GALOIS THEORY, ARITHMETIC AND GEOMETRY

UTSAV CHOUDHURY

Contents

1. Lecture 1 : Introduction 1
2. Lecture 2 : Group Theory basics 4
3. Lecture 3 7
4. Lectures 4-5-6 10
5. Lecture 8 19
6. lecture 9 23
7. Lecture 9 26
8. Lecture 10 28
9. Lecture 11 30
10. Trace, Norm, Discriminant 32
11. Galois Correspondence 35
12. Solvability by radicals 38
13. Algebraic Closure 42
14. Absolute Galois groups 43
15. Hilbert Theorem 90 46

1. Lecture 1 : Introduction

Let F be any of the following fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and let $f(x) \in F[x]$ be a polynomial.

$$Sol(f)(F) := \{\alpha \in F | f(\alpha) = 0\}.$$

We have the following fundamental theorem of algebra.

Theorem 1.1 (Gauss, 1799)**.** *Let $f(x)$ be non constant. Then $Sol(f)(\mathbb{C}) \neq \Phi$. Infact, $|Sol(f)(\mathbb{C})| = n = deg(f)$, if we count the roots with multiplicities. Therefore*

$$f(x) = a_n \prod_{i=1}^{n} (x - \alpha_i),$$

where α_i's are roots of $f(x)$ (not necessarily distinict).

Note that we have a $\mathbb{Z}/2\mathbb{Z}$ action on $\mathbb{C}$ given by $z \in \mathbb{C} \mapsto \bar{z} \in \mathbb{C}$, whose fixed points are precisely the real numbers $\mathbb{R}$. Note that if $z = a + ib$, then $\bar{z} = a - ib$ and $z.\bar{z} = a^2 + b^2$. On the other hand consider the map $l_z : \mathbb{C} \to \mathbb{C}$, given by $l_z(\alpha) := z.\alpha$.

Exercise 1.2. *(1) Show that l_z is $\mathbb{R}$-linear.*
(2) Show that $det(l_z) = z.\bar{z}$.
(3) Find $trace(l_z)$.

Observe that $z.\bar{z}$ is the constant term of the real polynomial $f_z(x) := x^2 - (z + \bar{z})x + z.\bar{z}$, which has z and $\bar{z}$ has its roots. If the imaginary part of z is non-zero then $f_z(x)$ can not be factorised over $\mathbb{R}$, therefore $f_z(x)$ is irreducible in $\mathbb{R}[x]$. If $F = \mathbb{Q}$ or $\mathbb{R}$ and $f(x) \in F[x]$, then $f(\alpha) = 0$ iff $f(\bar{\alpha}) = 0$ for $\alpha \in \mathbb{C}$. So, we get a $\mathbb{Z}/2\mathbb{Z}$ action on $Sol(f)(\mathbb{C})$ for such f such that

(1) The action is trivial on the subset $Sol(f)(F)$.
(2) The fixed points of this action is precisely the subset $Sol(f)(\mathbb{R})$.

Given a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$, with $a_i \in F$, we know from Vieta's formulae that the coefficients a_i can be expressed as symmetric polynomials on the roots.

Quadratic

$f(x) = a_2x^2+a_1x+a_0 = a_2(x-\alpha_1)(x-\alpha_2)$ with $a_2 \neq 0$. Putting $p = -a_1/a_2, q = a_0/a_2$, we see that α_1, α_2 satisfies the equation $x^2 + px + q = 0$. Completing quares we get $(x + p/2)^2 + (q - p^2/4) = 0$, then taking square roots we get the roots to be $-p/2 \pm \sqrt{p^2/4 - q}$. Note that the roots can be expressed using the four arithemtic operations and extrcating roots applied to the coefficients.

The discriminant $\triangle := p^2 - 4q = (\alpha_1 - \alpha_2)^2$ is non zero iff α_1, α_2 are different.

Cubic Let $f(x) = \sum_{i=0}^{3} a_i x^i = a_3(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ such that $a_3 \neq 0$. Making it monic and putting $X = x + a_2/3a_3$ we get $X^3 + pX + q = 0$. Note that $(a + b)^3 - 3ab(a + b) - (a^3 + b^3) = 0$, therefore if $p = -3ab$, $q = -(a^3 + b^3)$ then $X = (a + b)$ is root. Note that $-p^3/27 = a^3b^3$ and $-q = (a^3 + b^3)$. Therefore a^3, b^3 are roorts of the quadratic $g(T) = T^2 + qT - p^3/27$. Therefore taking cube roots of the roots of $g(T)$ and then adding them will give us a root of f.

Show that $\triangle := -(4p^3 + 27q^2) = ((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_1))^2$.

Quartic Let

$$f(x) = \sum_{i=0}^{4} a_i x^i = a_4 \prod_{i=1}^{4} (x - \alpha_i),$$

with $a_4 = 1$. Then

$$f(x) = (x^2 + (a_3/2)x + t/2)^2 - [(a_3^2/4 + t - a_2)x^2 + (a_3t/2 - a_1)x + (t^2/4 - a_0)] =$$
$$= f_1(x, t)^2 - g_1(x, t).$$

Note that both f_1 and g_1 are quadratic in x. If g_1 is a square for some t, then we can solve two quadratics to get roots of $f(x)$. Now, g_1 is a square for those t's satisfying

$$(a_3t/2 - a_1)^2 - 4(t^2/4 - a_0)(a_3^2/4 + t - a_2) = 0.$$

This is a cubic in t, therefore we are reduced to the previous case.

What happens for quintic :

Theorem 1.3 (Abel 1823, Ruffini 1799)**.** *It is impossible to express solutions of general quintic equations $f(x) \in \mathbb{Q}[x]$, using the four arithmetical operations and extracting roots applied to the coefficients.*

Galois theory Let F be as before.

Definition 1.4. *Let $\alpha, \alpha' \in \mathbb{C}$. Then α and α' are called conjugates over F (or F-conjugates) if for all non zero polynomials $p(x)$ with coefficients in F, $p(\alpha) = 0$ iff $p(\alpha') = 0$.*

Remark 1.5. *(1) α and α' are $\mathbb{C}$-conjugate iff $\alpha = \alpha'$.*

(2) *α and α' are $\mathbb{R}$ conjugate iff $\alpha = \alpha'$ or $\alpha' = \overline{\alpha}$. Indeed, for conjugates $\alpha \neq \alpha'$, $p(x) = (x-\alpha)(x-\overline{\alpha})$ has α as root therefore $\alpha' = \overline{\alpha}$. On the other hand if for non zero $p(x) \in \mathbb{R}[x]$, we have $p(\alpha) = 0$, then $\overline{p(\alpha)} = 0$, but as the coefficients are in $\mathbb{R}$ we have $\overline{p(\alpha)} = p(\overline{\alpha}) = 0$.*

(3) *If α and α' are $\mathbb{R}$-conjugate then they are $\mathbb{Q}$-conjugate too. Therefore for any $f \in \mathbb{R}[x]$ such that there exists $\alpha \in \mathbb{C} \setminus \mathbb{R}$ such that $f(\alpha) = 0$, then $Sol(f)(\mathbb{C})$ has a non-trivial C_2 action.*

(4) *Note that α, α' are $\mathbb{R}$ (resp. $\mathbb{Q}$) conjugate such that $\alpha \in \mathbb{R}$ (resp. $\alpha \in \mathbb{Q}$), then $\alpha = \alpha'$.*

(5) *Note that $\sqrt{2}$ and $-\sqrt{2}$ are $\mathbb{Q}$-conjugate. Though they are not $\mathbb{R}$-conjugate.*

(6) *Let $f(x) = 1 + x + x^2 + x^3 + x^4 \in \mathbb{Q}[x]$. Using Eisenstein criteria and P.I.D porperty of $\mathbb{Q}[x]$ we know that any polynomial $g(x) \in \mathbb{Q}[x]$ vanishing on any root of $f(x)$ is divisible by $f(x)$. The complex roots of $f(x)$ are $\omega, \omega^2, \omega^3, \omega^4$, such that $\omega = e^{2\pi i/5}$. Using these observations we see that $Sol(f)(\mathbb{C})$ has cardinality 4 and all the elements are $\mathbb{Q}$- conjugate to each other. On the other hand ω, ω^4 and ω^2, ω^3 are $\mathbb{R}$-conjugate. So $\mathbb{Q}$-conjugate does not imply $\mathbb{R}$-conjugate.*

Therefore, we conclude that conjugacy over $\mathbb{Q}$ is more subtle than conjugacy over $\mathbb{R}$.

Definition 1.6. *Let $k \geq 1$ and let $\underline{z} := (z_1, \ldots, z_k) \in \mathbb{C}^k$ and $\underline{z}' := (z_1', \ldots, z_k') \in \mathbb{C}^k$. We say that $\underline{z}$ and $\underline{z}'$ are F-conjugate if for all non zero polynomials $p(t_1, \ldots, t_k) \in F[t_1, \ldots, t_k]$, $p(z_1, \ldots z_k) = 0$ iff $p(z_1', \ldots, z_k') = 0$.*

Example 1.7. (1) *$(z_1, \ldots, z_k)$ and $(\overline{z}_1, \ldots, \overline{z}_k)$ are $\mathbb{Q}$ and $\mathbb{R}$-conjugates.*

(2) *$(z_1, \ldots, z_k)$ is $\mathbb{C}$-conjugate to $(w_1, \ldots, w_k)$ iff $z_i = w_i$ for all i.*

(3) *$(\omega, \omega^2, \omega^3, \omega^4)$ is $\mathbb{Q}$-conjugate to $(\omega^4, \omega^3, \omega^2, \omega)$. It is non trivial to show that $(\omega, \omega^2, \omega^3, \omega^4)$ is $\mathbb{Q}$-conjugate to $(\omega^2, \omega^4, \omega, \omega^3)$. Using the polynomial $t_2 - t_1^2$ one can show that $(\omega, \omega^2, \omega^3, \omega^4)$ and $(\omega^2, \omega, \omega^3, \omega^4)$ are not $\mathbb{Q}$-conjugate. This shows that $(z_1, \ldots, z_k)$ and $(z_1', \ldots, z_k')$ are $\mathbb{Q}$-conjugate then z_i and z_i' are $\mathbb{Q}$-conjugate for every i. The converse is not true.*

Definition 1.8. *Let $f \in \mathbb{Q}[t]$ and $f \neq 0$. Let $\alpha_1, \ldots, \alpha_k$ be all the distinct roots of f in $\mathbb{C}$.*

$$Gal(f) := \left\{\sigma \in S_k | (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are } \mathbb{Q} \text{ conjugates}\right\}.$$

Remark 1.9. *Let f and α_i as above. Then for any $\sigma \in S_k$ we have an isomorphism of $\mathbb{Q}$-algebras $\sigma : \mathbb{Q}[t_1, \ldots t_k] \to \mathbb{Q}[t_1, \ldots, t_k]$, such that $\sigma(t_i) = t_{\sigma(i)}$. Consider the subfield of $\mathbb{C}$ denoted by $L := \mathbb{Q}(\alpha_1, \ldots \alpha_k)$ generated by α_i's and $\mathbb{Q}$. And consider the $\mathbb{Q}$ morphism $ev_f : \mathbb{Q}[x_1, \ldots x_k] \to L$, given by $ev_f(x_i) = \alpha_i$. One can show that this map is surjective. Then let $m = ker(ev_f)$. This m is a maximal ideal. Then for $\sigma \in Gal(f)$ iff $\sigma(m) = m$. This shows that $Gal(f)$ is indeed a group.*

Remark 1.10. (1) *If f has all rational roots then $Gal(f) = \{e\}$.*

(2) *If f is quadratic and non real roots then $Gal(f) = S_2$. If it has two distinct real roots non rational roots then also $Gal(f) = S_2$.*

Definition 1.11. *A complex number is called radical if it can be obtained from the rationals using only the four arithmetical operations and extracting n-th roots. A polynomial $f \in \mathbb{Q}[t]$ is said to be solvable by radicals if all its roots are radical.*

Theorem 1.12 (Galois)**.** *A polynomial $f \in \mathbb{Q}[t]$ is solvable by radicals if and only if $Gal(f)$ is a solvable group.*

2. Lecture 2 : Group Theory basics

Definition 2.1. *A group is a pair $(G, .)$, where G is a set and $. : G \times G \to G$ is a map of sets (binary operation) such that*

1. *$(x.y).z = x.(y.z)$ $\forall x, y, z \in G$,*
2. *$\exists e \in G$ such that $e.x = x.e = x$, $\forall x \in G$,*
3. *For any $x \in G$, $\exists x^{-1} \in G$, such that $x^{-1}.x = x.x^{-1} = e$.*

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

Remark 2.2.

1. *e is unique.*
2. *For any x, the inverse x^{-1} is unique.*
3. *Since $x.(y.z) = (x.y).z$, therefore for any $x_1, \ldots, x_n \in G$ we can inductively define $x_1.x_2 \ldots .x_n$. Therefore for any $x \in G$ we can define x^n for $n \geq 0$ ($x^0 = e$), and using inverse we can define $x^{-n} := (x^n)^{-1} = (x^{-1})^n$.*

Definition 2.3. *A ring is a triple (R, ϕ, ψ), where R is a set $\phi, \psi : A \times A \to A$ maps (we will denote $x + y := \phi(x, y)$ and $x.y := \psi(x, y)$) such that*

1. *$(R, +)$ is an abelian group. The identity element of this abelian group is denoted by 0.*
2. *(associativity of multiplication) $x(yz) = (xy)z$ for all $x, y, z \in R$*
3. *(Distributive property of multiplication over addition and vice versa) $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$ for all $x, y, z \in R$.*

A ring is called unital if there exists an element $1 \in R$ such that $x.1 = 1.x = x$ for all $x \in R$. A ring is called commutative if $xy = yx$ for all $x, y \in R$.

Definition 2.4. *A commutative unital ring $(R, +, .)$ is called a field if for any $x \neq 0$, there exists $y \in R$ such that $yx = xy = 1$*

Example 2.5.

1. *Let X be a set. The set $Bij(X) := \{f : X \to X | f \text{ bijection}\}$ is group where composition of functions is the composition law. This group will be denoted by S_X. If $X := \{1, 2, \ldots, n\}$, then S_X will be denoted by S_n.*
2. *Let n be a positive integer and $\mathbb{Z}/n\mathbb{Z}$ denote the set $\left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$. The operations $\bar{a} + \bar{b} := \overline{a + b(mod)n}, \bar{a}.\bar{b} := \overline{a.b(mod)n}$, makes $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$ an abelian group and $(\mathbb{Z}/n\mathbb{Z}, +, ., \bar{0}, \bar{1})$ a commutative unital ring.*
3. *(Exercise) Show that for a prime p, the commutative unital ring $\mathbb{Z}/p.\mathbb{Z}$ is a field.*
4. *Let F be a field then $F \setminus \{0\}$ is an abelian group under multiplication operation.*
5. *Let A be a ring M be A-module, then $Aut_{A-mod}(M)$, the set of A-module automorphisms of M forms a group, where composition of A-module homomorphism is the group operation.*

Loop Space Let X be a topological space and let $x \in X$ be a point. Let

$$\Omega_x(X) := \{f : [0, 1] \to X | f(0) = f(1) = x, f \text{ continuous}\}.$$

Let $f, g \in \Omega_x(X)$. Then define

$$g \circ f(t) := \begin{cases} f(2t), & 0 \leq t \leq 1/2 \\ g(2t-1), & 1/2 \leq t \leq 1 \end{cases}$$

Let $e : [0,1] \to X$ be the constant loop, that is $e(t) = x, t \in [0,1]$ and let for any $f \in \Omega_x(X)$ we define $f^{-1}(t) := f(1-t)$. Show the following

(1)
$$h \circ (g \circ f)(t) := \begin{cases} f(4t), & 0 \leq t \leq 1/4 \\ g(4t-1), & 1/4 \leq t \leq 1/2 \\ h(2t-1), & 1/2 \leq t \leq 1 \end{cases}$$

(2)
$$(h \circ g) \circ f(t) := \begin{cases} f(2t), & 0 \leq t \leq 1/2 \\ g(4t-2), & 1/2 \leq t \leq 3/4 \\ h(4t-3), & 3/4 \leq t \leq 1 \end{cases}$$

(3) Show that there exists a continous map $F : [0,1] \times [0,1] \to X$, Such that $F(0,t) = F(1,t) = x$ and $F(t',0) = h \circ (g \circ f)(t')$ and $F(t',1) = (h \circ g) \circ f(t')$.
(4) Show that $f \circ e \neq f$ in general similarly $e \circ f \neq f$ in general.
(5) Show that in all of these cases we have equality upto base point preserving homotopy.

Definition 2.6. *A subgroup H of a group G is a non-empty subset H of G such that if $x, y \in H$ then $x^{-1}y \in H$.*

Note that $H \subset G$ is a subgroup iff

(1) $e \in H$
(2) $x, y \in H$ implies $x.y \in H$
(3) $x \in H$ implies $x^{-1} \in H$.

Definition 2.7. *Let G and G' be groups. A map $f : G \to G'$ is called a group homomorphism if $f(x.y) = f(x).f(y)$ for all $x, y \in G$. For such a homomorphism f, define*

$$ker(f) := \{g \in G | f(g) = e_{G'}\},$$

$$Im(f) := \{h \in G' | \exists g \in G, f(g) = h\}.$$

A homomorphism $f : G \to G'$ is called an isomorphism if there exists $\tilde{f} : G' \to G$ homomorphism, such that $f \circ \tilde{f} = id_{G'}$ and $\tilde{f} \circ f = id_G$.

Remark 2.8. *(1) Let $x \in G$ and let $(x) := \{x^n | n \in \mathbb{Z}\}$. Then (x) is a subgroup of G. This subgroup is finite iff there exists $i \neq j$ such that $x^i = x^j$.*
(2) f is a homomorphism then $f(e_G) = e_{G'}$ and $f(x^{-1}) = f(x)^{-1}$.
(3) Note that $Im(f) \subset G'$ is a subgroup of G' and $ker(f) \subset G$ is a subgroup of G.
(4) Composition of homomorphism is a homomorphism.
(5) A homomorphism f is an isomorphism iff f is bijective.
(6) If $ker(f) = \{e_g\}$ then $f : G \to Im(f)$ is an isomorphism.
(7) Let $\psi : X \to Y$ be a bijection between two sets, then we get an isomorphism $S_Y \to S_X$ given by $h \mapsto \psi \circ h \circ \psi^{-1}$.

(8) *Let G be any group, define $l : G \to S_G$ (resp. $r : G \to S_G$) , by $l(g)(h) := g.h$ (resp. $r(g)(h) = h.g^{-1}$. Then l (resp. r) is an injective group homomorphism. Therefore, any group is a subgroup of a permutation group.*

(9) *Let $Aut(G)$ denote the group whose elements are isomorphisms $G \to G$ and group operation is given by composition of homomorphism. Consider the map $con : G \to Aut(G)$, given by $con(g)(h) := ghg^{-1}$. Then con is a group homomorphism and*

$$ker(con) = \{g \in G | gh = hg \forall h \in G\}.$$

This is called the center of the group G and it is denoted by $Z(G)$.

Definition 2.9. *A group G is called finite if $|G| < \infty$. For any group G and an element $g \in G$, $ord(g) := |(g)|$. A subgroup $N \subset G$ is called normal if $\forall g \in G, n \in N$ we have $gng^{-1} \in N$.*

Let $H \subset G$ be a subgroup. We define a relation on G as follows : $g_1 \sim g_2$ if $g_2^{-1}g_1 \in H$. This is an equivalence relation on G. Indeed, The following lemma is an exercise

Lemma 2.10. *(1) $g_1 \sim g_2$ iff $g_1 \in g_2.H$ iff $g_2 \in g_1H$ iff $g_1H = g_2H$.*

(2) For $g, g' \in g_1H$, we have $g \sim g'$. Therefore equivalence class of g is $g.H$.

(3) There is a natural bijection $H \to g.H$ given by $h \mapsto g.h$.

Proof. (1) If $g_1 \sim g_2$, then $g_1 \in g_2H$, also as H is a subgroup $(g_2^{-1}g_1)^{-1} = g_1^{-1}g_2 \in H$ so $g_2 \in g_1H$. Now $g_1.h = g_2.h'.h$ for some $h' \in H$. Therefore $g_1.H \subset g_2H$. Similarly one show that $g_2H \subset g_1H$. Now let $g_2H = g_1H$, then $g_2.e = g_2 \in g_1H$ and similarly $g_1 \in g_2H$. Then $g_2^{-1}g_1 \in H$.

(2) If $g, g' \in g_1H$, then $g = g_1.h_1, g' = g_1.h_2$. Therefore, $(g')^{-1}g = h_2^{-1}(g_1)^{-1}g_1h_1 = h_2^{-1}h_1 \in H$. Therefore $g \sim g'$. If $g' \sim g$, then by part 1, we get $g' \in g.H$ and every element of $g.H$ are equavalent to g. Therefore, $g.H$ is the equivalence class of g.

(3) The given map has an inverse given by $\alpha \mapsto g^{-1}.\alpha$.

□

The set of equivalence classes under this equivalence relation is denoted by G/H.

Corollary 2.11. *Let G be a finite group, then $|G| = |H||G/H|$. Therefore, for any $g \in G$, $ord(g)||G|$.*

Proof. Let G be any group and H subgroup. Then $G = \coprod_{[g.H] \in G/H} g.H$. Now H is bijective to $g.H$ for all $g \in G$. Therefore if G is finite then $|G| = |G/H||H|$. Now if $g \in G$ is an element. Then $o(g) = |(g)|$. Then the assertion follows.

