SFU Math 440 Galois Theory
Lecture Notes
Lecturer: Nathan Ilten
Written by: Grayson Davis

Midterm Notes
February 6, 2023 11:37 AM

Field Extension Basics

Def'n: A field extension is a homomorphism $\varphi: L \longrightarrow K$ where L, K are fields.

Remark: Given a field F, there is a unique homomorphism $\psi: \mathbb{Z} \longrightarrow F$, $n \longmapsto \underbrace{1+\dots+1}_{n \text{ times}}$.

Def'n: $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$ is the prime subfield of F if F has characteristic p or 0.

Def'n: The degree of K over L is $[K:L] = \dim_L K$.

Proposition: Let $F \hookrightarrow K$, $K \hookrightarrow L$ be field extensions. Then $[L:F] = [L:K][K:F]$.

Pf: We'll assume $[K:F]$, $[L:K]$ are finite.

Then K has a basis $\{a_1, \dots, a_d\}$ over F, and L has basis $\{b_1, \dots, b_e\}$ over K.

We claim $A = \{a_i b_j\}_{\substack{i=1..d \\ j=1..e}}$ is a basis of L over F.

We first show the elements of A are linearly independent.

Suppose $\sum_{\substack{1 \le i \le d \\ 1 \le j \le e}} c_{ij} a_i b_j = 0$, for $c_{ij} \in F$. Then $\sum_{i,j} c_{ij} a_i b_j = \sum_j \left(\sum_i c_{ij} a_i\right) b_j = 0$.

But $\{b_1, \dots, b_e\}$ is a basis of L over K and $\sum_i c_{ij} a_i \in K$ $\forall 1 \le j \le e$.

Thus, $\sum_i c_{ij} a_i = 0$. But $\{a_1, \dots, a_d\}$ is a basis of K over F, so $c_{ij} = 0$ $\forall i,j$.

To show A is a spanning set of L, take any $\alpha \in L$. Then

$\alpha = \sum_j c_j b_j$, for some $c_j \in K$. But then $c_j = \sum_i f_{ij} a_i$, for some $f_{ij} \in F$.

Thus, $\alpha = \sum_j \left(\sum_i f_{ij} a_i\right) b_j = \sum_{i,j} f_{ij} (a_i b_j)$, so A spans L.

Overall, we see that A is a basis of L over F and

$[L:F] = |A| = de = [L:K][K:F]$. $\square$

Def'n: A field extension $F \longrightarrow K$ is finite if $[K:F]$ is finite.

Def'n: Let F_1, F_2 be subfields of a field K. The compositum of F_1 and F_2 in K is $F_1 F_2$, the smallest subfield of K containing F_1 and F_2.

Def'n: Let $F \rightarrow K$ be a field extension, $S \subseteq K$. Then $F(S)$ is the smallest subfield of K containg S and F. We call $F(S)$ the field generated by S over F.

Def'n: An extension $F \rightarrow K$ is finitely generated if $\exists \alpha_1, \dots, \alpha_n \in K$ such that $F(\alpha_1, \dots, \alpha_n) = K$.

Proposition: If $F \rightarrow K$ is finite, then it is finitely generated.

Pf: Any finite basis of K over F is a generating set of K over F.

Def'n: Let $F \rightarrow K$ be an extension and consider $\alpha \in K$. We say α is algebraic over F is $\exists f \in F[x]$, $f \neq 0$, such that $f(\alpha) = 0$ in K.

Def'n: Let α be algebraic over F. The minimal polynomial of α over F is the monic polynomial of minimal degree in $F[x]$ such that α is a root.

We denote this polynomial as $m_{\alpha,F}$.

Proposition: Suppose α is algebraic over F, $f \in F[x]$ such that $f(\alpha) = 0$.

Then $m_{\alpha,F} \mid f$.

Pf: Suppose $m_{\alpha,F} \nmid f$. Then $\exists q, r \in F[x]$, $\deg(r) < \deg(m_{\alpha,F})$ such that $f = q \cdot m_{\alpha,F} + r$.

