : G \rightarrow GL(k) \cong k^* \).

**Definition 12.** Fix \( \rho : G \rightarrow GL(V) \) finite dim rep over \( \mathbb{C} \), \( |G| < \infty \). The **character** \( \chi \) of \( \rho \) is the function \( \text{trace} : g \mapsto \text{tr}(g) \).

• \( \chi \) is a class function, same value under conjugation, seen as vector space \( C \subset \mathbb{C}^{[G]} \).

**Theorem 13.** Main results:

• The characters of the isomorphism class of irreducible reps form an orthonormal basis of \( C \) with \( \langle \chi, \chi' \rangle = \frac{1}{|G|} \sum g \chi(g)\chi'(g) \).

• Each \( G \) as above has finitely many irreducible-reps, correspond to the number of conjugacy classes.

• Denote \( d_i \) as the dim of the \( t \) different irreps, so \( \sum d_i^2 = |G| \).

• \( \text{dim} = \chi(e) \).

• \( \chi V \otimes W = \chi V + \chi W \).

• \( \langle \chi, \chi \rangle = 1 \iff \chi \) is the character of an irr-rep.

• Center elements acts as scalar multiplication for any representation.

• \( \chi V \otimes W = \chi V \chi W \).

• \( V \cong W_1^{a_1} \oplus ... \oplus W_t^{a_t} \), \( a_i = \langle \chi V, \chi W_i \rangle \geq 0 \in \mathbb{Z}_{\geq 0} \).

• \( G \) acts on itself by left mul. **regular representation.** \( \chi_{\text{reg}} = (|G| \text{ for } e, 0, 0, ... 0) = \sum d_i \chi W_i \). Also \( V_{\text{reg}} \cong \mathbb{C}[G] \).

• Row orthogonally of the columns \( \langle C_i, C_j \rangle = \frac{|G|}{l_i} \delta_{ij} \), \( l_i \) - number of elements in the class.
• \( \langle \chi_V, \chi_V \rangle = \sum a_i^2 \)
• \( \chi_{\Lambda^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)). \)
• \( \chi_{S^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)). \)
• \( \chi_{\text{Hom}(W, V)} = \chi_V \chi_W \)

7 Fields

Definition 13.  
• a prime subfield is the filed get by 1: \( \mathbb{Q} \) or \( \mathbb{F}_p \).
• An extension \( k \hookrightarrow L \) is algebraic if every \( \theta \in L \) is algebraic over \( k \).
• \( k \hookrightarrow L \), \( \theta \in L \) so \( k[x] \rightarrow L \) by \( x \mapsto \theta \). The ker is \( (g(x)) \). If non trivial, \( g \) if minimal polinomial of \( \theta \in L \) over \( k \). If injective - transcendental. \( k[x]/(g(x)) \cong k[\theta] \).
• If algebraic - \( k[\theta] \cong k(\theta) \), Else \( k[\theta] \subsetneq k(\theta) \).
• \([L : k]\) - dimension of \( L \) as a v.s. over \( k \).
• \( k \hookrightarrow L \hookrightarrow F \Rightarrow [F : k] = [F : L][L : k] \) if all finite.

Definition 14. algebraically independence. Fix Field extension \( L/k \).
• A set \( S = \{\theta_1, \theta_2, \ldots\} \) is algebraically independent over \( k \) if any polynomial in \( k[x_1, x_2, \ldots] \) satisfied by \( S \) is the zero polynomial.
• A set \( S = \{\theta_1\} \) is algebraically independent \( \iff \) \( \theta_1 \) is algebraic over \( k \).
• The cardinality of the maximal algebraically independent set is the transcendence degree. \( S \) called a transcendence basis
• transcendence degree is \( \theta \iff \) extension is algebraic.
• \( S \) a basis for \( L/k \Rightarrow L/k(S) \) is algebraic.

Theorem 14. Every finite field extension of \( \mathbb{Q} \) is simple.

7.1 From HW6

Separability
• A polynomial is separable over \( k \) if it has no multiple root in any extension.
• Separable \( \iff \) relatively prime to its derivative.
• \( g(x) \) irreducible. Separable \( \iff \) \( g' \neq 0 \).
• over char 0 and over a finite field, every irreducible is separable.

7.2 Constructible numbers - Not in the QR
• A number \( a \in \mathbb{R} \) is constructible if segment of length \( |a| \) can be constructed.
• The set \( C \) of constructible is a field \( \mathbb{Q} \subset C \subset \mathbb{R} \). Algebraic and infinite.
7.3 Splitting fields - p30

Theorem 15. splitting fields

- $g(x) \in L[x]$ factors completely over $L$ if all its roots are in $L$.
- $L$ is the splitting field of $g \in k[x]$ if it is the smallest extension of $k$ in which $g$ splits.
- Such $L$ over $k$ exists and unique, algebraic of degree at most $\deg(g)!$.