□

Lemma 2.12. *Let p be a prime number and let $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$*

Proof. Let

$$(\mathbb{Z}/p\mathbb{Z})^* := \{a \in \mathbb{Z}/p\mathbb{Z} | \exists b \in \mathbb{Z}/p\mathbb{Z}, ab \equiv 1 \mod p\}.$$

Note that for any $1 \leq r < p$ integer there exists $a, b \in \mathbb{Z}$ such that $a.r + b.p = 1$. Therefore, for any $1 \leq r < p$ integer there exists $a \in \mathbb{Z}/p\mathbb{Z}$, such that $ar \equiv 1 \mod p$. Therefore,$(\mathbb{Z}/p\mathbb{Z})^*$ is a group (under multiplication mod p) of order $p - 1$. So for

any $a \neq 0 \bmod p$, we have order of $a \bmod p$ divides $p-1$, therefore $a^{p-1} \equiv 1 \bmod p$, on the other hand $a \equiv 0 \bmod p$, implies $a^p \equiv a \bmod p$.

□

3. Lecture 3

Theorem 3.1. *Let $N \subset G$ be a normal subgroup, then there is a well defined operation on G/N, given by $g_1N.g_2N := g_1g_2N$, making G/N a group and $\pi : G \to G/N$ given by $\pi(g) = gN$ a surjective group homomorphism. Moreove, G/N and $\pi : G \to G/N$ satisfies the following universal property : Let $f : g \to G'$ be any group homomorphism such that $N \subset ker(f)$, thene there exists a unique homomorphism $\bar{f} : G/N \to G'$ such that $\bar{f} \circ \pi = f$.*

Proof. If $g_1N = g_1'N$ and $g_2N = g_2'N$ then there exists $n_1, n_2 \in N$, such that $g_1' = g_1n_1$ and $g_2' = g_2n_2$.As N is normal we get

$$g_1'g_2' = g_1n_1g_2n_2 = g_1g_2g_2^{-1}n_1g_2n_2 = g_1g_2n,$$

for some $n \in N$. This shows the binary operation on G/N is well defined. The map π is a surjective group homomorphism with $ker(\pi) = N$ is left as an exercise. For the second part, it is clear that if $\bar{f}$ exists satisfying $\bar{f} \circ \pi = f$, then it is unique. The existence of $\bar{f}$ will follow if we can show for $g_1, g_2 \in G$ such that $g_1N = g_2N$, then $f(g_1) = f(g_2)$. But this is true beacuse, $g_1^{-1}g_2 \in N$, and $N \subset Ker(f)$, so $f(g_1)^{-1}f(g_2) = e_G'$.

□

Definition 3.2. *Let G be a group and X be a set. An action of G on X is a map $G \times X \to X$ $((g, x) \mapsto g.x)$ such that*

1. *$e.x = x$ for all $x \in X$*
2. *$(g_1g_2).x = g_1.(g_2.x)$ for all $g_1, g_2 \in G$.*

Example 3.3.

1. *Let G be a group and $X = G$. Then there are two actions corresponding to $l, r : G \to S_G$. The actiion corresponding l is $(g, x) \mapsto g.x$. (corresponding to r the action is $(g, x) \mapsto x.g^{-1}$).*
2. *Again G acts on itself via conjugation, i.e $(g, x) \mapsto gxg^{-1}$.*
3. *$G = S_n$, then G acts on $X = \{1, \ldots, n\}$, such that $(\sigma, i) \mapsto \sigma(i)$.*

Let G be a group and let X be a set. Let

$$Hom(G, S_X) := \{\phi : G \to S_X | \phi \text{ homomorphism } \},$$

and

$$A(G, X) := \{a : G \times X \to X | a \text{ is an action}\}.$$

Let $a \in A(G, X)$, then for any $g \in G$, the map $a(g, -) : X \to X$ given by $x \mapsto a(g, x)$ is a bijection where the inverse is given by $x \mapsto a(g^{-1}, x)$. This way we get a map $\phi_a : G \to S_X$, given by $\phi_a(g) = a(g, -)$. Now

$$\phi_a(g.h)(x) = a(g.h, x) = a(g, a(h, x)0 = \phi_a(g) \circ \phi_a(h)(x),$$

for all $x \in X$. Therefore, ϕ_a is a group homomorphism.

Proposition 3.4. *Let G be a group and X be a set. Then $a \in A(G, X) \mapsto \phi_a \in Hom(G, S_X)$, induces a bijection*

$$A(G, X) \to Hom(G, S_X).$$

Proof. Let $\phi : G \to S_X$ be a homomorphism, define $a_\phi : G \times X \to X$ as $a_\phi(g, x) := \phi(g)(x)$. Verify that $a_\phi \in A(G, X)$. Moreover, it is easy to verify that $a \in A(G, X) \mapsto \phi_a \in Hom(G, S_X)$ has an inverse the map $\phi \in Hom(G, S_X) \mapsto a_\phi \in A(G, X)$.

□

Isometry

Definition 3.5. *An isometry or rigid motion of $\mathbb{R}^n$ is a function $h : \mathbb{R}^n \to \mathbb{R}^n$ such that $||h(u) - h(v)|| = ||u - v||$, $\forall u, v \in \mathbb{R}^n$. The set of isometries of $\mathbb{R}^n$ is denoted by $Isom(\mathbb{R}^n)$.*

The identity map $Id : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry. composition of isometries is an isometry. For any vector $u \in \mathbb{R}^n$, the map $t_u : \mathbb{R}^n \to \mathbb{R}^n$ defined as $t_u(v) = v + u$. Then t_u is an isometry.

Proposition 3.6. *The following are equivalent conditions on a $n \times n$ matrix A.*

(1) A is orthogonal.
(2) For all $v, w \in \mathbb{R}^n$ we have $A(v).A(w) = v.w$
(3) Columns of A are mutually orthogonal unit vectors.

Proof. (1) $1 \implies 2$ $v^t w = v^t A^t A w = (Av)^t Aw$ as $A^t A = Id$.
(2) $2 \implies 1$. if $v^t A^t A w = v^t.w$ for all $v, w \in \mathbb{R}^n$, then $v^t(A^t A - Id)w = 0$ for all $v, w \in \mathbb{R}^n$. Therefore $B = (A^t A - Id) = 0$ by choosing $v = e_i$ and $w = e_j$.
(3) Let A_i be the i-th column of A. Then $A^t A = Id$, iff $A_i.A_j = \delta_{ij}$. This shows that 3 is euiqvalent to 1.

□

Proposition 3.7. *Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be a map. Then the following are equivalent*

(1) T is an isometry such that $T(0) = 0$ (fixing the origin).
(2) T preserves dot products.
(3) T is left multiplication by an orthogonal matrix.

Proof. (1) $1 \implies 2$. Indeed $(T(v) - T(w)).(T(v) - T(w)) = (v - w).(v - w)$. This will imply that $(v.v) = T(v).T(v)$. $3 \implies 1$ is obvious.
(2) $2 \implies 3$. We just have to show that T is a linear operator. Let $u, v \in \mathbb{R}^n$ and let $w = T(u) + T(v)$ and $w' := T(u + v)$. To show $w' = T(u) + T(v)$. Note that $w'.w' = (u + v).(u + v)$ as T preserves dot product.
Now

$$w'.w = w'.(T(u) + T(v)) = w'.T(u) + w'.T(v) =$$

$$= (T(u + v)).T(u)) + (T(u + v).T(v)) = (u + v).u + (u + v).v = (u + v)(u + v).$$

Similarly we have

$$w.w = w.(T(u) + T(v)) = (T(u) + T(v))(T(u) + T(v)) =$$

$$= T(u).T(u) + 2T(u).T(v) + T(v).T(v) = u.u + 2u.v + v.v = (u + v).(u + v).$$

Then $(w - w').(w - w') = w.w - 2w.w' + w'.w' = 0$. Therefore $w = w'$.

□

Definition 3.8. *Let R_n be a fixed regular n-gon. Then D_n is the set of isometries of $\mathbb{R}^2$ which maps R_n to itself.*

Lemma 3.9. *Let R_n be a regular polygon and let x_i, x_{i+1} be two neighbouring vertices of R_n. If P, Q two points on R_n such that $||P - x_i|| = ||Q - x_i||$ and $||P - x_{i+1}|| = ||Q - x_{i+1}||$, then $P = Q$.*

Proof. If P and Q satisfies the the condition of the lemma, then there exists circles C_1 centered at x_i with radius $||P - x_i||$ and C_2 centered at x_{i+1} with radius $||P - x_{i+1}||$, such that C_1 and C_2 intersects at P, Q. If $P \neq Q$, then P and Q lie on the opposite sides of the line joining x_i and x_{i+1}, which is absurd as R_n is convex.

□

Theorem 3.10. *The group D_n has $2n$ elements. In particular these are given by $r^i, 0 \leq i \leq n-1$, where r is rotation by angle $2\pi/n$ and reflections. If n is odd the n many reflections are given by reflections wrt to the lines joining a vertex with the midpoint of the opposite side. If n is even, there are $n/2$ reflections wrt the lines joining opposite vertices (diagonals) and $n/2$ relections wrt the lines joining midpoints of the opposite edges.*

Proof. Since rotations does not fix anything on R_n, therefore, no reflection is a rotation and no rotation is a reflection. The reflections listed above have different fixed points , therefore, the n reflections we get are distinct. Therefore $|D_n| \geq 2n$. Let $f \in D_n$. Then f maps vertices to vertices as f preserves distance and the vertices are the only points with a fixed distance with the origin. Moreover neighboring vertices gets mapped to neighbouring vertices. Now let x_1 and x_2, two neighbouring vertex and let $f(x_1) = y_1$ and $f(x_2) = y_2$. Then $P \in R_n$ is uniquely determined by its distance with x_1, x_2. As f preserves distance, $f(P)$ is completely determined by y_1 and y_2. So therefore there are n choices for $f(x_1)$ and after fixing $f(x_1)$ there are only two choices for $f(x_2)$. This shows that $|D_n| \leq 2n$.

□

Corollary 3.11. *Let $r \in D_n$ be the counterclockwise rotation by angle $2\pi/n$ and let s be any reflection. Then $srs = r^{-1}$. Therefore, the n reflections are given by $s, rs = sr^{-1}, \ldots, r^{n-1}s = sr^{-n+1}$.*

Proof. Hint : To show $srs = r^{-1}$ it is enough to show what RHS and LHS does to any neighbouring vertices. Let l be the line of reflection of s. Then s intersects the midpoint of a side (irrespective of parity of n). Choose the vertices of that side and see what happens.

□

Reflections and rotations

Example 3.12. *Let $f \in Isom(\mathbb{R}^2)$ such that $f(0) = 0$. Then f is given by one of the following matrices*

(1) (Rotation) Counter clockwise rotation by angle θ.

$$\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}$$

(2) (Reflection) Reflection across the line through the origin at angle $\theta/2$.

$$\begin{bmatrix} cos\theta & sin\theta \\ sin\theta & -cos\theta \end{bmatrix}$$

Definition 3.13. *Let G be a group acting on a set X and let $x \in X$.*

$$O_x := \{y \in X | g.x = y \text{ for some } g \in G\}.$$

$$Stab(x) := \{g \in G | g.x = x\}.$$

Remark 3.14. *Let G be a group acting on X. Define a relation on X by $x \sim y$ iff $\exists g \in G$ such that $y = g.x$. This is an equivalence relation and the equivalence class of x is precisely O_x. We will denote by X/G the set of equivalences classes.*

Theorem 3.15. *Let G be a group acting on a set X, and let $x \in X$. Then $\psi : O(x) \to G/Stab(x)$ such that $y = g.x \mapsto g.Stab(x)$, is a well defined bijection. Therefore when G is finite, we get*

$$|O_x|.|Stab(x)| = |G|.$$

Proof. If $y = g_1.x = g_2.x$, then $g_2^{-1}g_1.x = x$, therefore $g_2^{-1}.g_1 \in Stab(x)$. This implies $g_1.Stab(x) = g_2.Stab(x)$. Therefore ψ is well defined. Surjective of ψ is obvious. If $\psi(y_1) = \psi(y_2)$ and $y_1 = g_1x$ and $y_2 = g_2x$, then $g_2^{-1}g_1 \in Stab(x)$, so $y_2 = g_2.g_2^{-1}g_1x = g_1x = y_1$.

□

4. Lectures 4-5-6

Example 4.1. *(1) Let $p : E \to X$ be a covering space of a topological space X. Let $x \in X$ and let*

$$S := p^{-1}(x) := \{y \in E | p(y) = x\}.$$

Let $G = \pi_1(X, x)$. Then $f \in G$, there exists a continuous map $f : [0,1] \to X$, such that $f(0) = f(1) = x$. Let $y \in S$. Then there exists a unique $g : [0,1] \to E$ continuous such that $g(0) = y$ and $p \circ g = f$. Therefore, $g(1) \in S$. If f and f' are (base point preserving) homotopic and let g' be alift of f' such that $g'(0) = y$, then $g(1) = g'(1)$ by unique homotopy lifting. This gives an action $G \times S \to S$. Let $p_* : \pi_1(E, y) \to \pi_1(X, x)$ be the induced homomorphism for $y \in S$. Then $Stab(y) = Image(p_*)$. If E is connected then $O_y = S$

(2) Let

$$Gr(k, n) := \{V \subset \mathbb{R}^n | subspace\ , dim(V) = k\}.$$

The group $G = GL_n(\mathbb{R})$ acts on $Gr(k, n)$ in the following way $(T, V) \mapsto T(V)$ where $T \in GL_n(\mathbb{R})$ and $V \in Gr(k, n)$. For $k = 1$, and $l \in Gr(1, n)$,

$$Stab(l) = \{T \in GL_n(\mathbb{R}) | T(v) = \lambda.v, |v| = 1, \lambda \in \mathbb{R}, v \in l\}.$$

Definition 4.2. *Let G be a group acting on a set X and let $g \in G$.*

$$X^g := \{x \in X | gx = x\}.$$

$$X^G := \{x \in X | gx = x, \forall g \in G\}.$$

Lemma 4.3. *Let G be a group acting on a set X and let $x, y \in O_z$ for $x, y, z \in X$, then $Stab(x) \cong Stab(y) \cong Stab(z)$.*

Proof. As x, y is in same orbit, therefore there exist $g \in G$ such that $g.x = y$. Let $\phi : Stab(x) \to Stab(y)$ given by $\phi(h) = ghg^{-1}$. Note that $ghg^{-1}(y) = gh(x) = gx = y$. So we get the required homomorphism, whose inverse is given by $t \mapsto g^{-1}tg$.

□

Theorem 4.4. *Let G be a finite group acting on a finite set X. Then*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proof. Let $A \subset X \times G$ such that $A := \{(x,g)|g.x = x\}$. Then $A = \coprod_{g\in G} X^g \times g = \coprod_{x\in X} x \times Stab(x)$. Note that $X = \coprod_{[x]\in X/G} O_x$. Then

$$|A| = \sum_{g\in G}|X^g| = \sum_{x\in X} x \times Stab(x) =$$

$$= \sum_{[x]\in X/G}\sum_{y\in O_{[x]}}|Stab(y)| = \sum_{[x]\in X/G}|O_{[x]}|.|Stab([x])| = \sum_{[x]\in X/G}|G| = |X/G| \times |G|.$$

□

Definition 4.5. *Let G be a finite group acting on a finite set X and let $O_{x_1}, \ldots, O_{x_n}$ be the distinct non-trivial orbits.*

Then

$$|X| = |X^G| + \sum_{i=1}^{n}|O_{x_i}|.$$

If G acts on $X = G$ by conjugation action and let $O_{g_1}, \ldots, O_{g_n}$ be the distinct non-trivial orbits. Then the above equation becomes

$$|G| = |Z(G)| + \sum_{i=1}^{n}|O_{g_i}|.$$

Lemma 4.6. *Let G be a group of order p^n, then the center $Z(G)$ is non-trivial.*

Proof. If G is abelian then we are done. If not then $Z(G) \neq G$. Consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{n}|O_{g_i}|.$$

Now the orbits O_{g_i} are non trivial as $Z(G) \neq G$. Therefore $Stab(g_i) \neq G$ and this shows that $p||O_{g_i}|$ for all i. Therefore $p||Z(G)|$.

□

Theorem 4.7 (Cauchy's theorem)**.** *Let G be a finite group and p be a prime number such that $p||G|$. Then G has an element of order p.*

Proof. Let

$$X = \{(g_1, \ldots, g_p) \in G^p | g_1.g_2 \ldots g_p e\}.$$

Then $|X| = |G^{p-1}|$ (as the first $p-1$ elements uniquely determines the last). So $|X|$ is divisible by p. Now $g_1.g_2 \ldots g_p = e$ implies $g_p.g_1.g_2 \ldots g_{p-1} = e$. Therefore C_p acts on X via cylic permutation. So, the size of the orbits are p or 1. Now, $(e, e, \ldots, e)$ has orbit size 1. Therefore, there has to be another elemnt $(g_1, \ldots, g_p)$ whose orbit size is 1 as $p||X|$. An elemnt $(g_1, \ldots g_p)$ has orbit size one iff $g_i = g_j = g$ for all $i \neq j$ and $g^p = 1$.

Another proof By induction on $|G|$. If $|G| = p$, then nothing to show. If G is abelian let $g \in G$ an elment of order not divisible by p, then $G/(g)$ is a smaller group which is divisible by p and therefore has an elemnt of order p say $x(g)$. Then $x^p \in H$ and if x has order m then $x^m = e$ implies $(x(g))^m = (g)$ or $p|m$ and

therefore there exists an element of order p. The claim for p divides order of g is same.

If G is not abelian, and if $|Z(G)|$ is divisible by p then we are done by previous steps. Else, there exists as non central element whose cardinaly of conjugacy class is not divisible by p. Threfore, there exists a non trivial subgroup (namely the stablizer of non central element) whose cardinality is divisible by p. Now induction applies.

□

Example 4.8. *(1) Let G be a group and let $n||G|$ and let X be the set of all order n subgroups of G. Then G acts on X by conjugation, i.e. $(g, H) \mapsto gHg^{-1}$. Then*

$$Stab(H) = \left\{g \in G | gHg^{-1} = H\right\} := N_G(H),$$

it is called the normaliser of H in G. Note that H is a normal subgroup of $N_G(H)$. Note that orbit of a subgroup H under this action is trivial iff H is normal.

(2) Let G be a finite group and

$$X := \{(x_1, \ldots, x_n) \in G^n | x_1.x_2 \ldots x_n = e\}.$$

The cyclic group C_n of order n acts on G^n as cyclic premutation. Let $x := (g_1, \ldots, g_n) \in X$. Then $|O_x| = 1$, iff all the g_i's are equal to say g and $g^n = e$.

Definition 4.9. *Let G be a group and p-prime.*

(1) A group of order p^k for some $k \geq 1$ is called a p-group. A subgroup of order p^k for some $k \geq 1$ is called a p-subgroup.

(2) Let $|G| = p^n.m$ such that $(p, m) = 1$, then a subgroup of order p^n is called a Sylow p-subgroup of G.

$$Syl_p(G) := \quad \text{the set of Sylow } p - \text{subgroups of } G.$$

Theorem 4.10 (Sylows Theorem)**.** *$|G| = p^n.m$ and $(p, m) = 1$.*

(1) $Syl_p(G) \neq \Phi$.

(2) Let $P_1, P_2 \in Syl_p(G)$, then $\exists g \in G$ such that $P_2 = gP_1g^{-1}$. Therefore $n_p(G) = |G|/|N_G(P)|$, where $P \in Syl_p(G)$.

(3) Every p-subgroup of G is contained inside a Sylow p-subgroup.

(4) $n_p(G) \equiv 1 \mod p$.

Proof. (1) By induction on $|G|$. The case $|G| = 1$ is trivially true. Suppose we know that for all groups of cardinality $k < n$ and any prime p such that $k = p^a.b$ such that $(p, b) = 1$, we have a Sylow p-subgroup. Let $|G| = n$ and p be a prime mentioned in the statement of the theorem.

Case 1 : $p \nmid |Z(G)|$

Then using the class equation, we see that there exists a non trivial conjugacy class (i.e. non trivial orbit) not divisible by p. By orbit stabiliser theorem, this implies there exists an element $g \in G$ such that $C(g) \neq G$ and $p^n \mid |C(g)|$. Then we are done using induction.

Case 2:

$p \mid |Z(G)|$

Cauchy's theorem tells us that there is an element $h \in Z(G)$ of order p. Therefore, the cyclic subgroup generated by h, say H, is of order p. As every element of H commute with every element of G, H is a normal subgroup of G. The group G/H has cardinality $p^{n-1}.m$ and by induction there exists Sylow p-subgroup $\bar{P}$ of G/H, such that $\bar{P} = \pi(P)$ for a subgroup P of G containing H (infact $P := \pi^{-1}(\bar{P})$), where $\pi : G \to G/H$ is the canonical quotient homomorphism. Therefore, P is a Sylos p- subgroup of G.

(2) We have to show that the conjugation action of G on $Syl_p(G)$ is transitive. Let $P_1, Q \in Syl_p(G)$, and let $O_{P_1} = \{P_1, \ldots, P_l\}$ be the disntinct elements of the conjugacy classes of P_1. We want to that $Q \subset N_p(P_k)$ for some k. For that we note the following.
p ∤ l :
Indeed, if $p \mid l$, then $l = |O_{P_1}| = \frac{|G|}{|N_G(P_1)|}$ implies that $p \mid \frac{|G|}{|P_1|}$. This contradicts the fact that P_1 is a Sylow p-subgroup.