But then $r(\alpha) = f(\alpha) - q(\alpha) m_{\alpha,F}(\alpha) = 0$, a contradiction. $\square$

Def'n: The degree of α over F is $\deg(m_{\alpha,F})$.

Proposition: Let α be algebraic over F. Then $F(\alpha) \cong F[x]/\langle m_{\alpha,F}\rangle$.

Pf: Let $\varphi: F[x] \longrightarrow F(\alpha)$

$x \longmapsto \alpha$

$f(x) \longmapsto f(\alpha)$

Then $\ker(\varphi) = \{f \in F[x] \mid f(\alpha) = 0\} = \langle m_{\alpha,F}\rangle$.

But $\langle m_{\alpha,F}\rangle$ is prime, so is maximal. Hence, $F[x]/\langle m_{\alpha,F}\rangle$ is a field.

Thus, by the 1st isomorphism theorem $F[x]/\langle m_{\alpha,F}\rangle \cong \mathrm{im}(\varphi) \subseteq F(\alpha)$.

But then $\mathrm{im}(\varphi)$ is a field containing α and F so $F(\alpha) = \mathrm{im}(\varphi)$. $\square$

Corollary: $[F(\alpha):F] = \deg(m_{\alpha,F})$ = degree of α over F.

Def'n: $F \to K$ is algebraic if every $\alpha \in K$ is algebraic over F.

Lemma: If $F \to K$ is finite, then it is algebraic.

Pf: Take $\alpha \in K$, $\alpha \neq 0$. Then $\alpha^0, \alpha^1, \dots, \alpha^m \in K$ are linearly dependent

if $m > [K:F]$. i.e., $\exists \lambda_i \in F$ so that $\sum_{i=0}^{m} \lambda_i \alpha^i = 0$, with not all $\lambda_i = 0$.

Let $f(x) = \sum_{i=0}^{m} \lambda_i x^i \in F[x]$. Then $f(\alpha) = 0$, so α is algebraic over F. $\square$

Theorem: $F \to K$ is finite if and only if it is finitely generated and algebraic.

Pf: The only if direction follows from previous lemma & theorem.

Suppose $F \to K$ is finitely generated and algebraic. Then let $K = F(\alpha_1, \dots, \alpha_m)$, for $\alpha_i \in K$.

Note each α_i is algebraic over F. Consider $F \hookrightarrow F(\alpha_1) \hookrightarrow \underbrace{F(\alpha_1)(\alpha_2)}_{=F(\alpha_1,\alpha_2)} \hookrightarrow \dots \hookrightarrow \underbrace{F(\alpha_1,\dots,\alpha_{m-1})(\alpha_m)}_{=K}$.

We show each individual extension is finite.

Let $F' = F(\alpha_1, \dots, \alpha_k)$, consider $F' \hookrightarrow F'(\alpha_{k+1})$. α_{k+1} is algebraic over F so $\exists f \in F[x] \setminus \{0\}$

such that $f(\alpha_{k+1}) = 0$. But then α_{k+1} is algebraic over F'. By the above corollary,

$[F'(\alpha_{k+1}):F'] = \deg_{F'}(m_{\alpha,F'})$ is finite. Hence, since the composition of finite

extensions is finite, $[K:F]$ is finite. $\square$

Corollary: Compositions of $\begin{bmatrix}\text{algebraic}\\ \text{finitely generated}\end{bmatrix}$ field extensions are $\begin{bmatrix}\text{algebraic}\\ \text{finitely generated}\end{bmatrix}$.

Pf: Let $F \to K$, $K \to L$ be finitely generated. Then let $K = F(\alpha_1, \dots, \alpha_m)$, $\alpha_i \in K$, $L = K(\beta_1, \dots, \beta_n)$, $\beta_j \in L$.

Then $L = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ so L is finitely generated over F.

Let $F \to K$, $K \to L$ be algebraic. Choose $\alpha \in L$, we show α is algebraic over F.