Cyclotomic poly's

- $n$th cyclotomic field $K_n$ is the splitting of $x^n - 1$ over $\mathbb{Q}$.
- $K_n = \mathbb{Q}(\zeta_2^{3\pi/n})$. Poly is $\Phi_n = \prod_{\langle k, n \rangle = 1}(x - \zeta_k) \in \mathbb{Z}[x]$
- Degree $\phi(n)$ - Euler's function.
- $K_p$, $p$-prime, degree $p - 1$.
- Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Corollary 21. $\mathbb{F}_p$ is infinite, for any $n$ there is a irreducible poly of degree $n$ in $\mathbb{F}_p$, a factor of $x^n - x$

Field Aut

- For any category, $\text{Aut}(\text{object})$ is a group under composition.
- $L$ over $k$, $\text{Aut}_k(L) = \{ \phi : L \rightarrow L, \text{field iso}, \phi|_k = \text{id}_k \}$
- If $g(x) \in k[x]$, Then $\text{Aut}_k(L)$ permutes the set $B$ roots of $g(x)$ in $L$. $\text{Aut}_k(L) \hookrightarrow S_{|B|}$.
- Further, If $L = k(B)$ the the map above must be injective. Let $B = \{a_1, \ldots, a_t\}$ each $a_i$ with min poly $g_i \in k[x]$ and $r_i$ roots in $L$. Then Aut($L/k$) $\hookrightarrow S_{r_1} \times \ldots \times S_{r_t}$, each member permutes the roots of $g_i$ in $L$.
- If $L$ is the splitting field of $g(x)$ over $k$, $\text{Aut}_k(L) \hookrightarrow S_d$ ($d$-number of distinct roots of $g(x)$ not in $k$). After eliminating the roots in $k$, the action is transitive $\iff g(x)$ is irreducible. For a general splitting field, we get a transitive action $\text{Aut}(L/k) \hookrightarrow S_{r_1} \times \ldots \times S_{r_t}$.
- If $L = k(B) = k(\alpha)$ then $\text{Aut}_k(L)$ is trivial.
- For alg extension $|\text{Aut}_k(L)| | [L : k]$
- For a splitting filed of poly of degree $d$, $|\text{Aut}_k(L)| \leq d!$
- $k = \mathbb{F}_p(t), g(x) = x^{2p} - t \Rightarrow L = k(t^{1/2p})$, Aut = $S_1$ or $S_2$, not of order $[L : k] = 2p$.
- $\phi_1, \ldots, \phi_n \in \text{Aut}(L/k)$ are linearly independent as $L \rightarrow L$ functions.

Galois

- Thm/Def For finite alg’ extension $|\text{Aut}_k(L)|$ divides $[L : k]$. When equals - Galois extension and group.
- Thm $L/k$ Galois $\iff L$ is a splitting field and $L$ is separable - Every minimal poly in $L$ is separable over $k$. $\iff L$ is a splitting field of a separable poly.
Every extension of char 0 is separable.

$L$ over $k$, A map from intermediate fields to subgroup of $Aut_k(L)$: $[k \subset F \subset L] \mapsto Aut(L/F) < Aut(L/k), H < Aut(L/k) \mapsto L^H = \{x \in L : hx = x, \forall h \in H\}$.

$\cdot |H| = [L : L^H]$ For any subgroups of $Aut(L/k)$. Further if Galois, then the subgroups are also Galois.

$\cdot$ Action of $\phi \in Aut(L/k)$ on its subgroups and intermediate fields $F$: $H \leq G, \phi \cdot H = \phi H \phi^{-1}$, and $F$ field over $k, \phi \cdot F = \phi(F)$. Correspondence $L^H \phi^{-1} = \phi(L^H)$.

$\cdot F = L^H$ over $k$ is Galois $\iff$ $H = Aut(L/F) \triangleleft G$ and then $Aut(F/k) \cong G/H$. Also there is surjection $Aut(L/k) \to Aut(L^H/k), \phi \mapsto \phi|_{L^H}$ with $ker = H$. In general, $[L^H : k] = [G]/|H|$. - $G \supset H_1 \triangleright H_2 \triangleright \{e\} \Rightarrow L^{H_2}/L^{H_1}$, Galois

$L/k$ galois $\iff$ the maps are bijections and mutually inverse, and order reversing.

$\mathbb{F}_p^n / \mathbb{F}_p$ is Galois, $Aut = C_n$ gen by Frobenius $x \mapsto x^p$ $x^n - x$ is separable.

$L/k$ splitting $g(x) \in k[x]$ and $\phi : k \cong k'$. So there are $[L : k]$ ways to extend $\phi$ to $\phi'$:

$$\phi' \cong \phi \quad \quad \phi'^{-1}$$

$\cdot$ Any separable finite extension is contained in a Galois extension. The intersection of them all - Galois Closure. Corollary: Every extension like the above admits finitely many intermediate fields.

simple extension $\iff$ admits finitely many intermediate fields.