Note that Q acts on O_{P_1} and as $p \nmid l$, there exists atleast one orbit of this action of size not divisible by p. Assume that this happens for P_k, i.e $p \nmid \frac{|Q|}{|N_Q(P_k)|}$. As $|Q|$ is p-group, this implies $Q = N_Q(P_k) = N_G(P_k) \cap Q$. This implies $Q \subset N_G(P_k)$. Now $H := N_G(P_k)/P_k$ is a group (P_k is normal subgroup of $N_G(P_k)$) whose order is not divisible by p as P_k is a Sylow p-subgroup, and therefore $Q \subset ker(\pi) = P_k$, where $\pi : N_G(P_k) \to N_G(P_k)/P_k$ is the canonical group homomorphism. Therefore, $Q = P_k$.

(3) First note the following claim :
Let P be a Sylow p-subgroup and Q be a any p-subgroup, then $Q \cap P = Q \cap N_G(P)$.
It is clear that $Q \cap P \subset Q \cap N_G(P) =: H$, and H is a either trivial or a p-subgroup again. Again $N_G(P)/P$ is not a p-group as P is a Sylow p-subgroup. Therefore like the previous proof $H \subset P$. It is clear that $H \subset Q$, so $H \subset P \cap Q$. This settles the claim.

Let H be any p-subgroup of G and let it act on $Syl_p(G)$ via conjugation. Then , we know by the previus part that $p \nmid n_p(G)$. Therefore, there exists atleast one orbit of size not divisible by p. This implies $p \nmid \frac{|H|}{|N_H(P_i)|}$ for some $P_i \in Syl_p(G)$. As the groups in question are all p-groups, therefore $\frac{|H|}{|N_H(P_i)|} = 1$ or $H = N_H(P_i) = H \cap N_H(P_i) = H \cap P_i$ and we are done.

(4) Let $P_1 \in Syl_p(G)$ act on $Syl_p(G)$ by conjugation. Thne the orbit of P_1 is the Sylow-p subgroup P_1. If $P_j \in Syl_p(G)$ and $P_j \neq P_1$, then orbit of P_j under this action is of the size

$$[P_1 : N_{P_1}(P_j)] = [P_1 : P_1 \cap N_G(P_j)] = [P_1 : P_1 \cap P_j],$$

and the size of the orbit is a non trivial power of p. Therefore $n_p(G) = 1 + k.p$ for some positive integer k.

□

Definition 4.11. *A permutation $\sigma \in S_n$ is called a k cycle for $k \leq n$, if there exists k distinct elements $a_1, a_2, \ldots, a_k \in [n]$, such that $\sigma(a_i) = a_{i+1 \ mod \ k}$ for all i and $\sigma(x) = x$ for all $x \in [n] \backslash \{a_1, \ldots, a_k\}$. In this case we write $\sigma = (a_1 \ a_2 \ \ldots \ a_k)$. The set $\{a_1, \ldots, a_k\}$ is called the underlying set of σ and is denoted by S_σ.*

Lemma 4.12. *If $\sigma = (a_1\ a_2\ \dots\ a_k)$, then k is the least positive integer such that $\sigma \circ \sigma \circ \dots \sigma := \sigma^k = e$.*

Proof. We claim that $\sigma^i(a_j) = a_{j+i \bmod k}$ and $\sigma^i(x) = x$ for all $x \in [n] \setminus \{a_1, \dots, a_k\}$. We prove this by induction. For $i = 1$ this is the definiton. Let the claim hold for $j < i$. Now

$$\sigma^i(a_j) = \sigma(\sigma^{i-1}(a_j)) = \sigma(a_{j+i-1 \bmod k}) = a_{j+i \bmod k}.$$

This shows that $\sigma^l(a_1) = a_1$ then $l \geq k$, and $\sigma^k(a_j) = a_j$ for all j. Therefore the lemma follows.

□

Example 4.13. *(1) Let $\sigma = (12)(34) \in S_4$ be the permutation such that*

$$\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 3.$$

Then σ is not a k-cycle.
(2) Let $\sigma = (13)(12)$, then $\sigma = (123)$.

Lemma 4.14. *Let $\sigma \in S_n$, be a k cycle given by $\sigma = (a_1\ a_2\ \dots\ a_k)$, then*

$$\sigma = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2).$$

Proof. Let $x \notin \{a_1, \dots, a_k\}$, then

$$x = \sigma(x) = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2)(x).$$

Now for $i < k$, we have $\sigma(a_i) = a_{i+1}$ and $\sigma(a_k)a_1$. But

$$((a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2))(a_k) = ((a_1\ a_k))(a_k) = a_1,$$

and for $i < k$ we have

$$((a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2))(a_i) = ((a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_{i+1})(a_1\ a_i))(a_i) =$$

$$= ((a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_{i+1}))(a_1) = ((a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_{i+2}))(a_{i+1}) = a_{i+1}.$$

□

Definition 4.15. *A permutation $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_l$ such that σ_i is a k_i-cycle and $S_{\sigma_i} \cap S_{\sigma_j} = \Phi$ is called a composition of dsijoint cycles. Such a permutation is called a permutation of type $(k_1, \dots, k_l)$.*

Proposition 4.16. *Every $\sigma \in S_n$ is a unique composition of disjoint cycles.*

Proof. Indunction on n. The case $n = 2$ is obvious. Let $\sigma \in S_n$. Consider the set $A_1 := \{\sigma^i(1)\}$. If $A_1 = [n]$, then $\sigma = (1\ \sigma(1) \dots\ \sigma^{n-1}(1))$. Otherwise $|A_1| < n$ and $\sigma = \sigma' \circ (1\ \sigma(1) \dots\ \sigma^j(1))$. Sucha that σ' only premutes A_1^c. Therefore by induction σ' can be decomposed.

□

Lemma 4.17. *Let $(G, ., e)$ be a group and let $g, h \in G$, such that $g.h = h.g$ and both g and h has finite order. Then $g.h$ has finite order and $o(g.h)|lcm(o(g), o(h))$. Moreover, if $gcd(o(g), o(h)) = 1$, then $o(g.h) = o(g).o(h)$.*

Proof. First we claim that $h^i.g = gh^i$, whenever $g.h = h.g$. We prove this by induction on i . the case $i = 1$ is the relation $g.h = h.g$. Now

$$h^i g = h^{i-1}.h.g = h^{i-1}g.h = g.h^{i-1}.h = g.h^i.$$

Therefore, whenever $g.h = h.g$, we have $g^i.h^j = h^j.g^i$. We claim that $(g.h)^i = g^i.h^i$ for any $i \in \mathbb{N}$. We prove it by induction on i. The case $i = 1$ follows trivially. Now

$$(g.h)^i = (g.h)^{i-1}.g.h = g^{i-1}.h^{i-1}h.g = g^{i-1}.g.h^i = g^i.h^i.$$

Let $k = lcm(o(g), o(h))$, then $o(g), o(h)|k$. This implies

$$(g.h)^k = g^k.h^k = e.e = e.$$

Therefore $o(g.h) \leq k$, infact $o(g.h)|k$. Since $(g.h)^i = e$, then

$$e = (g.h)^{i.o(g)} = (g.h)^{i.o(h)}.$$

Therefore, $h^{i.o(g)} = g^{i.o(h)} = e$. This implies $o(h)|i.o(g)$ and $o(g)|i.o(h)$. Now let, $gcd(o(g), o(h)) = 1$. Then $o(h)|i$ and $o(g)|i$. Therefore, $o(h).o(g)|i$. This gives the result.

□

Definition 4.18. *Let $\sigma \in S_n$ be a premutation. The fixed set of σ is defined as follows*

$$F_\sigma := \{i \in [n] | \sigma(i) = i\}.$$

Two premutations $\sigma, \tau \in S_n$ is called disjoint permutations if

$$(F_\sigma)^c \cap (F_\tau)^c = \Phi.$$

Remark 4.19. *If σ and τ are disjoint permutations, then σ^i and τ^j are disjoint too.*

Lemma 4.20. *Let $\sigma, \tau \in S_n$, be disjoint permutations. Then $\sigma \circ \tau = \tau \circ \sigma$. Moreover, $o(\sigma \circ \tau) = lcm(o(\sigma), o(\tau))$.*

Proof. Let $i \in [n]$, then i is fixed by atleast one of σ or τ. WLOG, $i \in F_\sigma$, then $\tau(i) \in F_\sigma$ too. Therefore, $(\tau \circ \sigma)(i) = \tau(i) = (\sigma \circ \tau)(i)$. Therefore, we get our first claim. Note that for σ, τ disjoint cycles, such that $\sigma \circ \tau = e$, then $\sigma = e$ and $\tau = e$. Indeed, let $i \notin F_\sigma$, then $i \in F_\tau$, $i = \sigma \circ \tau(i) = \sigma(i)$, which is a contradiction. Therefore $[n] = F_\sigma$, similarly $[n] = F_\tau$.

Now , as $\sigma \circ \tau = \tau \circ \sigma$, therefore $o(\sigma \circ \tau)|lcm(o(\sigma), o(\tau))$. Let i be a positive integer such that $(\sigma \circ \tau)^i = e$, then $\sigma^i \circ \tau^i = e$. As σ^i and τ^i are disjoint, therefore $\sigma^i = e = \tau^i$. Therefore, $o(\sigma)|i$ and $o(\tau)|i$. Therefore, $lcm(o(\sigma), o(\tau))|i$. This shows that $lcm(o(\sigma), o(\tau))|o(\sigma \circ \tau)$.

□

Remark 4.21. *$g.h = h.g$ in a finite group G does not imply $o(g.h) = lcm(o(g), o(h))$ in general.*

Lemma 4.22. *Following are true in S_n*

(1) $(a\ b)(a\ b) = e$.
(2) $(a\ b)(c\ d) = (c\ d)(a\ b)$.
(3) $(a\ b)(b\ c) = (b\ c)(a\ c)$.
(4) $(a\ b)(a\ c) = (b\ c))(a\ b)$.

Proof. First two is obvious.

$$(a\ b)(b\ c)(a) = b = (b\ c)(a\ c)(a),$$
$$(a\ b)(b\ c)(b) = c = (b\ c)(a\ c)(b),$$
$$(a\ b)(b\ c)(c) = a = (b\ c)(a\ c)(c).$$

Similarly the last one can be checked. □

Proposition 4.23. *If $e = \tau_1 \dots \tau_n$ such that τ_i are transpositions. Then n is even.*

Proof. We will prove this by induction.For $n = 1$, e canot be a transposition. For $n = 2$, we get the result. Now let $n > 2$ and $e = \tau_1 \dots \tau_n$ such that τ_i are transpositions. Let $\tau_n = (a_1, b_1)$.

Step 1 :

If $\tau_{i-1}\tau_i = e$ for some i, then we get e as a length $n-2$ composition of transpositions. By induction, this implies that $n-2$ is even therefore n is even.

Step 2 : Otherwise , choose the first transposition from right having b_1, say τ_i and use lemma 4.22 to get $e = \sigma_1 \dots \ \sigma_{n-1}\sigma_n$, such that $\sigma_j = \tau_j$ for $j < i-1, j > i$ and σ_{i-1} is a transposition premuting b_1 and σ_i is a transposition fixing b_1.

If after applying Step 2, the condition of Step 1 is not satisfied then we apply Step 2 again until we satisfy Step 1 condition otherwise we reach a stage such that $e = \sigma_1 \dots \sigma_n$, such that σ_i's are trasnpositions and only σ_1 permutes b_1. This is not possible as e fixes b_1, but $\sigma_1 \dots \sigma_n$, such that σ_i's are trasnpositions and only σ_1 permutes b_1, does not fix b_1. So Step 1 condition is verified at some intermediate stage and therefore we get the result from Step 1.

□

Theorem 4.24. *Let $\sigma = \sigma_1 \dots \sigma_m = \tau_1 \dots \tau_n$, such that σ_i, τ_i's are transpositions. Then either m, n are both even or m, n are both odd.*

Proof. Note that in any group $(g.h)^{-1} = h^{-1}.g^{-1}$. Also note that if τ is a transposition then $\tau^{-1} = \tau$. Therefore, $\sigma = \sigma_1 \dots \sigma_m = \tau_1 \dots \tau_n$ implies that

$$e = \tau_n \tau_{n-1} \dots \tau_1 \sigma_1 \dots \sigma_m.$$

By previous proposition, this implies $m+n$ is even. Therefore, the theorem follows. □

Definition 4.25. *A permutation is called even if it can be written as composition of even number of permutations otherwise it is called odd. The set of even permutation in S_n is denoted by A_n. Let Odd_n, denote the set of odd premutations.*

Remark 4.26. *The cardinality of A_n is $n!/2$.*

Definition 4.27. *A subgroup $G \subset S_n$ is called transitive if the induced action of G on $\{1, 2, \dots, n\}$ is transitive.*

Lemma 4.28.
(1) Let $p \in S_n$ and $\sigma = (123)$, then $p\sigma p^{-1} = (p(1)p(2)p(3))$. If $\sigma = (123)(47)$ then $p\sigma p^{-1} = (p(1)p(2)p(3))(p(4)p(7))$.
(2) Show that two premutations $\sigma, \tau \in S_n$ are conjugate to each other iff they have the same cycle type.

Proof. Exercise. □

Lemma 4.29. *Let p bea prime and let G be a trnasitive subgroup of S_p. Then any normal subgroup $H \neq \{e\}$ of G is again a transitive subgroup.*

Proof. Let H act on $[p]$. Let $i, j \in [p]$ and let O_i and O_j be orbits under this action. Now there exists $\sigma \in G$ such that $\sigma(j) = i$. Let $x \in O_j$, then $x = h.j$ for some $h \in H$. Then $\sigma(x) = \sigma \circ h(j)$. As H is normal therefore there exists $h' \in H$ such that $\sigma \circ h = h' \circ \sigma$. So $\sigma(x) = h' \circ \sigma(j) = h'(i)$, so $\sigma O_j \subset O_i$. Similarly $O_i \subset \sigma O_j$. So O_i is in bijection with O_j for all i, j. This implies $p = m.|O_i|$ for any i. Note that if all $h \in H$ fixes all $i \in [p]$. Then $H = \{e\}$. Therefore $|O_i| > 1$. This implies $|O_i| = p$. Therefore H is a transitive subgroup. □

Proposition 4.30. *Any transitive subgroup G of S_p containing a transposition is the whole group S_p.*

Proof. Let $H \subset G$ be the subgroup generated by transpositions in G. Then $H \neq \{e\}$.Note that for any $\tau \in H$, $\tau = \tau_1 \circ \dots \tau_k$, τ_i transpositions in G. Then for any $g \in G$ we have $g\tau g^{-1} = g\tau_1 g^{-1} \circ \dots g\tau_k g^{-1}$ and $g\tau_i g^{-1}$ is again a transposition in G. Therefore, H is normal subgroup of G. Previous lemma implies that H is a therefore a transitive subgroup of G. Assume, WLOG, that $(1,2) \in H$ and suppose all $(1,j) \in H$, where $2 \leq j \leq q$. Note that $(1,i)(1,j)(1,i) = (i,j)$ and transpositions generate S_p. Therefore, it is enough to show $p = q$. Let $\sigma \in H$ such that $\sigma(1) = p$ and $\sigma = \tau_1 \circ \dots \tau_l$. It is not possible that all τ_i keeps the set $[q] := \{1, \dots q\}$ invariant as their somposition is σ which does not keep $[q]$, invariant. Therefore, one of the τ_k is $\tau_k = (i,j)$, such that $i \leq q$ and $q < j$. Then $(1,i)(i,j)(1,i) = (1,j) \in H$. Therefore $p = q$. □

Remark 4.31. *(1) Find out the class equations of S_3 and S_4.*

(2) Let $\sigma \in A_n$. Let $C_A(\sigma)$ and $C_S(\sigma)$ denote the conjugacy classes of σ in A_n and S_n respectively. Let $Stab_A(\sigma)$ and $Stab_S(\sigma)$ be the stabilizer of σ in A_n and S_n respectively. Then $|C_S(\sigma)||Stab_S(\sigma)| = |S_n|$ and $|C_A(\sigma)|.|Stab_A(\sigma)| = |A_n|$. Therefore, $|C_A(\sigma)|.|Stab_A(\sigma)| = 1/2|C_S(\sigma)||Stab_S(\sigma)|$. Note that $Stab_A(\sigma) \subset Stab_S(\sigma)$. If $Stab_A(\sigma) = Stab_S(\sigma)$, then $C_A(\sigma) = 1/2C_S(\sigma)$ (in A_n conjugacy class of σ splits into halves). So if $C_S(\sigma)$ is odd then it this is not possible. If $Stab_A(\sigma) \neq Stab_S(\sigma)$ then the conjugacy classes remain same as $|Stab_A(\sigma)| = 1/2|Stab_S(\sigma)|$.

(3) Class equation of S_5 is $120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$. The 10 and 30 belongs to odd permutation, therefore they do not contribute to the class equation of A_5. The number of permutations of cycle type $(2,2,1)$ is 15, which is odd number so they can not split in halves. As 24, the number of premutation of cycle type (5) does not divide the cardinality of A_5, it must split into halves. The conjugacy classes of cycle type $(3,1,1)$ contains the 3 cycle (123) and they give 20 many elements of S_5. But the odd premutation $(45) \in Stab_S((123))$, therefore $C_A(123) = C_S(123)$. Therefore, the class equation of A_5 is $60 = 1 + 15 + 20 + 12 + 12$.

Definition 4.32. *A group G with no non trivial normal subgroup is called a simple group.*

Remark 4.33. *(1) Simple abelian groups are precisely the groups $\mathbb{Z}/p\mathbb{Z}$ for p a prime. Indeed, Let G be an abelian group and let $g \neq e$. If $(g) \neq G$, thene this is a non trivial normal subgroup so G is not simple. If $G = (g)$, and $o(g)$ is not prime or infinite. In both cases we will get non trivial normal subgroups.*

(2) The group A_5 is simple. The class equation of A_5 gives us that there are 1 conjugacy class of size 1 (type $(1,1,1,1)$), size 20 (type $(3,1,1)$), size 15 (type $(2,2,1)$), and 2 conjugacy classes each having size 12 (type (5), classes $[(12345)]$ and $[(13524)]$. Any normal subgroup of A_5 contains the conjugacy class of size 1, plus whole conjugacy classes for some of the non trivial conjugacy classes. Also the cardinality of the normal subgroup must divide 60. This is not possible unless the normal subgroup is one of the trivial normal subgroups.

(3) *Let G be a group*

$$G^1 := [G,G] :=< \left\{ghg^{-1}h^{-1} | g,h \in G\right\} >,$$

is the commutator subgroup of G. It is normal in G, and $G^{ab} := G/G^1$ is an abelian group such that any homormorphism $\phi : G \to A$, with A an abelian group uniquely factors through $G \to G^{ab}$. If G is simple non abelian then $G = G^1$, if G is abelian then $G^1 = \{1\}$.

Remark 4.34. *(1) We see that for any prime $p \mid |G|$, $n_p(G) = \frac{|G|}{|N_G(P)|}$ for any $P \in Syl_p(G)$. As $P \subset N_P(G)$, therefore $n_p(G)$ can not have a power of p divisor but it divides $|G|$. Threfore $n_p(G)||G|/p^n$, where $|G| = p^n.m$ with $(p,m) = 1$.*

(2) *A Sylow p-subgroup P is normal iff it is the unique Sylow p-subgroup iff $n_p(G) = 1$ as all the Sylow p-subgroup are conjugate to each other and all conjugates of a Sylow p-subgroup is again a Sylow p-subgroup.*

(3) *If G is abelian and p be a prime dividing $|G|$, then $n_p(G) = 1$.*

(4) *Sylow p subgroup and Sylow q-subgroup for $p \neq q$ have trivial intersection.*

(5) *Let $|G| = p.q$ where p, q primes and $p < q$. Then G has exactly one subgroup of order q, which is therefore normal. Indeed, $n_q|p$, and $n_q \equiv 1 \mod q$. Therefore $n_q = 1$.*

(6) *Let $|G| = 12$. Then either G has normal Sylow 3-subgroup or else it is isomorphic to A_4.*

Proof. We know $n_3|4$ and $n_3 \equiv 1 \mod 3$. So $n_3 = 1 or 4. n_3 = 1$ gives the first condition. If $n_3 = 4$. Then $|Syl_3(G)| = 4$ and the conjugation action of G on $Syl_3(G)$ is transitive. This action gives a group homomorphism $\phi : G \to S_4$. Note that

$$ker(\phi) = \left\{g \in G | g \in \cap_{i=1}^4 N_G(P_i)\right\}.$$

Alos note that $|N_G(P_i)| = 12/n_3 = 3$. Therefore $N_G(P_i) = P_i$. But $P_i \cap P_j = \{e\}$ as they are disctinct subgroups of prime cardinality. Therefore ϕ is injective. So $im(\phi)$ as a subrgoup of S_4 is of order 12. The generator of P_i's give order 3 elements in the imgae of ϕ in S_4. There are eight such order 3 elements. The order 3 elements of S_4 are 3-cycles, which are even premutation. Therefore, $|A_4 \cap Im(\phi)|$ cardinality is atleast 8.Lagrange tells us that therefore $|A_4 \cap Im(\phi)| = 12$ and we get our claim. □

Definition 4.35. *Given a group G, a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

is called a solvable series of G if , G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian for all $0 \leq i < n$. A group G is called solvable if it has a solvable series.