Let $m_{\alpha,K} = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in K[x]$. Then $m_{\alpha,K} \in F(c_0, \dots, c_{n-1})[x]$. Let $K' = F(c_0, \dots, c_{n-1})$.

Then $K'(\alpha) \cong K'[x]/\langle m_{\alpha,K'}\rangle$ is finite over K'. In particular, we have that

$F \longrightarrow K' \longrightarrow K'(\alpha)$ is a composition of finite extensions, so $F \to K'(\alpha)$ is finite. But then

α is algebraic over F (note: $K'(\alpha) \subseteq L$). $\square$

Def'n: A field F is algebraically closed if every non-constant $f \in F[x]$ has a root in F.

Proposition: If F is algebraically closed, then every $f \in F[x]$ non-constant factors completely.

Pf: Consider $f \in F[x]$, non-constant. Then f has a root in F, say α, so $f = (x-\alpha)g$, for some

$g \in F[x]$ of degree less than f. We can repeat this process on g until f factors completely (by induction).

$\square$

Proposition: F is algebraically closed if and only if every algebraic extension $F \to K$ has $[K:F]=1$.

Pf: Consider any algebraic $F \to K$, let $\alpha \in K$. Then α is a root of $m_{\alpha,F} \in F[x]$. But $m_{\alpha,F}$ is irreducible over F. Since F is algebraically closed, $m_{\alpha,F} = x-\alpha$, so $\alpha \in F$ and hence $K=F$. Thus, $[K:F]=1$.

Conversely, assume $[K:F]=1$ for every algebraic extension $F \to K$. Let $f \in F[x]$ be non-constant. Write $f = f_1 \cdots f_k$, for f_i irreducible. Then $F \to F[x]/\langle f_1 \rangle$ is algebraic so $[F[x]/\langle f_1\rangle : F] = 1$. i.e., $F \cong F[x]/\langle f_1 \rangle$. But then $\deg(f_1) = 1$ so f has a linear factor in $F[x]$, and so f has a root in F. Thus, F is algebraically closed.

$\square$

Theorem (Kronecker): Let F be a field, $f \in F[x]$ non-constant. Then there is a finite extension $F \to K$ so that f has a root in K.

Pf: Write $f = f_1 \cdots f_m \in F[x]$ such that $f_i \in F[x]$ is irreducible.

Consider $F \to K$, where $K := F[x]/\langle f_1 \rangle$.

Let $\alpha = \bar{x} \in K$. Then $f(\alpha) = f(\bar{x}) = \overline{f(x)} = \overline{f_1(x)} \cdots \overline{f_m(x)} = 0$ in $F[x]/\langle f_1 \rangle$.

$\square$

Def'n: An algebraic closure of F is an algebraic extension $F \to K$ such that K is algebraically closed.

Remark: An algebraic extension K of F is an algebraic closure of f if $\forall f \in F[x]$ non-constant

(*) f factors in $K[x]$ as a product of linear factors

(**) f has at least one root in K

Fact: Requiring (**) is equivalent to K being algebraically closed.

Theorem: Every field F has an algebraic closure.

Pf: Let $F \to L_1$ be an algebraic extension such that any $f \in F[x]$ non-constant has a root in F (Kronecker's Theorem).

We can apply this same idea to get $L_1 \to L_2$ algebraic such that each non-constant $f \in L_1[x]$ has a root in L_2.

We continue inductively so that $L_i \to L_{i+1}$ satisfies this property. Let $L = \bigcup_{i\in\mathbb{N}} L_i$. We claim L is an algebraic closure of F.

Firstly, we show L is a field. Consider $\alpha, \beta \in L$. Then $\exists N, N' \in \mathbb{N}$ such that $\alpha \in L_N$, $\beta \in L_{N'}$. But then $\exists M \in \mathbb{N}$ so that $\alpha, \beta \in L_M$. But L_M is a field, so $\alpha+\beta \in L_M$, $\alpha\beta \in L_M$. But $L_M \subseteq L$, so L is closed under the operations.

Similarly, the other field axioms hold.