Separability

$\cdot$ An irreducible (DF does not require irreducible) polynomial $g(x) \in k[x]$ is separable over $k$ if it has no multiple roots in any filed extension of $k$

$\cdot \alpha$ multiple root of $g(x) \in k[x] \iff$ root of $g'$ $\iff$ the min poly of $\alpha$ divides both.

$\cdot g(x)$ separable $\iff$ $g$ relatively prime to $g'$.

$\cdot$ In char 0 and in finite fields, every irreducible is separable. separable $\iff$ product of distinct irreducible elements.

$\cdot$ For irreducible in char $p$ - separable $\iff$ $g' \neq 0$.

$\cdot$ Every extension of $\mathbb{Q}$ or a finite field is separable. Every finite separable extension is simple.

$\cdot$ finite extension $L/k$ is a splitting field $\iff$ every irreducible with root in $L$ splits completely. i.e. Normal field extension.

$\cdot$ Normal field extension is an extension $L/k$ where for every poly $g(x) \in k[x]$ with a root in $L$ splits completely.

$\cdot$ finite extension is normal $\iff$ it is a splitting field.
Symmetric poly’s

- **Symmetric polynomial** is a poly in $k[t_1,\ldots,t_N]$ fixed by the action of $S_n$ interchanging the variables.

- $E_m = \sum_{i_1<\ldots<i_m} t_{i_1}\cdots t_{i_m}$ the coef of $\prod(x - t_i)$ - The generic monic poly.

- **Thm**
  - The ring of sym.polys is $k[E_1,\ldots,E_N]$.
  - this is a poly ring, each sym.poly can be written uniquely by $E_i$’s.
  - the extension $k(E_1,\ldots,E_N) \hookrightarrow k(t_1,\ldots,t_N)$ is galois with group $S_N$.

- The $N$th Discriminant $\Delta_N = \prod_{i<j}(t_i - t_j)^2$

- $f(x) = x^N + a_1x^{n-1} + \ldots + a_N \in k[x]$ has a multiple root $\iff \Delta_N(-a_1, +a_2, \ldots, (-1)^Na_N) = 0$

- for $\sigma \in S_N, \sigma\sqrt{\Delta} = \text{sgn}(\sigma)\sqrt{\Delta}$.

- For $\text{char} \neq 2$, The Galois group of $f(x)$ as above lies in $A_N \iff \Delta_N$ is a square of the field.

### 7.4 Solvability by radicals

- **Given** $k$, $\theta$ lag’ over $k$. we say the $\theta$ is **solvable by radicals** if $\exists$ a Radical Tower of field ext’ $k \subset k_1 \subset \ldots \subset k_N$ s.t. $\theta \in k_N, k_{i+1} = k_i(\beta_i), \beta_i^{n_i} = b_i \in k_i$.

- **Thm** $k$ of char 0, $\theta \in K$ then $\theta$ is exp’-by-rad $\iff \text{Gal}(f(x)/k)$ is a solvable where $f(x)$ is the min poly of $\theta$ over $k$ (if one root is exa-by-rad, all the others as well)

- **Kummer Ext** $K$ of char 0, $E/K$ Galois with group $G \cong \mathbb{Z}/(p)$ for a prime $p$, $K$ contains all the $p$th roots of unity THEN exists $b \in K$ s.t. $E = K(\sqrt[p]{b})$.

- If exp-by-rad, the tower be can where each extension is Galois with cyclic group (can be refined further to even prime order cyclic group).

### Trace and Norm

- **Trace and Norm** of $a \in L/K$ is the trace and determinant of $L \to L$ linear map of multiplication by $a$.

- $K \hookrightarrow L, \text{tr} : L \to K$ is a $K$ vector space. $\text{Norm} : L \to K$ is a $L^\times \to K^\times$ multiplicative group map.

- $K \hookrightarrow E \hookrightarrow L$, so $\text{tr}_{E/K} \circ \text{tr}_{L/E} = \text{tr}_{L/K}$. Same for Norm.

- Same min.poly as in fields. Char poly = $(\text{min.poly})^{[L:K(a)]}$

- **If Galois**:
  - Char.poly = $\prod_{g \in G}(x - ga)$.
  - $\text{tr}(a) = \sum_{g \in G} ga$
  - $\text{Norm}(a) = \prod_{g \in G} ga$
7.5 examples

- $\text{Gal}(x^n - 1/\mathbb{Q}) = (\mathbb{Z}/n)^\times$.

- For irreducible of degree $p$-prime, with exactly 2 non real roots, $\text{Gal} = S_p$. Properties of $S_n$
  - $S_n$ is gen’ by $(1,2,...,n)$ and $(1,2)$.
  - $A_n$ is gen’ by the 3-cycles.
  - $S_p$, $p$-prime, is ten by any $p$ cycle and any transposition.
  - $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, $\text{Aut} = C_n$ gen by Frobenius $x \mapsto x^p$ $x^{p^n} - x$ is separable.