Examples of Solvable groups Abelian groups are solvable. Simple non abelian groups are not solvable. Therefore, A_5 is not solvable. S_1 and S_2 are obviosuly solvable. The series

$$S_3 \supset A_3 \supset \{e\}$$

is a solvable series of S_3. Let

$$V_4 := \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Then V_4 is a normal subgroup of A_4 and A_4/V_4 is group of order 3 so cyclic and V_4 is abelian. Therefore

$$S_4 \supset A_4 \supset V_4 \supset \{e\}$$

is a solvable series of S_4.

Lemma 4.36. *Let G be a group. Define $G^1 := [G, G]$ and $G^i := [G^{i-1}, G^{i-1}]$. Then G is solvable iff there exists a natural number n such that $G^n = \{1\}$.*

Proof. If G staisfies that $G_n = \{1\}$, then G is solvable is obvious as commutator subgroups are normal and quotienting by commutator subgroup gives abelian groups. Now suppose G is solvable and

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

be a solvable series of G. Now for any $K \subset H \subset G$, such that H is normal in G and K is normal in H and such that G/H and H/K are abelian then G^1 is a subgroup of H and $G^1/K \cap G^1$ is abelian as G/H is abelian and H/K is abelian. As $G^1/K \cap G^1$ is abelian, we get that $G^2 \subset K$. So inductively one can prove that $G^n \subset G_n$ and we are done.

□

5. Lecture 8

Definition 5.1. *Given a group G, a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

is called a solvable series of G if , G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian for all $0 \leq i < n$. A group G is called solvable if it has a solvable series.

Examples of Solvable groups Abelian groups are solvable. Simple non abelian groups are not solvable. Therefore, A_5 is not solvable. S_1 and S_2 are obviosuly solvable. The series

$$S_3 \supset A_3 \supset \{e\}$$

is a solvable series of S_3. Let

$$V_4 := \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Then V_4 is a normal subgroup of A_4 and A_4/V_4 is group of order 3 so cyclic and V_4 is abelian. Therefore

$$S_4 \supset A_4 \supset V_4 \supset \{e\}$$

is a solvable series of S_4.

Theorem 5.2. *(Second Isomorphism Theorem) Let H be a subgroup of a group G and N a normal subgroup of G. Then HN is a subgroup of G , $H \cap N$ is a normal subgroup of H, and $H/H \cap N \cong HN/N$.*

Proof. As N is normal $h_1.n_1.h_2.n_2 = h_1h_2h_2^{-1}n_1h_2n_2 = h_1h_2n'n_2$ for some $n' \in N$. In particular we get that $HN = NH$. Therefore, $H.N$ is a subgroup of G. The subgroup $N \subset HN$ is normal and $H \subset HN$ is a subgroup. The homomorphism $H \to HN/N$ sending $h \mapsto h.N$ has kernel $H \cap N$. For all $h \in H, n \in N$, we have $h.n.N = h.N$. Therefore the map $H \to HN/N$ is surjective. Now apply theorem **??**.

□

Theorem 5.3. *(Correspondence Theorem) Let N be a normal subgroup of G and let $\pi : G \to G/N$ be the canonical quotient group homomorphism. Then $H \mapsto \pi(H)$ is a one to one correspondence between the set of subgroups H conatining N and the set of subgroups of G/N. Moreover, the normal subgroups of G containing N correspond to normal subgroups of G/N.*

Proof. First of all $\pi(H)$ is subgrioup of G/N and for any subgroup $H' \subset G/N$, $\pi^{-1}(H')$ is a subgroup of G. Since $\pi(N) = e.N \in H'$, therefore $\pi^{-1}(H')$ contains N. We will verify that for any subgroup H containing N, we have $\pi^{-1}(\pi(H)) = H$. It is clear that $H \subset \pi^{-1}(\pi(H))$. Let $g \in \pi^{-1}(\pi(H))$, therefore we have $\pi(g) = \pi(h)$ for some $h \in H$. This implies $g.h^{-1} \in N$, therefore $g.h^{-1} \in H$. This implies $g \in H$. Next we show that for any subgroup $H' \subset G/N$, we have $\pi(\pi^{-1}(H')) = H'$. Again $\pi(\pi^{-1}(H')) \subset H'$ is obvious. Let $h' \in H'$. Then there exists $g \in G$ such that $\pi(g) = h'$ as π is surjective. Then $g \in \pi^{-1}(H')$, therefore $\pi(g) = h \in \pi(\pi^{-1}(H'))$. Now for any normal subgroup $N' \subset G/N$, we have $\pi^{-1}(N')$ is a normal subgroup of G containing N (see exercise). Let $H \subset G$ be a normal subgroup of G containing N. Then $\pi(g)\pi(H)\pi(g)^{-1} = \pi(g.Hg^{-1}) = \pi(H)$ for all $g \in G$. As π is surjective, this shows that $\pi(H)$ is normal. Note that $\pi(H) = H/N$.

□

Theorem 5.4. *(Third isomorphism theorem) Let G be a group and $N, H \subset G$ normal subgroups of G such that $N \subset H$, then $G/H \cong G/N/(H/N)$.*

Proof. See exercise.

□

Lemma 5.5. *Let G be a group. Define $G^1 := [G, G]$ and $G^i := [G^{i-1}, G^{i-1}]$. Then G is solvable iff there exists a natural number n such that $G^n = \{1\}$.*

Proof. If G staisfies that $G_n = \{1\}$, then G is solvable is obvious as commutator subgroups are normal and quotienting by commutator subgroup gives abelian groups. Now suppose G is solvable and

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

be a solvable series of G. Now for any $G \subset H \supset K$, such that H is normal in G and K is normal in H and such that G/H and H/K are abelian then G^1 is a subgroup of H and $G^1/K \cap G^1$ is abelian as G/H is abelian and H/K is abelian. As $G^1/K \cap G^1$ is abelian, we get that $G^2 \subset K$. So inductively one can prove that $G^n \subset G_n$ and we are done.

□

Lemma 5.6. *Let*

$$1 \to N \to G \to H \to 1,$$

be an exact sequence of groups. Then G is solvable iff H and N are both solvable.

Proof. Let $p : G \to H$ be the quotient map and $N \to G$ we think it as an inclusion. Ket G be solvable with solvable series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

then

$$N = N_0 \supset G_1 \cap N \supset \cdots \supset G_n \cap N = \{1\},$$

is a solvable series of N as subgroups of abelian groups are abelian and intersection $H \cap N$ of normal subgroup N with a subgroup H is a normal subgroup of H. On the other hand as quotients of abelian groups are abelian and quotient of a normal subgroup is normal we get

$$H = H_0 \supset p(G_1) \supset \cdots \supset p(G_n) = \{1\},$$

is a solvable series of H.

On the other hand if

$$N = N_0 \supset N_1 \supset \cdots \supset N_n = \{1\},$$

be a solvable series of N and

$$H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\},$$

a solvable series of H, then

$$G = p^{-1}(H_0) \supset p^{-1}(H_1) \supset \cdots \supset p^{-1}(H_m)(N = N_0) \supset N_1 \supset \ldots N_n = \{1\},$$

is a solvable series of G.

□

Proposition 5.7. *Every group of order p^n for some prime p is solvable. Moreiver a finite group G is solvable iff there exists a sequence of sub groups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is cyclic of prime order for all $0 \leq i < n$.

Proof. We prove the first part of induction on n. If a group G is of order p^1 then there is nothing to prove. Suppose we know the statement for all $1 < r < n$. Let $|G| = p^n$ and G is non abelian then the $|Z(G)| = p^k$ where $1 \leq k < n$. Then $Z(G)$ and $G/Z(G)$ are solvable by induction hypothesis and therefore we are done. For the second part suppose

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

such that G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is cyclic of prime order for all $0 \leq i < n$, then offcourse G is solvable. On the other hand suppose the finite group G is solvable and

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

be a solvable series. Let H be a finite group and let N be a normal subgroup such that H/N is abelian. Let K be a maximal proper normal subgroup containing N. Then H/K is simple and it is a quotient subgroup of an abelian group H/N, therefore H/K is of order p for some prime p. Therefore, inductively we can construct subgroups $H_{i,j}$ of G_i containing G_{i+1} such that $H_{i,0} = G_i$ and $H_{i,m} = G_{i+1}$, $H_{i,j+1}$ is normal subgroup $H_{i,j}$ and $H_{i,j}/H_{i,j+1}$ is or prime order for $0 \leq j < m$.

□

Theorem 5.8. *The group S_n is not solvable for $n > 4$.*

Proof. We know that A_5 is non abelian simple therefore non solvable. This implies S_5 is not solvable as subgroups of solvable groups are solvable. For every $n > 4$, there exists n injective group homomorphism $S_5 \to S_n$ by premuting just the first 5 letters. Then S_n for $n > 4$ solvable will imply S_5 is solvable. Which is a contradiction.

□

Direct Product

Let H and K be groups $H \times K$ has group structure given by $(h_1, k_1).(h_2, k_2) = (h_1.h_2, k_1.k_2)$ with identity $(1, 1)$ and inverse of (h, k) given by (h^{-1}, k^{-1}). Note that $\phi_H : H \to H \times K$ given by $h \mapsto (h, 1)$ and $\phi_K : K \to H \times K$ given by $k \mapsto (1, k)$ are injective group homomorphism, making $\phi_K(K) \cong K$ and $\phi_H(H) \cong H$ normal subgroups of G with $\phi_H(H) \cap \phi(K) = \{(1, 1)\}$ and $\phi_H(H).\phi_K(K) = H \times K$ and every element of $\phi_H(H)$ commutes with every element $\phi_K(K)$.

Theorem 5.9 (Detection of direct product)**.** *Let G be a group and H and K be subgroups such that*

(1) $G = HK$,
(2) $H \cap K = \{1\}$,
(3) $hk = kh$ for all $h \in H, k \in K$.

Then the natural map $f : H \times K \to G$ given by $f(h, k) = hk$ is an isomorphism of groups.

Proof.

$$f((h_1, k_1).(h_2, k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1, k_1)f(h_2, k_2).$$

If $hk = e$, then $h, k \in H \cap K$. So f is injective. The homomorphism f is surjective as $G = HK$.

□

Semi direct product

(1) Let

$$G : \{\phi : \mathbb{R} \to \mathbb{R} | \phi(x) = ax + b, a \in \mathbb{R}^* and b \in \mathbb{R}\}.$$

Then

$$G \cong \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in Gl_2(\mathbb{R} \right\}.$$

Let

$$H := \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right\},$$

and

$$K := \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Then $H \cap K = \{Id\}$ and $G = HK$. Also note that H is normal in G, $G/H \cong K$ and G is not abelian. Therefore $G \ncong H \times K$.

(2) Let $G = Gl_2(\mathbb{R})$, $H = Sl_2(\mathbb{R})$ and

$$K := \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} a \in \mathbb{R}^* \right\}.$$

Then $G = HK$, $H \cap K = \{Id\}$ and H is normal in G, but elements of H does not commute with elements of K.

6. lecture 9

Note that if H is a normal subgroup of G and let K be a subgroup of G such that $H \cap K = \{1\}$. Then we have the following obeservations

(1) We get a homomorphism $\phi : K \to Aut(H)$, given by $\phi(k)(h) = khk^{-1}$. This is a group homomorphism.
(2) $(h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2 = h_1\phi(k_1)(h_2)k_1k_2$
(3) $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} = \phi(k^{-1})(h^{-1}).k^{-1}$.

Proposition 6.1. *Let H and K be two groups and let $\phi : K \to Aut(H)$ homomorphism. The set $H \times K$ has a group structure (the group is denoted by $H \rtimes_\phi K$), such that*

(1) $(h_1, k_1)(h_2, k_2) := (h_1\phi(k_1)(h_2), k_1k_2)$.
(2) The subset $H\times 1$ (resp. $1\times K$) is a subgroup with the obvious group structure on $H \times 1$ (resp. $1 \times K$) coming from the group structure of H (resp. K).
(3) $(H \times 1)(1 \times K) = H \rtimes_\phi K$ and $(H \times 1) \cap (1 \times K) = \{(1, 1)\}$.
(4) $(H \times 1)$ is a normal subgroup and the conjugation action of $1 \times K$ on $H \times 1$ can be identified with homomorphism ϕ.
(5) Every element of $H \times 1$ commutes with every elemnt of $1 \times K$ iff ϕ is the trivial homomorphism.

Proof. $(h, 1)(1, k) = (h.\phi(1)(1), 1.k) = (h, k)$. Therefore $(H \times 1)(1 \times K) = H \rtimes_\phi K$. Note that

$$(h_1, k_1)(h, 1)(h_1, k_1)^{-1} = (h_1\phi(k_1)(h), k_1)(\phi(k_1^{-1})(h^{-1}), k_1^{-1}).$$

Therefore normality of $H \times 1$ follows. Note that

$$(1, k)(h, 1)(1, k)^{-1} = (1\phi(k)(h), k)(1, k^{-1}) = (\phi(k)(h), 1).$$

□

Theorem 6.2. *Let G be a group and let H, K subgroups of G such that*

(1) $G = HK$,
(2) $H \cap K = \{1\}$.
(3) H is normal in G.

Then $\phi : K \to Aut(H)$ given by $\phi(k)(h) = khk^{-1}$ is group homomorphism such that $f : H \rtimes_\phi K \to G$ gievn by $f(h, k) = hk$ is an isomorphism of groups.

Proof. □

Example 6.3. *(1) If $\phi(k)$ is the identity automorphism of H, then $H \times_\phi K \cong H \times K$.*

(2) $H = \mathbb{R}$ and $K = \mathbb{R}^*$, $\phi : \mathbb{R}^* \to Aut(\mathbb{R})$ such that $\phi(x)(a) = x.a$. Then

$$H \rtimes_\phi K \cong \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in Gl_2(\mathbb{R} \right\},$$

where $(b, a) \mapsto \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$

(3) If $H = \mathbb{Z}/m$ and $K = (\mathbb{Z}/m)^*$. Then $Aut(\mathbb{Z}/m) \cong (Z/m)^*$, and we view this isomorphism by mapping a unit $a \in \mathbb{Z}/m$ to the group automorphism of $\mathbb{Z}/m$ defined by multiplication by a. This identification gives a non trivial homomorphism (infact isomorphism) $\phi : K \to Aut(H)$ and we get the semidirect product $H \rtimes_\phi K$.

(4) *A group which is direct product of $H \times K$ can also be non trivial semidirect product $H \rtimes_\phi K$. Indeed, Let n be odd take $G = Gl_n(\mathbb{R})$, $H = Sl_n(\mathbb{R})$ and*

$$K := \left\{ \begin{bmatrix} a & 0 \\ 0 & Id_{n-1} \end{bmatrix} | a \in \mathbb{R}^* \right\} \cong \mathbb{R}^*.$$

We have already seen that the conjugation action of K on H gives a non trivial homomorphism $\phi : K \to Aut(H)$. Therefore $G \cong H \times_\phi \mathbb{R}^*$.

Now the center of G is $Z(G) = \{c.Id_n | c \in \mathbb{R}^*\} \cong \mathbb{R}^*$. Let $K' = Z(G)$. As n is odd $HK' = G$, $H \cap K' = \{Id_n\}$, note that both H and K' are normal in G therefore $G \cong H \times K' \cong H \times \mathbb{R}^*$.

Theorem 6.4. *Let H_1, H_2, K_1, K_2 be groups and $f_1 : H_1 \to H_2$ and $f_2 : K_1 \to K_2$ be group isomorphisms. Then $F : H_1 \times K_1 \to H_2 \times K_2$ given by $F(h, k) = (f_1(h), f_2(k)$ is an isomorphism of groups.*

Proof. □

Theorem 6.5. *Let H_1, H_2, K_1, K_2 be groups and $f_1 : H_1 \to H_2$ and $f_2 : K_1 \to K_2$ be group isomorphisms and let $\phi_1 : K_1 \to Aut(H_1)$ be group homomorphism. Then there exists $\phi' : K_2 \to Aut(H_2)$ homomorphism such that $H_1 \rtimes_{\phi_1} K_1 \cong H_2 \rtimes_{\phi_2} K_2$.*

Proof. Using f_2 we get an isomorphism $f_1^* : Aut(H_1) \to Aut(H_2)$, given by $f_1^*(\sigma) = f_1 \circ \sigma \circ f_1^{-1}$. Using this and f_2 get $\phi' := f_1^* \circ \phi_1 \circ f_2^{-1}$.

□

Theorem 6.6 (Chinese Remainder Theorem)**.** *Let $G = \mathbb{Z}/mn\mathbb{Z}$ with $(m, n) = 1$. Then thre exists unique copy of $H = \mathbb{Z}/m\mathbb{Z}$ and $K = \mathbb{Z}/n\mathbb{Z}$ such that $H \cap K = \{1\}$ and $H + K = G$, $G/H \cong K$ and $G/K \cong H$. Inparticular, the map $K \times H \to G$ given by $(k, h) \mapsto k + h$ gives an isomorphism.*

Same method of the proof can be used to prove the following

Theorem 6.7. *Let G be an abelian group $|G| = \prod_{i=1}^k p_i^{n_i}$ be the prime factorisation of $|G|$ and let P_i be the Sylow p_i-subgroup. Then $G \cong \prod_{i=1}^k P_i$.*

Proof. Let us consider the map $\theta : \prod_{i=1}^k P_i \to G$ giben by $\theta((a_1, \dots a_k)) = \sum_{i=1}^k a_i$. This is a group homomorphism. If $\sum_{i=1}^k a_i = 0$ with $a_i \in P_i$, then a_i which has order a power of p_i is equal to $-\sum_{j \neq i} a_j$ which has order dividing $\prod_{j \neq i} p_j^{n_j}$. This is only possible if the order of a_i is 1, in that case $a_i = 0$. Therefore, θ is injective. Now compare cardinality.

□

Definition 6.8. *A commutative ring F is a field if every non zero element is a unit.*

Remark 6.9. *Let $\phi : F \to A$ be a ring homomorphism and let F be a field then ϕ is injective. Moreover, $\phi(F)$ is a field isomorphic to F.*

Definition 6.10. *A field E containing a field F is called an extension field of F. In this situation E can be regarded as an F vector space. The dimension of E as an F vector space is called the degree of the extension E/F and is denoted by $[E : F]$. Given two extension E_1/F and E_2/F an F homomorphsm is a homomorphism $\phi : E_1 \to E_2$ such that $\phi|_F = id_F$. An F-isomorphism is a bijective F-homomorphism.*

Proposition 6.11 (Substitution principle)**.** *Let A be a ring and let B be an A algebra (assume $A \subset B$). Then an A algebra homomorphism $\phi : A[x_1, \dots, x_n] \to B$ is completely determined by $\phi(x_i)$'s. Let I be an ideal of $A[x_1, \dots, x_n]$ such that $A \cap I = 0$, then an A-algebra homomorphism $\phi : A[x_1, \dots, x_n]/I \to B$ is natural bijection with the set of points $(b_1, \dots b_n) \in B^n$ such that $f(b_1, \dots, b_n) = 0$ for all $f \in I$.*

Proof. Given $\phi(x_i) \in B$, the natural map $\phi(\sum_I a_I x^I) := a_I \sum_I \phi(x^I)$ gives a well defined A-algebra homomorphism where $I = (i_1, \dots, i_n)$ and $x^I = x_1^{i_1} \dots . x_n^{i_n}$, $\phi(x^I) := \phi(x_1)^{i_1} \dots ., \phi(x_n)^{i_n}$. This gives the first part. An A algebra homomorphism $A[x_1, x_n]/I \to B$ is determined by A-algebra homomorphism $\phi : A[x_1, \dots, x_n] \to B$ such that $\phi(I) = 0$. Now the second claim follows.

□

Example 6.12. *(1) Let A be an integral domain then*

$$K(A) = \{(a, b) | a \in A, b \in A \setminus 0\} / ((a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = b_1 a_2)$$

is the fraction field. There is a natural map $l : A \to K(A)$ which is injective and $l(a) = [(a, 1])$ It has the universal property, that any ring homomorphism $\phi : A \to B$ such that the nonzero elements of A maps to units in B, then ϕ can be uniquely extended to a ring homomorphism $\psi : K(A) \to B$ such that $\psi \circ l = \phi$. Let F be a field and let $A = F[x]$, then $K(A)$ is denoted by $F(x)$. It is an infinite dimensional vector space over F.

*(2) **Characteristic of a field** : Given any integral domain A, consider the unique homomorphism $\phi : \mathbb{Z} \to A$, which is completely determined by $\phi(1) = 1$. As A is an integral domain, we see that $Im(\phi)$ is an integral domain, therefore $ker(\phi)$ is a prime ideal of $\mathbb{Z}$. When $ker(\phi)$ is trivial then we say that the characteristic of A is 0. Else $ker(\phi) = (p)$ for some prime p, which is called the characteristic of A. The field $\mathbb{F}_p$, the ring $\mathbb{F}_p[x]$, the field $\mathbb{F}_p(x)$ are all characteristic p field.*

(3) Let F be a field and $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be an irreducible polynomial. Then the ideal generated by $f(x)$ is a prime ideal as $F[x]$ is an U.F.D and it is infact maximal because $F[x]$ is a P.I.D. Let $E := F[x]/(f(x))$. This a field. As F sits as a subring in $F[x]$ as constant polynomials, the map $F \to F[x] \to F[x]/(f(x))$ is injective, and therefore E is an extension of F and it has a distinguised element the imga eof x denoted by $\bar{x}$. The element $f(t) = \sum_{i=0}^n a_i t^i \in E[t]$ has $\bar{x}$ as the root. The degree $[E : F] = n = deg(f)$. Indeed, the set $(1, \bar{x}, \dots, \bar{x}^{n-1})$ is basis because of division algorithm and irreducibility of $f(x)$.

(4) Any finite field is of characteristic p for some prime p and it has p^n elements. It is also the case that there exists innfinitely many irreducible polynomials in $\mathbb{F}_p[x]$ of degree greater than 1, so there exists finite fileds whose elements are greater than p.

(5) Extension of finite fields are simple. Let F be a field of cardinality $p^n = q$. Then $|F^*| = q - 1$. Let t be the maximum of the orders of the elements of F^* and let α be an element of order t. Since the group is abelian, order of every element is a divisor of t. This show that the $q - 1$ many elements of F^* satusfies $f(x) = x^t - 1$ equation. As f can have atmost $q - 1$ roots and $t|q - 1$,we have $t = q - 1$, or F^* is cyclic with generator α. So F is a simple extension of $\mathbb{F}_p$.

(6) *Let E/F be an extension, let $\alpha_1, \ldots, \alpha_n$ be elements in E. Then $F(\alpha_1, \ldots, \alpha_n)$ denote the subfield of E generated by F and $\alpha_1, \ldots, \alpha_n$. First of all such a field exists because $F[\alpha_1, \ldots, \alpha_n] \subset E$ exists by substitution principle and it is an integral domain. $F(\alpha_1, \ldots, \alpha_n)$ is the fraction field of $F[\alpha_1, \ldots, \alpha_n]$. We can describe the elements in $F(\alpha_1, \ldots, \alpha_n)$ as rational functions evaluated on $(\alpha_1, \ldots, \alpha_n)$. The field $F(\alpha)$ is called a simple extension. Let $\alpha \in E$, then we have an F algebra homomorphism $ev_\alpha : F[x] \to E$ such that $ev_\alpha(x) = \alpha$. The image is $F[\alpha]$. If ev_α injective then α is not a root of any non zero polynomial in $F[x]$ therefore α is called transcendental over F. In this case $F(\alpha) \cong F(x)$. Infact the degree in this case is infinite.*

(7) *$\mathbb{C}$ is an extension of $\mathbb{R}$ of degree 2 as $(1, i)$ is a basis. Note that the $\mathbb{R}$ extension $\mathbb{R}[x]/(x^2 + 1)$ is $\mathbb{R}$-isomorphic to $\mathbb{C}$. Note that for any degree 2 real polynomial $f(x)$ with non real roots we have the $\mathbb{R}$ extension $\mathbb{R}[x]/f(x)$ is isomorphic to $\mathbb{C}$.*

(8) *The $\mathbb{Q}$-extension $\mathbb{Q}(i)$ is a field extension of degree 2, so is the $\mathbb{Q}$-extension $\mathbb{Q}(\sqrt{2})$. But this two fields are not isomorphic as $\mathbb{Q}$ extensions.*

Lemma 6.13 (Degrees in tower)**.** *Let $F \subset E \subset L$ be fields. Then L/F is of finite degree iff L/E and E/F are of finite degree. In this case $[L : F] = [L : E][E : F]$*

Proof. Let L/E have E basis $(l_1, \ldots l_m)$ and E/F has F basis $(e_1, \ldots, e_n)$. Then $(e_i f_j)$'s generates L as an F vector space is obvious. So L/F is of finite degree. Note that $\sum_{i,j} a_{ij} e_i f_j = 0$ and let $b_j = \sum_i a_{i,j} e_i$, then $\sum_j b_j f_j = 0$ so $b_j = 0$ for all j and this implies $a_{i,j} = 0$ for all i, j. Therefore, $(e_i f_j)$ is a basis of L/F. So $[L : F] = [L : E][E : F]$. If L/F is of finite degree, then any F generating set L will be an E generating set of L as $F \subset E$. On the other hand E is a sub F vector space of L, therefore E/F will have finite degree.

□

7. Lecture 9

Definition 7.1. *Let L/k be a field extension. An element $\alpha \in L$ is called algeraic over k if there exists a non zero polynomial $f(x) \in k[x]$, such that $f(\alpha) = 0$. An α is called trascendental over k if it is not algebraic over k.*

Remark 7.2. *Let L/k be a field extension and let $\alpha \in L$. The smallest subring of L containing k and α is denoted by $k[\alpha]$ and the smallest subfield of L containing k and α is denoted by $k(\alpha)$. Given such an $\alpha \in L$, we define a ring homomorphism $ev_\alpha : k[x] \to L$ such that $ev_\alpha(x) = \alpha$ and $ev_\alpha|_k$ is just the inclusion $k \to L$. Note that $Im(ev_\alpha)$ is a subring of L containing k and α. It is also an integral domain, being a subring of a field. Therefore the fraction field $K(Im(ev_\alpha))$ can be throught of as a sufield of L containing α and k using universal property of the fraction field.*

Lemma 7.3. *Let L/k be any extension and let $\alpha \in L$. Then $k[\alpha] = Im(ev_\alpha)$ and $k(\alpha) = K(Im(ev_\alpha))$ (rather the image using universal property)*

Proof. Let $R \subset L$ be a subring containg α, k, then any polynomial expression in α with coefficients in k is in R. Therefore $ev_\alpha : k[x] \to L$ factors through R and this shows that $k[\alpha] = Im(ev_\alpha)$. Let $F \subset L$ be a subfield of L containing k and α, then $k[\alpha] \subset F$ and ev_α factors through F. Now $k[\alpha] \to F$ is an injection such that every non zero element of $k[\alpha]$ is a unit in F, therefore the unique homomorphism

$K(Im(ev_\alpha)) \to L$ preserving the inclusion $k[\alpha] \subset L$ factors through F. Therefore, $k(\alpha) \subset F$.

□

Lemma 7.4. *Let L/k be an extension and $\alpha \in L$. Then α is algebraic over k iff $k[\alpha] = k(\alpha)$, iff $k(\alpha)/k$ is a finite extension.*

Proof. Note that $k(\alpha)$ is the fraction field of $k[\alpha]$, therefore $k[\alpha] = k(\alpha)$ iff $k[\alpha]$ is already a field. Consider the homomorphism $ev_\alpha : k[x] \to L$, whose image is $k[\alpha]$. Since the image is an integral domain, the $ker(ev_\alpha)$ is a prime ideal in $k[x]$. Now the kernel is the set of all polynomial in $k[x]$ which has α as a root. Therefore it is non zero iff there exists a non zero polynomial with α as a root iff α is algebraic over k. The kernel is non zero iff it is a non zero prime ideal iff it is a maximal ideal ($k[x]$ is a P.I.D) iff there exists irreducible polynomiakl $f(x) \in k[x]$, such that $ker(ev_\alpha) = (f)$ and this happens iff $k[\alpha]$ is a field. Now $k[\alpha]$ is a field iff $k(\alpha) = k[\alpha]$. Now $k[\alpha]$ is field implies it is a finite extension of k, therefore $k(\alpha)$ is a finite extension over k. Now if $k(\alpha)/k$ is a finite extension and $k[\alpha]$ is a not field, then $ker(ev_\alpha) = 0$, therefore the k subvector space of $k(\alpha)$ denote by $k[\alpha]$ is infinite dimensional k-vector space. This absurd. So $k(\alpha)/k$ is a finite extension iff $k[\alpha] = k(\alpha)$.

□

Definition 7.5. *Let L/k is an extension. Then L/k is called an algebraic extension if all $\alpha \in L$ are algebraic over k. An extension L/k is called a purely transcendental extension if $\alpha \in k$ are the only algberaic elements in L.*

Lemma 7.6. *(1) Let L/k be a finite extension t hen L/k is an algebraic extension.*

(2) Let $k(t)$ be the fraction field of the polynomial ring $k[t]$, then $k(t)/k$ is a purely transcendental extension.

(3) Let $k \subset F \subset L$ be field extensions and $\alpha \in L$. Then α is algebraic over k implies α is algebraic over F.

(4) If L/k be an algebraic extension and $\alpha, \beta \in L$ algebraic over k. Then $\alpha \pm \beta$, $\alpha.\beta$ and $\alpha^{-1}.\beta$ are algebraic over k.

Proof. (1) As L/k is a finite extension, therefore for any subfield $k \subset F \subset L$, we have F/k is also a finite extension over k. Let $\alpha \in L$. Then $k(\alpha)/k$ is a finite extension. This implies α is algebraic over k. Therefore L/k is an algebraic extension.

(2) Let $\alpha = f(t)/g(t) \in k(t)$ such that $(g(t), f(t)) = 1$, $g(t) \neq 0$ and $\alpha \notin k$. Let $h(x) = \sum_i^n a_i x^i$ such that $a_n \neq 0$ and $h(\alpha) = 0$. Then $0 = \sum_i^n a_i (f(t)/g(t))^i$. Multiplying both sides by $g(t)^n$ we get $a_n f(t)^n = g(t).l(t)$ for some polynomial $l(t) \in k[t]$. This implies $g(t)$ is a non zero constant in k ($gcd(f, g) = 1$). In this case degree of $g(t).l(t)$ is atmost $(n-1).deg(f)$, on the other hand degree of $f(t)^n$ is $n.deg(f)$. This implies $f(t) \in k$.

As there exists a non zero $f(x) \in k[x]$ such that $f(\alpha) = 0$, therefore there exists $f(x) \in F[x]$ such that $f(\alpha) = 0$.

Let α, β be algebraic over k. Let $k(\alpha, \beta) \subset L$ smalles subfield of L containing α, β. Therefore $k(\alpha, \beta) = k(\alpha)(\beta)$. As $\alpha \in k(\alpha)$ is algebraic over k, we get $k(\alpha)$ is a finite extension of k. On the other hand β is algebraic over k, implies β is algebraic over $k(\alpha)$. therefore $k(\alpha)(\beta)$ is finite extension of $k(\alpha)$. Therefore, the tower formula

gives us $k(\alpha)(\beta)$ is a finite extension of k. Therefore, it is an algebraic extension of k.

□

The field extension $\mathbb{Q}(2^{1/3})$ is subfield of $\mathbb{R}$ and the equation x^3-2 has two non real roots, therefore in $\mathbb{Q}(2^{1/3})$ the polynomial $x^3-2=(x-2^{1/3})g(x)$ where $g(x)$ is a irreducible polynomial in $\mathbb{Q}(2^{1/3})[x]$. On the other hand the field $\mathbb{Q}(2^{1/3},\omega)$ is a field where x^3-2 splits in linear factor and the field is genrated by the roots of x^3-2 over $\mathbb{Q}$. Note that the degree of the extension $[\mathbb{Q}(2^{1/3},\omega):\mathbb{Q}]=6$ using the degrees in tower formula.

Definition 7.7. *Let $f(x)\in k[x]$ be a non constant polynomial. A splitting field K of f over k is a field extension K/k such that*

1. *$f(x)$ splits into linear factors in $K[x]$, equivalently $f(x)=c.\prod_{i=1}^{n}(x-\alpha_i)$ with $c\in k$, $\alpha_i\in K$ and $deg(f)=n$,*
2. *$k(\alpha_1,\ldots,\alpha_n)=K$.*

Lemma 7.8. *Let $f\in k[x]$ be a non constant polynomial. Then there exists a splitting field K of f over k.*

Proof. We will prove this theorem using induction on degree of f. If $deg(f)=1$. Then $K=k[x]/f\cong k$, where $f(x)=ax+b$ and $a\neq 0$, so root is $-b/a\in k$. If we know the result upto degree $k<n$. Let $f(x)$ be of degree n. Let $f_1(x)$ be an irreducible component of degree $d\leq n$. Then, let $K':=k[x]/f_1$. Therefore, $K'=k(\alpha)$ where $\alpha=\overline{(x)}$, and $f(\alpha)=f_1(\alpha)=0$. So in K' the polynomial $f(t)$ has a linear factor $(t-\alpha)$, or $f(t)=(t-\alpha)g(t)$ with $g(t)\in K'[t]$ and degree $g(t)=n-1$. By induction, There exists K/K' splitting field of $g(t)$. It is clear that K/k is a splitting field of f.

□

Lemma 7.9. *Let F be a field with $q=p^n$ elements, then F is a splitting field of the polynomial x^q-x over $\mathbb{F}_p$.*

Proof. We know that $F^*=(\alpha)$ and therefore every element of F^* satisfies $x^{q-1}-1=0$, which implies the q elements of F satisfies x^q-x.

□

Lemma 7.10. *Let $q=p^n$. Then there exists a field $F/\mathbb{F}_p$ of cardinality q.*

Proof. Take a splitting field $F/\mathbb{F}_p$ of the polynomial x^q-x. Let $S\subset F$ be the set of elements of F satisfying the equation $x^q-x=0$. This set is closed under multiplication and conatins 0 and 1. Since $(a+b)^q=a^q+b^q$ in char p, infact the set S is subfield of F containig $\mathbb{F}_p$, therefore $F=S$. Note that if α is a root of x^q-x, then $x^q-x-(\alpha^q-\alpha)=(x-\alpha).g(x)$, where $g(x)=(x-\alpha)^{q-1}-1$.Therefore $g(\alpha)\neq 0$. this implies the roots of x^q-x are distinct, so $|F|=q$.

□

8. Lecture 10

Let $\sigma:k\to k'$ be an isomorphism. Let $f(x)\in k[x]$ be an irreducible polynomial.The isomorphism σ can be extended to give an isomorphism of rings $\sigma':k[x]\to k'[x]$, such that $\sigma'(x)=x$ and $\sigma'|_k=\sigma$. Note that $\sigma'(f(x))$ is irreducible. Therefore σ' induces an isomorphism $\sigma':k[x]/(f)\to k'[x]/(\sigma'(f))$ such that $\sigma'|_k=\sigma$.

Assume, moreover, $k, k' \subset K$ such that $\alpha \in K$ is a root of $f(x)$ and $\alpha' \in K$ is a root of $\sigma'(f)$. Then previous isomorphism $\sigma' : k[x]/(f) \to k'[x]/(\sigma'(f))$ can be used together with the k (resp. k') isomorphisms $ev_\alpha : k[x]/(f) \to k(\alpha)$ (resp. $ev_{\alpha'} : k'[x]/(\sigma'(f)) \to k'(\alpha')$) to construct an isomorphism $\tau : k(\alpha) \to k'(\alpha')$ such that $\tau|_k = \sigma$ and $\tau(\alpha) = \alpha'$. Inparticular if $\sigma = id : k \to k$, then any two roots α, α' of $f(x)$ gives an isomorphism $\tau : k(\alpha) \to k(\alpha')$ such that $\tau|_k = id$ and $\tau(\alpha) = \alpha'$.

Definition 8.1. *Let K/k be an algebrai extension. Two elements $\alpha, \alpha' \in K$ are called k-conjugates if there exists a k-isomorphism $\tau : k(\alpha) \to k(\alpha')$ such that $\tau(\alpha) = \alpha'$.*

Lemma 8.2. *Let K/k be an algebraic extension and $\alpha, \alpha' \in K$. Then α, α' are k-conjugates iff α and α' have the same minimal polynomial over k.*

Proof. Consider the map $ev_\alpha : k[x] \to K$ and $ev_{\alpha'} : k[x] \to K$. The images of this to maps are $k(\alpha)$ and $k(\alpha')$ respectively. The kernel of this maps are generated by the minimal polynomials p_α and $p_{\alpha'}$ and $ev_\alpha : k[x]/(p_\alpha) \cong k(\alpha)$ and $ev_{\alpha'} : k[x]/(p_{\alpha'}) \to k(\alpha')$ are k- isomorphisms . If the minmimal polynomials are same then the k-automorpohism $\phi : k(\alpha) \to k(\alpha')$ is given by $ev_{\alpha'} \circ ev_\alpha^{-1}$. On the other hand if $\tau : k(\alpha) \to k(\alpha')$ is a k-isomorphism such that $\tau(\alpha) = \alpha'$, then the k-homomorphism sends $\tau \circ ev_\alpha : k[x] \to k(\alpha')$ sends $x \mapsto \alpha'$. We see that

$$\tau \circ ev_\alpha(p_\alpha(x)) = \tau(p_\alpha(\alpha)) = p_\alpha(\alpha') = 0.$$

Therefore, α' is a root of p_α, which is monic and irreducible of $p_{\alpha'} = p_\alpha$. □

Proposition 8.3 (Uniqueness of splitting fields)**.** *Let $\sigma : k \to k'$ be a field isomorphism. Let $f(x) \in k[x]$ be a nonconstant polynomial and let K and K' be splitting fields of f over k and $\sigma(f)$ over k' respectively. Then there exists an isomorphism $\tau : K \to K'$ such that $\tau|_k = \sigma$.*

Proof. We will prove it using induction on degree of f. If $deg(f) = 1$, then this is obvious as the the splitting filed are k and k' respectively. If $deg(f) = n$ and let f_1 be an irreudicble component of f. Then $\sigma(f_1)$ is an irreducible component of $\sigma(f)$. Let $\alpha \in K$ be a root of f_1 and let $\beta \in K'$ be a root of $\sigma(f_1)$. Then there exists a isomorphism $\sigma_1 : k(\alpha) \to k'(\beta)$ such that $\sigma_1|_k = \sigma$ and $\sigma_1(\alpha) = \beta$. Over $k(\alpha)$ we have $f(x) = (x - \alpha)g(x)$ with $g(x) \in k(\alpha)[x]$ and K is a splitting field of $g(x)$ over $k(\alpha)$. On the other hand $\sigma_1(g(x)).(x - \beta) = \sigma(f(x))$ and $K'/k'(\beta)$ is a splitting field of $\sigma_1(g(x))$. Now by induction we get the desired result.

□

Corollary 8.4. *For every $q = p^n$, there exists a unique field (unique upto $\mathbb{F}_p$-isomorphism) $F/\mathbb{F}_p$ of cardinality q.*

Proof. □

Lemma 8.5. *Let K/k be a splitting field of some non constant $f(x) \in k[x]$. Let $K \subset L$ be any extension. Then for any k-homomorphism $\sigma : K \to L$, we have $\sigma(K) = K$.*

Proof. □

Proposition 8.6. *Let K be the splitting field of f over k and let g be an irreducible polynomial over k. If g has a root in K then g splits in K. Conversely, if K/k is a finite extension such that irreducible polynomial over k having a root in K splits in K, then K is the splitting field of some polynomial over k.*

Proof. □

Definition 8.7. *An algebraic extension K/k is called normal if any irreducible polynomial over k having a root in K splits in K.*

Proposition 8.8. *(1) Every finite extension K/k is subfield of a finite normal extension L/k. Infact for finite extensions K_i/k with $i = 1, 2 \dots, n$, there exists a finite normal extension L/k and k-homomorpshim $\sigma_i : K_i \to L$.*

(2) Let $k \subset K \subset L$ finite extensions, let N/k normal extension containinig L. Let m be the numbere of distinct k homomorphism $K \to N$ and let n be the number of distinct K-homomorphism $L \to N$. Then the number of distinct k-homomorphism $L \to N$ is mn.

(3) Let K/k be an extension of degree n and let N/k be a finite normal extension such that $K \subset N$ subfield. Then, there are at most n distinct k-homomorphism $\sigma : K \to N$.

Proof. □

9. Lecture 11

Remark 9.1. *(1) Let $f(x) \in k[x]$ irreducible of degree n. Let N be a splitting field of $g(x) \in k[x]$ and let $f(x)$ have a root in L, say α. Then the degree n extension $k(\alpha) \subset N$. Then f splits in N and the splitting field L of f is contained in N.*

(2) Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Let N be the splitting field of f. The three district roots of f, then there are 3 distinct $\mathbb{Q}$-homomorphism $\sigma : \mathbb{Q}(^{1/3}) \to N$.

(3) Let $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$. Morever $f(x)$ has no root in $\mathbb{F}_p(t)$ and it isirreducible. Indeed, infact let F be char p field then $f(x) = x^p - a$, for $a \in F$, either has root in F or it is irreducible in $F[x]$. Suppose L/F be a splitting field of $f(x)$ over F, let α, β are roots. Then $\alpha^p = \beta^p$, then $(\alpha - \beta)^p = 0$. Therefore $\alpha = \beta$. So all the roots of $x^p - a$ are equal in L. If $\alpha \notin F$, let $g(x)$ be an irreducible factor of $f(x)$ of degree $m > 1$. If $m < p$, then as $g(x)$ has all roots equal to α, therefore $\alpha^m \in F$ and $(p, m) = 1$. As $\alpha^p \in F$, we get $\alpha^{ap+bm} \in F$ for all integers a, b. Therefore $\alpha \in F$. Contraiction. Therefore $m = p$ and $f(x)$ is irreduicble. Note that $t^{1/p} \in \mathbb{F}_p(t)$, implies, there exists $f(t), g(t) \in \mathbb{F}_p[t]$, such that $gcd(f(t), g(t)) = 1$ and $g(t)^p.t = f(t)^p$. Comparing the , highest powers (or factorisation), we see that this is not possible. So $x^p - t$ does not have a root in $\mathbb{F}_p(t)$. The number of $\mathbb{F}_p(t)$-homomorphism $\phi : \mathbb{F}_p(t)(t^{1/p}) \to \mathbb{F}_p(t)(t^{1/p})$ is 1.

Definition 9.2. *Let k be a field. An irreducible polynomial $f(x) \in k[x]$ is called separable if all its roots (in a splitting field) are simple. Otherwise, f is called inseparable. Let L/k be an algebraic extension. Let $\alpha \in L$. The element α is called separable over k if the minimal polynomial is separable, otherwise it is called inseprable over k. The extension L/k is called seprable if every element $\alpha \in L$ is separable. If there exists an $\alpha \in L$ such that α is inseprable over k, then L/k is called inseparable.*

Proposition 9.3. *(1) A polynomial $f(x) \in k[x]$ has multiple roots α iff $f(\alpha) = f'(\alpha) = 0$.*

(2) An irredducible polynomial $f(x) \in k[x]$ has multiple roots iff $f' = 0$.

(3) *An irreducible polynomial $f(x) \in k[x]$ is inseperable iff $char(k) = p$ and $f(x) = g(x^p)$ for some irreducible $g(x) \in k[x]$.*

Proof. (1) $f(x) = (x-\alpha)^2 g(x)$, then $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2.g'(x)$. Therefore if $f(x)$ has multiple root α, then $f(\alpha) = f'(\alpha) = 0$. On the other hand if $f(\alpha) = f'(\alpha) = 0$, then $f(x) = (x-\alpha).g(x)$, and $f'(x) = g(x) + (x-\alpha)g'(x)$. Since $f'(\alpha) = 0$, therefore $g(\alpha) = 0$. Then α is a multiple root of $f(x)$.

(2) Consider the homomorphism $ev_\alpha : k[x] \to L$, where L is a splitting field of f. Then $f(x)$ generate the kernel and α is a multiple root iff $f'(x) \in (f(x))$. As $f'(x)$ has degree less than $f(x)$ and $f(x)$ irreducible, therefore $f'(x) \in (f(x))$ iff $f'(x) = 0$.

(3) $f(x)$ is inseperable iff $f'(x) = 0$. So if $f(x) = g(x^p)$ and $char(k) = p$ and $g(x)$ is irreducible, then $f'(x) = p.x^{p-1}g'(x^p) = 0$. On the other hand suppose $f'(x) = 0$, then $f(x) = \sum_{i=0} a_i x^i$ and $f'(x) = \sum_{i=1} a_i.i.x^{i-1} = 0$. Therefore, $a_i.i = 0$. Therefore, i has to be a multiple of p where $char(k) = p$, so $f(x) = \sum_j a_j x^{jp}$. Let $g(x) = \sum_j a_j x^j$. Then $f(x) = g(x^p)$. As $f(x)$ is irreducible, therefore $g(x)$ is irreducible too.

□

Example 9.4. *$\mathbb{F}_p(t)(t^{1/p})$ is an inseprable extension over $\mathbb{F}_p(t)$.*

Proposition 9.5. *Let K/k be a finite field extension of degree n. K/k is seperable if and only if for any finite normal extension N/k such that $K \subset N$ is a subfield, there are n-distinct k-homomorphism $K \to N$.*

Proof. Suppose there are n-distinct k-homomorphism $K \to N$. Let $\alpha \in K$. Then by Proposition 8.8, the number of $k(\alpha)$ embedding of $K \to N$ is atmost $[K : k(\alpha)]$ and number of k-embedding of $k(\alpha) \to N$ is atmost $[k(\alpha) : k]$. As the number of k-embedding $K \to N$ is $n = [K : k(\alpha)][k(\alpha) : k]$ and it is equal to the product of number of $k(\alpha)$ embedding $K \to N$ and the number of k-embedding $k(\alpha) \to N$, we get $[k(\alpha) : k] = deg(f_\alpha)$ is equal to the number of k embedding of $k(\alpha) \to N$. Now the number of k -embedding $k(\alpha) \to N$ is the number of distinct roots of f_α, therefore all the roots of f_α is distinct and we get α is separable over k.

Now let K/k be a finite separable extension of degree n. We want to show that there are n-distinct k-homomorphism $K \to N$. We will do it by induction on n. If $n = 1$, then it is trivial as $K = k$. If $n > 1$, let $\alpha \in K \setminus k$. Then note that $K/k(\alpha)$ is a finite seprable extnesion and has degree less than n and $N/k(\alpha)$ is normal. Therefore, the number of $k(\alpha)$ homomorphism $K \to N$ is equal to $[K : k(\alpha)]$. Now the number of k homomorphism $k(\alpha) \to N$ is equal to the number of distinct roots of f_α which is equal to the degree of f_α as α is seperable. Therefore the number of k homomorphism $k(\alpha) \to N$ is equal to $[k(\alpha) : k]$. Now again using Proposition 8.8 we get the number k homomorphism $K \to N$ is equal to $[K : k(\alpha)][k(\alpha) : k] = n$.

□

Corollary 9.6. *Let $k \subset K \subset L$. Let L/K and K/k are finite seprable, then L/k is finite seprable.*

Theorem 9.7. *Let K/k be a finite seprable extension. Then there exists $\alpha \in K$ such that $k(\alpha) = K$.*

Proof. Let F be a finite field K/F be a finite extension. Then F is a finite extension of $\mathbb{F}_p$ and $K/\mathbb{F}_p$ is finite seprable as K is a splitting field of a separable polynomial

over $\mathbb{F}_p$. Therefore K/F is seprable and morover $K = \mathbb{F}_p(\alpha)$ so $K = F(\alpha)$. Let F be an infinite field and Let K/F be a finite seprable extension of degree n.Let N/F be a normal extension such that $K \subset N$. Then the number of distinct F-homomorphism $\sigma_i : K \to N$ is n. Let for $i \neq j$,

$$V_{ij} := \{x \in K | \sigma_i(x) = \sigma_j(x)\}.$$

Then V_{ij} are prooper F vector subspaces of K. As F is infinite , therefore $\cup_{ij} V_{ij} \neq K$. This implies, there exists $\alpha \in K$ such that $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for all $i \neq j$. Therefore, the number of F homomorpshim $F(\alpha) \to N$ is atleast n and by separability it is $n \leq [F(\alpha) : F]$. But $F(\alpha) \subset K$. Therefore $[F(\alpha) : F] \leq n$. This implies $F(\alpha) = K$. □

Lemma 9.8. *Any non trivial vector space V over an infinite field K is not finite union of proper K-subspaces.*

Proof. We do it by induction of number of proper subspaces n. If $n = 1$, then properness implies the claim. Let $V_1, \ldots, V_n$ be proper subspaces. Let $v \notin \cup_{i=1}^{n-1} V_i$. If $v \notin V_n$, we are done. If $v \in V_n$, and choose $w \notin V_n$. Then $v + cw \notin V_n$, for all $c \in K^*$. If $v + cw$ belongs to some V_i for all $c \in K^*$ and $i \leq n-1$, then by pigeon hole, there exists $c_1 \neq c_2 \in K^*$ such that $v + c_1 w, v + c_2 w \in V_i$ for some $i \leq n-1$. This will imply $w \in V_i$ and therefore $v \in V_i$, which is a contradiction. So there exists $c \in K^*$ such that $v + cw \notin V_i$ for all $i \leq n$.

□

10. Trace, Norm, Discriminant

Definition 10.1. *Let E/k be a finite extension and let $\alpha \in E$. Then the trace is defined as $tr_{E/k}(\alpha) := trace(m_\alpha)$ and the norm is defined as $Norm_{E/k}(\alpha) = det(m_\alpha)$, where $m_\alpha : E \to E$ is the k-linear transformation $m_\alpha(\beta) = \alpha.\beta$.*

Definition 10.2. *Let $f \in k[t]$ and let L be a splitting field of f such that $f = \prod_{i=1}^{n} a(t - \alpha_i)$ for $a, \alpha_1, \ldots, \alpha_n \in L$. Define $\triangle_f := \prod_{i<j}(\alpha_i - \alpha_j)$. Then the discriminant of f is defined as*

$$D_f := \triangle_f^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Remark 10.3.

(1) *E/k as before such that $[E : k] = n$ and let $x \in k$. then $Norm_{E/k}(x) = x^n$ and $tr_{E/k}(x) = n.x$.*

(2) *Let $k = \mathbb{Q}$, $E = \mathbb{Q}(i)$. For any $a + bi \in \mathbb{Q}(i)$, the matrix of m_{a+bi} with respect to the basis $1, i$ of $\mathbb{Q}(i)/\mathbb{Q}$ is*

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Therefore, $tr_{E/k}(a + bi) = 2a$ and $Norm_{E/k}(a + bi) = a^2 + b^2$.

(3) *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$, with $a_n = 1$ irreducible, α a root in some extension. Then $k(\alpha)$ has a k basis given by $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. The matrix of m_α with respect to this basis has the charateristic polynomial same as minimal polynomial $= f(x)$. The matrix is the following $n \times n$ companion matrix*

$$m_\alpha = \begin{bmatrix} 0 & 0 & \dots & \dots & -a_0 \\ 1 & 0 & \dots & \dots & -a_1 \\ 0 & 1 & 0 & \dots & -a_2 \\ & & & & \\ & & & & \\ 0 & \dots & 1 & 0 & -a_{n-2} \\ 0 & \dots & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

$$Norm_{k(\alpha)/k}(\alpha) = det(m_\alpha) = (-1)^n a_0, tr_{k(\alpha)/k}(\alpha) = tr(m_\alpha) = -a_{n-1}.$$

(4) Note that $D_f \neq 0$ if and only if f has no multiple roots.

Lemma 10.4. *Let L/k be finite k-extension, let V be a ffinite dimensional L-vector space and let $T : V \to V$ be a L-linear transformation. Then*

$$det_k(T) = Norm_{L/k}(det_L T), tr_k(T) = tr_{L/k}(tr_L T).$$

Proof. Let $\{e_i\}$ be an L basis with respect to which T is in rational canonical form, that is T is block diagonal where each diagonal block looks like

$$\begin{bmatrix} 0 & 0 & \dots & \dots & a_0 \\ 1 & 0 & \dots & \dots & a_1 \\ 0 & 1 & 0 & \dots & a_2 \\ & & & & \\ & & & & \\ 0 & \dots & 1 & 0 & a_{n-2} \\ 0 & \dots & \dots & 1 & a_{n-1} \end{bmatrix}.$$

As norm is multiplcative and trace is additive and

$$det(\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}) = det(A).det(B), tr(\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}) = tr(A) + tr(B),$$

So we can assume T is one of the diagonal block. Then $det_L(T) = (-1)^{n-1}a_0$, $tr_L(T) = a_{n-1}$. Let $\{l_j\}$ be the k-basis of L. Then $\{l_j e_i\}$ is a k-basis for V. With respect to this basis, we get the matrix

$$\begin{bmatrix} m_0 & m_0 & \dots & \dots & m_{a_0} \\ m_1 & m_0 & \dots & \dots & m_{a_1} \\ m_0 & m_1 & m_0 & \dots & m_{a_2} \\ & & & & \\ & & & & \\ m_0 & \dots & m_1 & m_0 & m_{a_{n-2}} \\ m_0 & \dots & \dots & m_1 & m_{a_{n-1}} \end{bmatrix},$$

where for any element $a \in L$, $m_a : V \to V$ is the L-linear (thus k-linear) map given by multiplication by a. Let $r = [L : k]$, then

$$tr_k(T) = tr_k(m_{a_{n-1}}) = tr_{L/k}(a_{n-1}).$$

Therefore $tr_k(T) = tr_{L/k}(tr_L T)$. Similarly,

$$det_k(T) = (-1)^{r(n-1)} det_k(m_{a_0}) = Norm_{L/k}((-1)^{n-1}a_0) = Norm_{L/k}(det_L T).$$

□

Corollary 10.5. *Let $k \subset L \subset K$ be finite extensions and let $\alpha \in K$. Then*

$$Norm_{K/k}(\alpha) = Norm_{L/k}(Norm_{K/L}(\alpha)), tr_{K/k}(\alpha) = tr_{L/k}(tr_{K/L}(\alpha)).$$

Corollary 10.6. *Let L/k be finite extension, $\alpha \in L$ and $r = [L : k(\alpha)]$. Let $P_\alpha = t^n + \sum_{i=0}^{n-1} a_i t^i$ be the minimal polynomial of α over k. Then*

$$tr_{L/k}(\alpha) = -ra_{n-1}, Norm_{L/k}(\alpha) = (-1)^{nr} a_0^r.$$

Proof. For the k-linear transformation $m_\alpha : k(\alpha) \to k(\alpha)$, the minimal polynomial is same as the characteristic polynomial, which is equal to P_α. Then

$$Norm_{L/k}(\alpha) = Norm_{k(\alpha)/k}(Norm_{L/k(\alpha)}(\alpha)) =$$
$$= Norm_{k(\alpha)/k}(\alpha^r) = (Norm_{k(\alpha)/k}(\alpha))^r = (-1)^{nr} a_0^r.$$

The formula for trace follows similarly.

□

Theorem 10.7. *Let L/k be finite inseperable extension. Then $tr_{L/k}(\alpha) = 0$ for every $\alpha \in L$*

Proof. Let $\beta \in L$ inseparable over k. Then $P_\beta = g(t^p)$, where P_β is the minimal polynomial of β over k and $g(t) \in k[t]$ is an irreducible polynomial. Note that $[k(\beta) : k] = deg(P_\beta)$, and g is the minimal polynomial of P_{β^p} of β^p over k. Therefore, $[k(\beta) : k(\beta^p)] = p$. Therefore, $1, \beta, \beta^2, \ldots, \beta^{p-1}$ gives a basis of $k(\beta)/k(\beta^p)$ and note that the minimal polynomial P_{β^i} of β^i over $k(\beta^p)$ is nothing byt $x^p - \beta^{ip}$, for $o < i < p$. Therefore, $tr_{k(\beta)/k(\beta^p)}(\beta^i) = 0$. This implies

$$tr_{L/k}(\alpha) = tr_{k(\beta^p)/k}(tr_{k(\beta)/k(\beta^p)}(tr_{L/k(\beta)}(\alpha))) = 0,$$

for all $\alpha \in L$.

□

Proposition 10.8. *Let L/k be a separable extension and let $L \subset N$ subfield such that N/k be normal. Let $\{\phi_1, \ldots, \phi_n\} = Hom_k(L, N)$. Then*

$$tr_{L/k}(\alpha) = \sum_{i=1}^{n} \phi_i(\alpha), Norm_{L/k}(\alpha) = \prod_{i=1}^{n} \phi_i(\alpha).$$

Proof. For $\alpha \in L$ let P_α denote the minimal polynomial of α over k. Then the set $Hom_k(k(\alpha), N)$ is in bijection with the set of roots of P_α, given by $(\alpha_1, \ldots, \alpha_d)$. As α is separable we get

$$|Hom_k(k(\alpha), N)| = [k(\alpha) : k] = deg(P_\alpha) = d.$$

Consider the map $r : Hom_k(L, N) \to Hom_k(k(\alpha), N)$, where $r(\phi) = \phi|_{k(\alpha)}$. This map is surjective (prove it) and $r^{-1}(\theta)$ has size $[L : k(\alpha)]$ for every θ (prove it). Therefore

$$\sum_{i=1}^{n} (\phi_i(\alpha)) = [L : k(\alpha)] \sum_{\psi \in Hom_k(k(\alpha), N)} \psi(\alpha)$$

$$= [L : k(\alpha)] \sum_{i=1}^{d} \alpha_i = [L : k(\alpha)] tr_{k(\alpha)/k}(\alpha) = tr_{L/k}(\alpha).$$

Similarly we get the formula for norm.

□

Lemma 10.9. *(Independence of characters) Let L, N are field extensions of k, $\lambda_1, \ldots, \lambda_n \in N$ and $\phi_1, \ldots, \phi_n \in Hom_k(L, N)$ distinct such that for all $\alpha \in L$, we have $\sum_{i=1}^{n} \lambda_i \phi_i(\alpha) = 0$. Then $\lambda_i = 0$ all i.*

Proof. Induction on n. The case $n = 1$ is stratight forward as $\phi(1) = 1$ for any $\phi \in Hom_k(L, N)$. Let $n > 1$, then there exists $\beta \in L$ such that $\phi_1(\beta) \neq \phi_n(\beta)$ and $\sum_i \lambda_i \phi_i(\alpha.beta) = 0$ for $\alpha \in L$. Therefore, we get following two equations

$$\sum_i \lambda_i \phi_i(\alpha).\phi_i(\beta) = 0;$$

$$\sum_i \lambda_i \phi_i(\alpha)\phi_n(\beta) = 0.$$

Subtracting, we get

$$\sum_{i=1}^{n-1} \lambda_i(\phi_i(\beta) - \phi_n(\beta))\phi_i(\alpha) = 0,$$

for all $\alpha \in L$. This gives by induction, $\lambda_i(\phi_i(\beta) - \phi_n(\beta)) = 0$ for all $0 < i < n$, which gives $\lambda_1 = 0$. Then again by induction $\lambda_i = 0$ for all $1 < i \leq n$. □

Corollary 10.10. *Let L/k be a finite separable extension. Then there exists soem $\alpha \in L$ such that $tr_{L/k}(\alpha) \neq 0$.*

Proof. Let $k \subset L \subset N$ extensions such that N/k normal. And let $\{\phi_1, \ldots, \phi_n\} = Hom_k(L, N)$. Now $tr_{L/k}(\alpha) = \sum_{i=1}^{n} \phi_i(\alpha)$. Using, the previous lemma we get our result.

□

Theorem 10.11. *Let k be a field and let $f \in k[t]$, be monic irreducible separable of degree n and let L/k be the splitting field of f over k and let $\alpha \in L$ be any root of f. Then*

$$D_f = (-1)^{n(n-1)/2} Norm_{k(\alpha)/k}(f'(\alpha)).$$

Proof. There is a bijection between the set $Hom_k(k(\alpha), L)$ and the roots of f. There are n disntinct roots of f, say $\alpha_1, \ldots, \alpha_n$. Then $f = \prod_i (x - \alpha_i)$ and $f'(\alpha_i) = \prod_{i \neq j}(\alpha_i - \alpha_j)$. Then

$$\prod_{i \neq j}(\alpha_i - \alpha_j) = \prod_i f'(\alpha_i) = \prod_i \phi_i(f'(\alpha)) = Norm_{k(\alpha)/k}(f'(\alpha)),$$

where $\phi_i(\alpha) = \alpha_i$.

□

11. Galois Correspondence

Definition 11.1. *(1) Let K/k be an extension. Let $G(K/k)$ denote the set of k-isomorphism of $K \to K$. It is a subgroup of the group of automorphisms of K, denoted by $Aut(K)$.*

(2) Let $G \subset Aut(K)$ be a subgroup,

$$K^G := \{\alpha \in K | \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

.

Remark 11.2. *K^G is a subfield of K. Indeed, $\alpha, \beta \in K^G$ and $\sigma \in G$, then $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta) = \alpha+\beta$, similarly $\sigma(\alpha.\beta) = \alpha.\beta$, $0, 1 \in K^G$, $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$.*

Proposition 11.3. *Let E be a splitting field of a seprable irreducible polynomial $f \in k[x]$, then $G(E/k)$ has order $[E : k]$.*

Proof. By Proposition 9.5 (using E as K and N in the proposition), we get the number of distinct k homomorphism $E \to E$ is equal to $[E : k]$. As E a finite dimension k-vector space, we get that injective linear transformations are bijective. Therefore, we get the result.

□

Example 11.4. *(1) Let $E = k(\alpha)$, f be the minimal polynomial of α over k and α is the only root of f in E. Then $G(E/k) = \{1\}$, even if f is separable.*
(2) Let $E = \mathbb{F}_p(t)(t^{1/p})$, and $k = \mathbb{F}_p(t)$. Then $G(E/k) = \{1\}$ even though E/k is normal.

Theorem 11.5. *Let E be a field and let G be a finite subgroup of $Aut(E)$. Then $[E : E^G] \leq |G|$.*

Proof. Let $k := E^G$ and let $G = \{\sigma_1, \ldots, \sigma_m\}$ and let $\{\alpha_1, \ldots, \alpha_n\} \subset E$ such that $n > m$. We want to show α_i's are linearly dependent over k. We get the following m equations with n unknowns x_i's.

$$\sum_{i=1}^{n} \sigma_j(\alpha_i)x_i = 0, 1 \leq j \leq m.$$

Therefore there exists non trivial solution in E. Let $\{c_1, \ldots, c_n\} \subset E$ a non trivial solution with minimum number of non -zeroes and assume after a premutation of α_i's that $c_1 = 1$. If all the other c_i's are in k we are done by just taking $j = 1$ in the above system of equations, as $\sigma_1 = id$. If there is a c_i for $i \neq 1$ such that $c_i \notin k$, then there exists $j \neq 1$ such that $\sigma_j(c_i) \neq c_i$. Applying this σ_j to the above equation and using the fact that composing with σ_j gives a bijection $G \to G$, we get $\{c_1, \sigma_j(c_2), \ldots, \sigma_j(c_i), \ldots, \sigma_j(c_n)\}$ is also a solution of the above system of equation. Therefore,

$$\{0, c_2 - \sigma_j(c_2), \ldots, c_i - \sigma_j(c_i), \ldots, c_n - \sigma_j(c_n)\}$$

is also a system of non trivial solution with more zeroes than $\{c_1, \ldots, c_n\}$. Contradiction.

□

Corollary 11.6. *Let G be a finite subgroup of $Aut(E)$. Then $G = G(E/E^G)$.*

Proof. By previous proposition $[E : E^G] \leq |G|$. As $G \subset G(E/E^G)$, we get $|G| \leq |G(E/E^G)|$. AS E/E^G is a finite extension, there exists a smallest normal extension N/E^G (splitting field of the minimal polynomials of the generators E/E^G) such that $E \subset N$. Then $|G(E/E^G)|$ is less than or equal to the number of distinct E^G homomorphism $E \to N$, say m. Note that N/E^G is separable if and only if E/E^G is separable. The number of distinct E^G homomorphism $E \to N$ is less than or equal to $[E : E^G]$. Therefore

$$[E : E^G] \leq |G| \leq |G(E/E^G)| \leq m \leq [E : E^G].$$

Therefore,

$$[E : E^G] = |G| = |G(E/E^G)| = m.$$

□

Definition 11.7. *Let L/k be a finite extension. We say that L/k is Galois if L/k is normal and separable.*

Corollary 11.8. *Let G be a finite subgroup of $Aut(E)$, then E/E^G is Galois.*

Proof. By the similar argument as corollary 11.6we get E/E^G is separable. Also we get $|G(E/E^G)| = |Hom_{E^G}(E, N)|$. This says that the map $G(E/E^G) \to Hom_{E^G}(E, N)$ composing by the inclusion $E \subset N$ is a bijection. Therefore every $\theta \in Hom_{E^G}(E, N)$ comes from an $\alpha \in G(E/E^G)$ by composing with the inclusion $E \subset N$, equivalently for any such θ, the image is E. Let $\alpha \in E$ such that $f(x) \in E^G[x]$ is the minimal polynomial of α. Then any other root $\alpha \neq \beta$ of $f(x)$ can be used to construct an E^G isomorphism $\phi : E^G(\alpha) \to E^G(\beta)$, which can be extended to an E^G auto morphism $\phi : N \to N$. Now this $\phi|_E \in Hom_{E^G}(E, N)$ and $\phi(E) = E$ so $\beta \in E$. So E/E^G is normal. □

Proposition 11.9. *Let K/k Galois extension. Then $G(K/k)$ is a finite group of order $[K : k]$ and $k = K^{G(K/k)}$.*

Proof. By proposition 11.3 $|G(K/k)| = [K : k]$. If $K \neq k$ and $\alpha \in K \setminus k$, then for $\alpha \neq \beta$ another k conjugate we have a k-isomorphism $\phi : k(\alpha) \to k(\beta)$ mapping α to β. This by normality of K/k can be extended to $\sigma : K \to K$ a k-automorphism. Therefore, for any $\alpha \in K \setminus k$, there exists $\sigma \in G(K/k)$ such that $\sigma(\alpha) \neq \alpha$.

□

Corollary 11.10. *Let K/k be finite. Then K/k is Galois iff $[K : k] = |G(K/k)|$ iff $K^{G(K/k)} = k$.*

Proof. K/k Galois implies both conditions. Using corollary 11.8 we get $K^{G(K/k)} = k$ implies $K/(K^{G(K/k)} = k)$ is Galois and corllary 11.6 gives us that $|G(K/k)| = [K : k]$. On the other hand $[K : k] = |G(K/k) := G|$, then we get a tower of extension $k \subset K^G \subset K$. Since K/K^G is Galois and by 11.6 $G = G(K/K^G)$ and $|G| = [K : K^G]$, therefore $[K : K^G] = [K : k]$, therefore $k = K^G$. and K/k is Galois.

□

Lemma 11.11. *Let K/k be a finite normal extension and let $k \subset F \subset K$ be a tower of extensions. Then F/k is normal if and only if for all $\sigma \in G(K/k)$, $\sigma(F) = F$.*

Proof. If F/k is nnormal then we have proved before that $\sigma(F) = F$. Let $\alpha \in F \setminus k$, then any conjugate of α is in K. Let β be one such conjugate. Then the k isomorphism $\tau : k(\alpha) \to k(\beta)$ can be extended to a k-automorphism $\theta : K \to K$, then $\theta(F) = F$, implies $\theta(\alpha) = \tau(\alpha) = \beta \in F$.

□

Let K/k be a Galois extension and let $G := G(K/k)$ be the Galois group. Denote by

$$S(G) := \{H \subset G| \text{ subgroup}\},$$
$$S(K/k) := \{k \subset K_1 \subset K| \text{ subfield of } K \text{ containing } k\}.$$

Let $\Phi : S(K/k) \to S(G)$ be the map given by

$$k \subset K_1 \subset K \mapsto G(K/K_1) \subset G$$

and $\Psi : S(G) \to S(K/k)$ be the map given by

$$H \subset G \mapsto k \subset K^H \subset K.$$

Theorem 11.12 (Fundamental theorem of Galois theory)**.** *The maps $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are identity maps. Therefore, Φ and Ψ induces bijections between $S(G)$ and $S(K/k)$. Moreover, under this bijection a normal subgroup $N \subset G$ corresponds to the Galois extension K^N/k with Galois group $G(K^N/k) = G/N$. Conversely, given $k \subset L \subset K$ extension such that L/k Galois, we have $G(K/L)$ and $G(K/k)/G(K/L) \cong G(L/k)$.*

Proof. Let $k \subset K_1 \subset K \in S(K/k)$, then K/K_1 is finite separable, therefore Galois, then $K^{G(K/K_1)} = K_1$ by proposition 11.9. This shows $\Psi \circ \Phi = id$. Let $H \subset G$ be a subgroup and let K^H be the fixed field, then K/K^H is Galois by corollary 11.8. Note that $H \subset G(K/K^H)$ and $[K : K^H] = |G(K/K^H)|$. So $[K : K^H] \geq |H|$. On, the other hand by theorem 11.5, $[K : K^H] \leq |H|$. Therefore, $G(K/K^H) = H$. This shows $\Phi \circ \Psi = id$.

For the second part we first show that K_1/k is Galois iff $G(K/K_1)$ is normal in G. Let $\sigma \in G$. Then $K^{\sigma G(K/K_1)\sigma^{-1}} = \sigma(K)$.

□

Proposition 11.13. *Let k be a finite field and let K/k be a finite extension, then K/k is Galois and $G(K/k)$ is cyclic.*

Proof. □

12. Solvability by radicals

Proposition 12.1. *Let k be a field L/k be the splitting field fo $x^m - 1$ over k, such that $(m, char(k)) = 1$. Then,*

1. *L/k is Galois.*
2. *The roots of the equation $x^m - 1$ forms a cyclic subgroup ζ_m of L^*, therefore $L = k(\rho)$. Here ρ is a generator (called the primitive m-th root of unity) of the group ζ_m.*
3. *The map $\sigma \in G(L/k) \mapsto i(mod)m$, where $\sigma(\rho) = \rho^i$ is well defined (does not depend on the choice of the primitive root ρ) injective homomorphism into $(\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. (1) L/k is finite normal being splitting field. Ther dervative of $x^m - 1$ is $m.x^{m-1}$ and $(m, char(k)) = 1$, it is non zero with a signle root 0. Therefore , it is separable.

(2) Let $\zeta_m := \{\rho_1, \ldots, \rho_m\}$ be the roots. They are distinct. It is clear that ζ_m forms a group under multiplication. It is a finite abelian group. Let $\rho \in \zeta_m$ be an element such that it has maximum order l. Then any element of ζ_m satisfies $x^l = 1$. As it has atmost l solution therefore $l = m$ and ζ_m is cyclic.

(3) Any $\sigma \in G(L/k)$ only permutes the root so $\sigma(\rho) = \rho^i$ for some i which only depends on σ and $(i, m) = 1$. For the last one we know that

$$\sigma(\rho^n) = \rho = \rho^{in}$$

asσ is surjective. Therefore $in = 1(\text{mod } m$. Note that If θ be another generator, then $\theta = \rho^j$ with $(j, m) = 1$. Then $\sigma(\theta) = \sigma(\rho^j) = \rho^{ij}$. So $ij = i(\text{mod } m)$. So the map $G(L/k) \to (\mathbb{Z}/m\mathbb{Z})^*$, is a well defined injective group homomorphism.

□

Remark 12.2. *Note that in the previous proposition, we have $G(K/k)$ is finite abelian. Therefore it is solvable.*

Definition 12.3. *Let K_1/k and K_2/k be two finite extensions such that $K_1, K_2 \subset N$ for some finite extension N/k. Then $K_1.K_2 \subset N$, is smallest subfield of N such that K_1, K_2 is both contained in K_1K_2.*

Remark 12.4. *Let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in N$, such that $K_1 = k(\alpha_1, \ldots, \alpha_m)$ and $K_2 = k(\beta_1, \ldots, \beta_n)$. Then it is easy (using the smallest subfield description) to verify that $K_1.K_2 = k(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$.*

Proposition 12.5. *Let K_1/k be a Galois extension, then K_1K_2/K_2 is a galois extension. Moreover, there is a natural injective group homomorphism $\theta : G(K_1K_2/K_2) \to G(K_1/k)$.*

Proof. As K_1/k is a splitting field of some seprable polynomial $f(x) \in k[x]$, therefore K_1K_2/K_2 is the splitting field of the same seprable $f(x)$ over K_2. So $K_1.K_2/K_2$ is Galois. Let $\phi \in G(K_1K_2/K_2)$, then ϕ fixes k. Moreover, K_1/k is normal implies, that $\phi(K_1) = K_1$. So we get a homomorphism $\theta : G(K_1K_2/K_2) \to G(K_1/k)$ such that $\theta(\sigma) = \sigma|_{K_1}$. If $\theta(\sigma) = id_{K_1}$, as $\sigma|_{K_2} = id_{K_2}$, we get $\sigma = id$, so θ is injective.

□

Remark 12.6. *If K_2/k is Galois, then K_1K_2/k is Galois. Any $g \in G(K_1/k)$ can be extented to $\tilde{g} \in G(K_1K_2/k)$ and $G(K_1K_2/K_2) \subset G(K_1K_2/k)$ is normal subgroup. So $\tilde{g}\sigma\tilde{g}^{-1} \in G(K_1K_2/K_2)$ for all $\sigma \in G(K_1K_2/K_2)$. This implies $im(\theta)$ is normal subgroup. Blah blah.....*

Definition 12.7. *An extension K/k is called cyclic if it is Galois and $G(K/k)$ is cyclic.*

Proposition 12.8. *Let k be a field containing all m-th roots of unity for $(m, char(k)) = 1$ and let L/k be a splitting field of $f(x) = x^m - a, a \in k$. Let $\alpha \in L$ be a root of $f(x)$. then $L = k(\alpha)$ and L/k is cyclic. If m is prime then $L = k$ or $[L : k] = m$.*

Proof. We have in $L[x]$, $f(x) = \prod_{i=0}^{m-1}(x - \alpha.\rho^i)$, where α is any root of $f(x)$ and ρ is a primitive m-th root of unity., Moreover $L = k(\alpha)$ as k contains all m-th roots of unity . since f is seprable we get L/k is Galois extension. Let $\sigma \in G(L/k)$, then $\sigma(\alpha) = \alpha.\rho^i$. Therefore we get a well defined (!) group homomorphism $\theta : G(L/k) \to \mathbb{Z}/m\mathbb{Z}$ with $\theta(\alpha) = i\text{mod } m$. Kernel of this map is trivial . This implies $G(L/k)$ is cyclic. If m is prime thsn $G(L/k) = \mathbb{Z}/m\mathbb{Z}$ or the trivial subgroup, therefore, the second assertion follows.

□

Proposition 12.9. *Let k be a field containing all m-th roots of unity for m a prime with $(m, char(k) = 1$. Let L/k be a cyclic extension of degree m. Then there exists $\alpha \in k$ such that L is a splitting field of $x^m - \alpha$ over k.*

Proof. Let ρ be a primitive m-root of unity and a is an integer. Let $m|a$, then $\rho^{ia} = 1$, therefore $\sum_{i=0}^{m-1} \rho^{ia} = m$. If m does not divide a, then $\theta = \rho^a$ is again a primitive m-th root of 1. Therefore $\sum_{i=0}^{m-1} \rho^{ia} = \sum_{i=0}^{m-1} \theta^i = 0$ as it is the $m-1$-th coefficient of $x^m - 1$.

It is enough to show that there exists $\alpha \in L \setminus k$ such that $\alpha^m \in k$. Then $K(\alpha)/k$ is a nontrivial extension whose degree divides m, therefore it has to be equal to m. So $L = k(\alpha)$. Since L/k is separable we have $L = k(\beta)$ for some $\beta \in L$, then the minimal polynomial of of $P_\beta(x) = \prod_{i=1}^{m}(x - \beta_i)$, with $\beta_1 = \beta$. Since Galois group is cyclic and acts transitively on $\{\beta_1, \ldots, \beta_m\}$, therefore the action is by cyclic permutation. So we can assume that there exists a generator $\sigma \in G(L/k)$, such that $\sigma(\beta_i) = \beta_{i+1}$, $1 \leq i \leq m-1$ and $\sigma(\beta_m) = \beta_1 = \beta$.

Define for $1 \leq j \leq m$,

$$\alpha_j := \sum_{i=0}^{m-1} \rho^{ji} \beta_{i+1}.$$

Note the following

$$\sum_{j=1}^{m} \alpha_j = \sum_{i=0}^{m-1} \beta_{i+1} (\sum_{j=1}^{m} \rho^{ji}) = m\beta_1,$$

and α_m just the sum of the roots so $\sum_{j=1}^{m} \alpha_j \notin k$ and $\alpha_m \in k$.So there exists a $1 \leq j \leq m-1$ such that $\alpha_j \notin k$. Then

$$\sigma(\alpha_j) = \sum_{i=0}^{m-1} \rho^{ji} \sigma(\beta_{i+1}) = \sum_{i=0}^{m-2} \rho^{ji} \beta_{i+2} + \rho^{j(m-1)} \beta_1 = \rho^{-j} \sum_{i=0}^{m-1} \rho^{ji} \sigma(\beta_{i+1}) = \rho^{-j} \alpha_j.$$

So $\sigma(\alpha_j^m) = \alpha_j^m$. This implies $\alpha_j^m \in k$. Thus we get the result.

□

Definition 12.10. *Let k be a field. An extension K/k is calles simple radical extension if there exists $\alpha \in K$ such that $\alpha^m = a \in k$,$(m, char(k)) = 1$ and $K = k(\alpha)$.*

An extension K/k is called a radical extension if there exists subfields $k \subset K_i \subset K$, such that $K - 1 = k$, $K_n = K$, $K_i \subset K_{i+1}$ and K_{i+1}/K_i are simple radical extensions.

Remark 12.11.
1. *If $k \subset K \subset L$ and L/K and K/k both radical then L/k is radical.indeed, let $k \subset K_i \subset K$, such that $K_{-1} = k$, $K_n = K$, $K_i \subset K_{i+1}$ and K_{i+1}/K_i are simple radical extension and let $K \subset L_i \subset K$, such that $L_{-1} = K$, $L_m = L$, $L_i \subset L_{i+1}$ and L_{i+1}/L_i are simple radical extensions. Then the putting this towers together we get L/k is a radical extension.*
2. *Any simple radical extension is finite separable. Therefore, radical extension is finite separable.*
3. *Let K/k be a simple radical extension with $K = k(\alpha)$, let N/K be the splitting field of $x^m - \alpha^m$ over k, then N/k is a radical extension.*
4. *L/k radical and N/L be any extension such that $F \subset N$ be a subfield. Then LF/F is radical. Therefore $L_1, L_2/k$ radical then L_1L_2/k is radical.*

Proposition 12.12. *Let L/k be a radical extension. Then there exists an extension M/L such that M/k is Galois radical.*

Proof. We will prove this by induction on $[L : k]$. If $[L : k] = 1$, then $M = L = k$. Now suppose, for any radical extension L_1/L_2 such that $[L_1 : L_2] < n$, then there exists M_1/L_2 Galois radical such that $L_1 \subset M_1$. Now suppose $[L : k] = n$ and L/k be radical. If it is simple radical then we are done by one of the remark. If it is not, then there exists $k \subset L' \subset L$, such that L'/k is radical L/L' simple radical and $[L : L'], [L' : k] < n$. Then, by induction there exists Galois radical M_1/k such that $L_1 \subset M_1$ and there exists $\alpha \in L$ such that $\alpha^m \in L_1$, $(mchar(k)) = 1$ and $L = L_1(\alpha)$. Therefore $\alpha^m \in M_1$ and if $\alpha \in M_1$ we are done. Else, let M/M_1 be a splitting field of $x^m - \alpha^m$ over M_1. Thus M/M_1 is Galois radical and mapping α to any root of $x^m - \alpha^m$ in M lifts the inclusion $L_1 \subset M_1$ to give an injective homomorphism $L_1(\alpha) \to M$. Now M/M_1 is Galois radical and M_1/k is Galois radical therefore M/k is Galois radical.

□

Proposition 12.13. *Let L/k be a Galois radical extension. Then $G(L/k)$ is solvable.*

Proof. Let $L_1 = k \subset L_2 \cdots \subset L_n = L$ such that there exists $\alpha_i \in L_{i+1}, m_i \in \mathbb{N}$, such that $L_{i+1} = L_i(\alpha_i)$, $\alpha_i^{m_i} \in L_i$, $(m_i, char(k)) = 1$. Let $m = m - 1.m_2 \cdots_{n-1}$, then $(m, char(k)) = 1$. Let N/L be the splitting field of $x^m - 1$ over L and let $F \subset N$ be the smallest subfield of N containing k and the roots of $x^m - 1$. Then $LF = N$, F/k Galois radical extension with $G(F/k)$ solvable, L_iF contains all m_i-th roots of unity, (define $L_0F = k$), $L_{i+1}F = L_iF(\alpha_i)$ and they are Galois radical extnesion with $G(L_{i+1}F/L_iF)$ abelian group. Let $G_{n-i} := G(LF/L_iF)$, then $G_j \subset G(LF/k)$, $G_j \subset G_{j+1}$ normal subgroup and $G_{j+1}/G_j \cong G(L_{j+1}F/L_jF)$. This implies $G(LF/k) = G(N/k)$ is solvable. But L/k is Galois, therefore $G(L/k)$ is a quotient of $G(N/k)$ and we are done.

□

Proposition 12.14. *Let L/k be Galois such that $([L : k], char(k)) = 1$ and $G(L/k)$ is solvable. Then there exists M/L such that M/k is a radical extension.*

Proof. Let $G := G(L/k)$ and let $G_0 = \{e\} \subset G_1 \subset \ldots G_n = G$ be a solvable series such that G_i is normal in G_{i+1} and $G_{i+1}/G_i \cong \mathbb{Z}/p_i\mathbb{Z}$, with $p - i$'s are prime. Note that $[L : k] = |G|$ (as L/k is Galois), therefore $(p_i, char(k)) = 1$. Let $m = p_0.p_2 \ldots p_{n-1}$. Then $(m, char(k)) = 1$. Consider the splitting field N of $x^m - 1$ over L. Then N/L is Galois, so N/k is Galois. We will show that N/k is radical extension. Let $F \subset N$ be the smalles subfield containing k and roots of $x^m - 1$. Then F/k is Galois radical and $LF = N$ and F contains all p_i-th roots of unity for all p_i. Let $L_i := L^{G_{n-i}}$. Then L_{i+1}/L_i is Galois extension with Galois group $G_{n-i}/G_{n-i-1} \cong \mathbb{Z}/p_{n-i-1}$. Now $L_{i+1}F/L_iF$ is Galois and the Galois group is either trivial or $\mathbb{Z}/p_{n-i-1}$ and since L_iF contains all p_{n-i-1}-th roots of unity we get $L_{i+1}F/L_iF$ is Galois radical (infact simple radical). Therefore LF/F is Galois radical which implies LF/k is Galois radical.

□

Definition 12.15. *Let $f \in k[x]$, f is said to be solvable by radicals over k if the splitting filed L of f over k is a subfield of a radical extension of k.*

Theorem 12.16. *Let $f \in k[x]$, L splitting filed of f over k, such that $([L : k], char(k)) = 1$. Then L/k is Galois and moreover f is solvable by radicals over k iff $G(L/k)$ is solvable.*

Proof. Let $\beta \in L$ and let P_β be its minimal polynomial over k. Then $deg(P_\beta)|[L:k]$, therefore $deg(P_\beta))$ is not divisible by $char(k)$. This shows that P_β is separbale, hence L/k is Galois. Now if f is solvable by radicals then $L \subset N$, such that N/k is Radical. Infact we can choose N/k to be Galois radical. Then $G(N/L) \subset G(N/k)$ is a normal subgroup as L/k is Galois and $G(N/k)/G(N/L) \cong G(L/k)$. As N/k is Galois radical, therefore $G(N/k)$ is solvable. Quotient of solvable group is solvable. Therfore, we get $G(L/k)$ is solvable. The only if part follows from previous proposition.

□

Theorem 12.17. *Let p be a prime. Then there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p such that the Galois group $G(L/\mathbb{Q})$ of the splitting field $L/\mathbb{Q}$ of f is isomorphic to S_p. Therefore, for $p \geq 5$, there exists irreducible polynomial f of degree $p \geq 5$ such that f is not solvable by radicals.*

Proof. **Claim 1** : For each prime $p \geq 3$, there exists $f(x) \in \mathbb{Q}[x]$, irreducible, with exactly $p-2$ real roots. Threfore the Galois group of the splitting field of f is a trnasitive subgroup of S_p containing a transposition.

Proof. □

□

13. Algebraic Closure

Definition 13.1. *A field k is algebraically closed if any non constant $f \in k[x]$ has root in k. A field extension $\bar{k}/k$ is called an algebraic closure of k if $\bar{k}/k$ is algebraic and $\bar{k}$ is algebraically closed.*

Proposition 13.2. *Let $\bar{k}/k$ be an extension. Then the following are equivalent.*

1. *$\bar{k}/k$ is an algebraic closure.*
2. *$\bar{k}/k$ is an algebraic extension and any $f \in k[x]$ irreducible splits over $\bar{k}$.*
3. *$\bar{k}/k$ is an algebraic extension and $\bar{k}$ does not have any non trivial algebraic extension.*

Proof.
1. 1 implies 2 is trivial.
2. 2 implies 3 : If α algebraic over $\bar{k}$, then α is algbraic over k. Then the minimal polynomial of α over k has all the roots in $\bar{k}$ by 2, so $\alpha \in \bar{k}$.
3. 3 implies 1 : Let $f \in \bar{k}[x]$ non constant, then the splitting field of f over $\bar{k}$ is $\bar{k}$ by 3, therefore f splits in $\bar{k}$.

□

Corollary 13.3. *Let L/k extension such that L is algebrically closed. Let $\bar{k} := \{\alpha \in L | \alpha$ algebraic over $k\}$. Then $\bar{k}/k$ is an algebraic closure of k.*

Theorem 13.4. *Let k be a field , then there exists $\bar{k}/k$ which is an algebraic closure of k.*

Proof. New variables : Let

$$S := \{(f,i) | f \in k[x] \text{ monic non constant }, 1 \leq i \leq deg(f)\}$$

$$X_S := \{x_i(f) | (f,i) \in S\}.$$

Let $f(x) \in k[x]$, then

$$f = x^n - a_1(f)x^{n-1} + \cdots + (-1)^n a_n(f), a_i(f) \in k.$$

Here $a_i(f)$'s r i-th symmetric polynomial on the roots of $f(x)$. Let

$$\sigma_i(f) := \sum_{j_1<\cdots<j_l} x_{j_1}(f)\dots x_{j_l}(f), t_i(f) := \sigma_i(f) - a_i(f).$$

Consider the ideal $I := (t_j(f))_{j,f} \subset k[X_S]$. Then $I \neq (1)$. If not then there exists $r_1, \dots, r_N \in k[X_S]$, and $t_{i_1}(f_1), \dots, t_{i_N}(f_N)$ such that $\sum_{j=1}^N r_j t_{i_j}(f_j) = 1$ in $k[X_S]$. Let L/k be the splitting field of $f_1, \dots f_N$. Then consider the homomorphism $ev : k[X_S] \to L$ given by $ev|_k = id$, $ev(x_j(f_l))$ the j-th root of f_l and all the other variables goes to 0. Then $ev((t_j(f_l)) = 0$ for approriate i's and $1 \leq l \leq N$. Which is a contradiction as it gives $ev(1) = 0$.

Therefore there exists a maximal ideal $m \subset k[X_S]$ containing I. Define $\bar{k} := k[X_S]/m$ and let $q : k[X_S] \to \bar{k}$ be the canonical quotient map and let $j : k \to k[X_S] \to \bar{k}$. Then $\bar{k}/k$ is an algebraic closure. Indeed, $\bar{k}$ is generated over k by $q(x_j(f)$. Let $f = x^n - a_1(f)x^{n-1} + \cdots + (-1)^n a_n(f)$ then

$$j(f) = x^n - q(a_1(f))x^{n-1} + \cdots + (-1)^n q(a_n(f)) = x^n - q(\sigma_1(f))x^{n-1} + \cdots + (-1)^n q(\sigma_n(f)) =$$
$$= q(\prod_{i=1}^n (x - x_i(f)) = \prod_{i=1}^n (x - q(x_i(f)),$$

so f splits in $\bar{k}$ and and $q(x_i(f))$ are algebraic over k.

□

Theorem 13.5. *Let $i : k \to \bar{k}$ and $i' : k \to \bar{k}'$ be two algebraic closures of k, then there exists $j : \bar{k} \cong \bar{k}'$ isomorphism such that $j \circ i = i'$.*

Proof. **Claim** : Let L/k be an algebraic extension and K be algebraically closed then any $i : k \to K$ can be extended to $j : L \to K$.

Proof of claim Let

$$P := \{(L'/k, \theta) | L' \subset L, \theta : L' \to K \text{ extension of } i\}.$$

Usual inclusion of subfields and extension of homomorphism gives P a non empty poset structure. Let C be a chain then $N := \cup_{(L'/k,\theta') \in C} L'$ is subfield of L containing k and using θ' we can construct an extension $\beta : N \to K$ of i. Therefore there exists a maximal element $(L''/k, \theta)$ in P. If $L'' \neq L$, then there exists an $\alpha \in L$ algebraic over L'', therefore algebraic over k. As K is algebraically closed, the minimal polynomial of α has all the roots in K, so fixing a root we can extend θ to $L''(\alpha) \to K$. This contradicts the maximality.

Proof of the theorem There exists an extension of i' given by $j : \bar{k} \to \bar{k}'$. This is injective. Let $\alpha \in \bar{k}'$, then the minimal polynomial of α over k has all the roots in $\bar{k}$, so j is surjective.

□

14. Absolute Galois groups

Definition 14.1. *Let k be a field. k is called sperabely closed if every separable polynomial splits in $k[x]$. A separable closure of k is an algebraic extension K/k such that such that every element of K is seperable over k and K is separably closed*

Exercise 14.2. *Show that the following are equivalent for a extension K/k.*

1. *K/k is a seperable closure.*
2. *K/k is a separable extension and any irreducible separable polynomial $f(x) \in k[x]$ splits in K.*

(3) *K/k is a separable extension and there does not exists any non trivial seprable extension of K.*

Theorem 14.3. *Given any field k, there exists a unique (upto a k-isomorphism) a seprable closure k^{sep}/k.*

Proof. Let $\bar{k}/k$ be an algebraic closure. Then $k^{sep} := \left\{x \in \bar{k} | x \text{ separable over } k\right\}$. Then k^{sep} is seprable closure of k. Let L/k be a seprable extension an let K' be a separably closed field. Then any homomorphism $k \to K'$ can be extended to a homomorphism $L \to K'$ (Exercise). Using this we get the uniqueness.(Exercise). □

Let k^{sep}/k be a separable closure of k. The absolute Galois group G_k of k is defined as

$$G_k := \left\{\sigma : k^{sep} \to k^{sep} | k \text{ isomorphism}\right\}.$$

Let $\sigma \in G_k$ and $\alpha \in k^{sep}$. Let L/k be the splitting field of the minimal polynomial of α. Then L/k is Galois and $\sigma|_L : L \to L$ an k automorphism. Therefore given any L/k normal extension such that $L \subset k^{sep}$. We get a homomorphism $r_L : G_k \to G(L/k)$. These homomorphisms are surjective indeed, we can extend any $\sigma \in G(L/k)$ to a k homomorphism to a k-embedding $\sigma : L \to k^{sep}$. By Zorn's lemma this can be extended to a k-homomorphism $\sigma : k^{sep} \to k^{sep}$, which is surjective (exercise).

Definition 14.4. *Let I be a set with a partial order $\leq$. An inverse system (also called a projective system) indexed by I is a collection of sets (or groups or topological spaces) $(A_i)_{i\in I}$ together with maps (of sets, groups, rings, or topological spaces)*

$$\phi_{ij} : A_i \to A_j$$

for all $j \leq i$ such that $\phi_{ii} = id_{a=A_i}$ and for $k \leq j \leq i$ we have $\phi_{jk} \circ \phi_{ij} = \phi_{ik}$.

Example 14.5.
(1) *Let p be a prime and $A_i := \mathbb{Z}/p^i\mathbb{Z}$ for $i \in \mathbb{N}$ and $\phi_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ be the mod p^j map for $j \leq i$*
(2) *Let R be any ring $A_i := R[x]/x^i$ for $i \in \mathbb{N}$. Similar transition maps.*
(3) *k^{sep}/k seprable closure. Let I be the set of L/k finite Galois extension such that $L \subset k^{sep}$. The partial order is given by inclusion. By Galois correspondence we have, whenever $L \subset L'$ such that $L, L' \in I$, there exists a surjective groups homomorphism $G(L'/k) \to G(L/k)$, whose kernel is the normal subrgoup $G(L'/L)$. This groups are finite , so it has a discrete topology with respect to which these groups are topological groups. This can be done for any extension K/k such that it is separable and normal but not necessarily finite.*

Definition 14.6. *The inverse limit of the system (A_i, ϕ_{ij}) is the set/group/ring/topological space*

$$\lim_{\leftarrow i} A_i := \left\{(a_i)_{i\in I} \in \prod_i A_i | \phi_{ij}(a_i) = a_j, j \leq i\right\}.$$

If A_i's are topological space then we give $\prod_i A_i$ the product topology (that is open sets are product of open sets of each A_i such that only finitely many are not the whole space A_i) and $\lim_{\leftarrow i} A_i$ subspace topology.

Exercise 14.7. *(1) Let R be any ring $A_i := R[x]/x^i$ for $i \in \mathbb{N}$. Similar transition maps. Then show that the map $R[[x]] \to \lim_{\leftarrow i} A_i$ given by $f(x) \mapsto f(x) \mod x^i$ is a ring homomorphism.*

(2) Let p be a prime and $A_i := \mathbb{Z}/p^i\mathbb{Z}$ for $i \in \mathbb{N}$ and $\phi_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ be the mod p^j map for $j \leq i$. Show that $\lim_{\leftarrow i} A_i \cong \mathbb{Z}_p$.

Lemma 14.8. *Let K/k be normal seprable. Let I be the set of L/k finite Galois extension such that $L \subset K$. The partial order is given by inclusion. And let $L/k \in I$, $G(L/k)$ be the corresponding system of groups. Then the restriction map gives an isomorphism*

$$G(K/k) \cong \lim_{\leftarrow L/k \in I} G(L/k).$$

Proof. Let $\sigma \in G(K/k)$ and let $k \subset L' \subset L$ such that $L/k, L'/k \in I$. Then $r_L(\sigma) \in G(L/k)$ and $r_{L'}((\sigma) \in G(L'/k)$. Consider the restriction homomorphism $G(L/k) \to G(L'/k)$ which is surjective. Then $r_L(\sigma)|_{L'} = r_{L'}(\sigma)$. So the restriction homomorphism $r : G(K/k) \cong \lim_{\leftarrow L/k \in I} G(L/k)$ is well defined. Let $r(\sigma) = id$, then for any $\alpha \in K$, there exists a finite Galois extension L/k which is a splitting field of the minimal polynomial of α. Then $r(\sigma)|_L = id$, therefore $\sigma(\alpha) = \alpha$. This implies $\sigma = id$. So r is injective. Fro surjectivity, let $\sigma_L \in G(L/k)$ for $L/k \in I$ satisfy compatibility confition. Then define $\sigma(\alpha) = \sigma|_L(\alpha)$ where L/k is any splitting field of the minimal polynomial of α contaained in K. Because of compatiibility of the $\sigma|_L$'s this is well defined. □

Lemma 14.9 (Topological properties)**.** *Let K/k be a seprable normal extension.*

(1) $G(K/k)$ is compact.
(2) For every $k \subset L \subset K$ such that L/k is normal and seperable, the restriction map $G(K/k) \to G(L/k)$ is surjective and continuous with kernel $G(K/L)$.
(3) For every $k \subset L \subset K$ such that L/k is finite Galois, the subgroup $G(K/L)$ normal open and closed.
(4) For the sub extension L/k finite Galois, gives a basis of open sets $G(K/L)$ at the identity. Therefore $G(K/k)$ is totally disconnected.

Proof. (1) As $G(K/k)$ is a closed subgroups of product of compact groups , therefore Tychonoff implies it is compact.
(2) The restriction map $G(K/k) \to G(L/k)$ is just projection map (inverse limit wise only those finite Galois extension that is inside L is , it is projected).Therefore, surjective and continuous. The kernel is obviously $G(K/L)$. It is closed normal subgroup.
(3) it is obvious.
(4)

□

From now on any normal separable extension (even if infinite) will be called a Galois extension. Let K/k be a Galois extension. Let S_G denote the set of closed subgroups of $G := G(K/k)$ and let S_K denote the set of sub extensions $k \subset L \subset K$.

Theorem 14.10 (Infinite Galois correspondence)**.** *Let K/k be Galois extension. Then there exists an inclusion reversing bijection :*

$$S_G \to S_K$$
$$H \mapsto K^H$$

$$k \subset L \subset K \mapsto G(K/L).$$

Moreover under this correspondence closed normal subgroups corresponds to $k \subset L \subset K$ such that L/k is Galois. The open subgroups corresponds to $k \subset L \subset K$ such that L/k is finite.

Proof. □

15. Hilbert Theorem 90

Theorem 15.1. *Let K/k be a cyclic extension of degree n with Galois group $G = (\sigma)$. Then for any $\alpha \in K$, $tr_{K/k}(\alpha) = 0$ iff $\alpha = \beta - \sigma(\beta)$.*

Proof. Let $\alpha = \beta - \sigma(\beta)$. Then $tr_{K/k}(\alpha) = (\sum_{i=0}^{n-1} \sigma^i(\beta) - \sum_{i=1}^{n} \sigma^i(\beta)) = 0$. For the converse, note that as K/k is Galois, therefore separable. The indepnedence of character result implies that there exists $\theta \in K$ such that $tr_{K/k}(\theta) \neq 0$. That is $\sum_{i=0}^{n-1} \sigma^i(\theta) = 0$. Now it is given that $tr_{K/k}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha) = 0$. Let

$$f(\theta) = \alpha\theta + (\alpha + \sigma(\alpha))(\sigma(\theta)) + \cdots + (\alpha + \sigma(\alpha) + \ldots \sigma^{n-1}(\alpha))(\sigma^{n-1}(\theta)).$$

Then verify (done in class that) $\alpha = f(\theta)/tr_K/k(\theta) - \sigma(f(\theta)/tr_{K/k}(\theta))$.

□

Theorem 15.2. *Let k be a field of characteristic p.*

1. *For any $a \in k$, the polynomial $x^p - x - a$ is either irreducible over k or splits into linear factors over k.*
2. *Let K/k be a cyclic extension of degree p, then K is a splitting filed of some $x^p - x - a \in k[x]$.*

Proof.

1. Let $a \in k$, and let K be a field containing one root say α of the polynomial $f(x) = x^p - x - a$. Then for any $i \in \mathbb{Z}/p\mathbb{Z}$, we get $\alpha + i$ is also a root of $f(x)$. So all the roots of $f(x)$ are $\alpha + i, 0 \leq j \leq p-1$. Therefore K contains all the roots of $f(x)$. Now if $f(x)$ have no roots ion k and suppose $f(x) = g(x).h(x)$, $g(x), h(x) \in k[x]$ non constant. Then in the the splitting field K of $f(x)$ all the roots of $f(x)$ and $g(x)$ is there. Therefore there exists $A \subset \mathbb{Z}/p\mathbb{Z}$ proper non empty subset such that $(\alpha + j)$ for $j \in A$ are the roots of $g(x)$, where $n = |A|$ is the degree of $g(x)$. Therefore the $n-1$-th coefficient of $g(x)$, which is $-\sum_{j\in A}(\alpha + j)$ is in k. So $-n\alpha - \sum_{j\in A} j \in k$. This implies $n\alpha \in k$ and as n is a unit in k we get $\alpha \in k$, which is a contradiction. therefore $f(x)$ is irreducible in $k[x]$.
2. Note that $-1 \in k$ and $Tr_{K/k}(-1) = 0$. Therefore, there exists $\beta \in K$, such that $\beta - \sigma(\beta) = -1$ or $\sigma(\beta) = \beta + 1$. Since K/k is Galois, therefore $\beta \notin k$ and $\sigma^i(\beta) = \beta + j$ for all $0 \leq j \leq p-1$. Now $\sigma(\beta^p - \beta) = (\beta+1)^p - (\beta+1) = \beta^p - \beta$. Therefore $a = \beta^p - \beta \in k$. So , $\beta \in K$ is a root of $f(x) = x^p - x - a$. This has no root in k as $\beta \notin k$. Therefore, f is irreudicble and $k(\beta) \subset K$ is the splitting field whose degree over k is p. But K/k has degree p so $K = k(\beta)$.

□

Definition 15.3. *Let K/k be a Galois extension with Galois group G.*

1. *A map $\alpha : G \to K^*$ is called a 1-cocycle if $\alpha(\sigma \circ \tau) = \alpha(\sigma).\sigma(\alpha(\tau))$ for all $\sigma, \tau \in G$.*

(2) *A map $\alpha : G \to K^*$ is called a 1-coboundary if there exists a $\beta \in K^*$ such that $\alpha(\sigma)) = \sigma(\beta)/\beta$ for all $\sigma \in G$. (In this case $d\beta := \alpha$.)*

Remark 15.4. *Let K/k and G be as above. Then for $\beta \in K^*$, $d\beta$ is a 1-cocycle. Indeed,*

$$d\beta(\sigma\tau) = \sigma(\tau(\beta))/\beta = \sigma(\beta)/\beta.\sigma(\beta)^{-1}\sigma\tau(\beta) =$$
$$= \sigma(\beta)/\beta\sigma(\tau(\beta))/\sigma(\beta) = d\beta(\sigma)\sigma(d\beta(\tau))$$

Definition 15.5. *Let K/k be a Galois extension with Galois group G. Then $H^1(G, K^*) := \frac{1-cocycle}{1-coboundary}$.*

Theorem 15.6. *Let K/k be a Galois extension with Galois group G. Then $H^1(G, K^*) = \bullet$, i.e. every 1-cocycle is a 1-coboundary.*

Proof. Let $G := G(K/k)$. Let $\alpha : G \to K^*$ such that $\alpha(\sigma\tau) = \alpha(\sigma).\sigma(\alpha(\tau))$. We consider the the following function $K \to K$ given by $x \mapsto \sum_{\sigma\in G} \alpha(\sigma)\sigma(x)$. By independence of characters and as $\alpha(\sigma)$'s are non zero we get there exists a $\theta \in K$ such that $0 \neq \delta = \sum_{\sigma\in G} \alpha(\sigma)\sigma(\theta)$. Then for any $\sigma \in G$ we get

$$\sigma(\delta) = \sigma(\sum_{\tau\in G} \alpha(\tau)\tau(\theta)) = \sum_{\tau\in G} \sigma(\alpha(\tau))\sigma(\tau(\theta)) =$$
$$= \sum_{\tau\in G} \alpha(\sigma)^{-1}\alpha(\sigma)\sigma(\alpha(\tau))\sigma(\tau(\theta)) = \sum_{\tau\in G} \alpha(\sigma)^{-1}\alpha(\sigma\tau)\sigma(\tau(\theta)) =$$
$$= \alpha(\sigma)^{-1} \sum_{\tau\in G} \alpha(\sigma\tau)\sigma(\tau(\theta)) = \alpha(\sigma)^{-1}\delta.$$

Let $\beta = \delta^{-1}$. Then $\alpha(\sigma) = \sigma(\beta)/\beta$.

□

Corollary 15.7. *Let K/k be a cyclic Galois extension with $G(K/k) = (\sigma)$ and $[K : k] = n$. Then for any $\alpha \in K$, $N_{K/k}(\alpha) = 1$ iff $\alpha = \sigma(\beta)/\beta$ for some $\beta \in K^*$.*

Proof. If $\alpha = \sigma(\beta)/\beta$. Then

$$N_{K/k}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} (\sigma^i(\sigma(\beta)/\sigma^i(\beta) = 1.$$

On the other hand let $\alpha \in K$ such that $N_{K/k}(\alpha) = 1$. Then the map $\alpha : G \to K^*$ defined by $\alpha(\sigma^i) = \prod_{k=0}^{i-1} \sigma^k(\alpha)$ gives a 1 cocyle. But then it is a coboundary, that is there exists $\beta \in K$, such that $\alpha = \alpha(\sigma) = \sigma(\beta)/\beta$.

□

Theorem 15.8 (Kummer extension)**.** *Let k be a field and let $n \geq 1$ such that $(char(k), n) = 1$ and assume that k contains a primitive n-th root of unity ζ_n. Let K/k be a cyclic extension of degree n, then $\exists\alpha \in k$ such that $K = k(\alpha^{1/n})$.*

Proof. Let ζ_n be a primitive n-th root. Then

$$N_{K/k}(\zeta_n) = \prod_{i=0}^{n-1} \sigma^i(\zeta_n) = \zeta^n = 1.$$

Therefore, there exists $\beta \in K$ such that $\zeta_n = \sigma(\beta)/\beta$. Therefore, $\sigma(\beta) = \zeta_n.\beta$. Then

$$\sigma^i(\beta) = \sigma^{i-1}(\zeta_n.\beta) = \zeta_n.\sigma^{i-1}(\beta) = \zeta_n.\zeta_n^{i-1}.\beta = \zeta_n^i\beta.$$

Note that $\sigma(\beta^n) = \sigma(\beta)^n = \beta^n$. Therefore $\beta^n \in k$. Let $K' = k(\beta)$ and as $\beta \notin k$, we get $k(\beta)/k$ is a non-trivial extension contained in K. Now $[k(\beta) : k]$ is the number of distinct k -homomorphism $k(\beta) \to K$. As each σ^i gives a k homomorphism $k(\beta) \to K$ and they are distinct, therefore $n \leq [k(\beta) : k]$. On the other hand $[k(\beta) : k] \leq n$. Therefore $k(\beta) = K$.

□

Email address: prabrishik@gmail.com