Second, we show $F \to L$ is algebraic. Consider any $\alpha \in L$. Then $\exists N \in \mathbb{N}$ so that $\alpha \in L_N$.

Compositions of algebraic extensions are algebraic, so $F \to L_N$ is algebraic. Hence, α is algebraic over F.

Thus, each $\alpha \in L$ is algebraic over F.

Lastly, we show each non-constant $f \in F[x]$ factors completely in $L[x]$.

Consider any $f \in F[x]$ of degree n. Then in $L_1[x]$, $f = \ell_1 g_1$, for $\ell_1, g_1 \in L_1[x]$, ℓ_1 linear.

Similarly, in L_2, $g_1 = \ell_2 g_2$, for some $\ell_2, g_2 \in L_2[x]$, ℓ_2 linear. We can continue this process n times, as in if $g_i \in L_i[x]$ factors as $\ell_{i+1} g_{i+1}$, for $\ell_{i+1}, g_{i+1} \in L_{i+1}[x]$, with ℓ_{i+1} linear, then $\deg(g_i) = n-i$, so $\deg(g_{i+1}) = n-(i+1)$.

Hence, this process terminates in $L_n[x] \subseteq L[x]$, so f factors linearly in $L[x]$.

Thus, L is an algebraic closure of F.

$\square$

Theorem: Let K, K' be algebraic closures of a field F. Then there is an isomorphism $\varphi: K \longrightarrow K'$ which makes

$$\begin{tikzcd} F \arrow[r] \arrow[dr] & K \arrow[d, dashed, "\varphi"] \\ & K' \end{tikzcd}$$

commute. Note: φ is not unique, unless $F = K$.

Pf: See lecture notes.

Symmetric Polynomials

Note: Let $\sigma \in S_n$, and $f \in F[x_1, \dots, x_n]$, where F is a field. Then $\sigma \cdot f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Def'n: Let F be a field. We define $F[x_1, \dots, x_n]^{S_n} := \{f \in F[x_1, \dots, x_n] \mid \forall \sigma \in S_n,\ \sigma \cdot f = f\}$.

We call this the ring of symmetric polynomials in n variables.

Def'n: Let F be a field. Consider $\prod_{i=1}^{n}(y - x_i) \in F[x_1, \dots, x_n][y]$. Then

$\prod_{i=1}^{n}(y - x_i) = y^n - s_1 y^{n-1} + s_2 y^{n-2} - \dots + (-1)^n s_n$, where $s_1 = x_1 + x_2 + \dots + x_n$, $s_2 = x_1x_2 + x_1x_3 + \dots + x_ix_n, \dots, s_n = x_1x_2\dots x_n$.

We call $\{s_1, \dots, s_n\}$ the elementary symmetric polynomials in n variables.

Remark: Each s_i is symmetric since $\prod_{i=1}^{n}(y - x_i)$ is invariant under S_n.

Remark: Each s_i is homogenous of degree i.

Theorem (Fundamental Theorem of Symmetric Polynomials): Let F be a field. Then $F[x_1, \dots, x_n]^{S_n} = F[s_1, \dots, s_n]$.

That is, every symmetric polynomial is a polynomial in $s_1, \dots, s_n$, and there are no algebraic relations among the $s_1, \dots, s_n$.

Pf: See lecture notes/Assignment 3.

Remark: Let $f = y^n + a_{n-1}y^{n-1} + \dots + a_0 \in F[x]$. Then in $\bar{F}[y]$, $f = \prod_{i=1}^{n}(y - \alpha_i)$, where α_i is a root of f.

In particular, we have that $a_i = (-1)^{n-i} s_{n-i}(\alpha_1, \dots, \alpha_n)$, so symmetric expressions in $\alpha_1, \dots, \alpha_n$ are polynomials in $a_0, \dots, a_{n-1}$.

Def'n: Let F be a field and $f \in F[x]$. Assume F has roots $\alpha_1, \dots, \alpha_n \in \bar{F}$. We define the discriminant of f to be $\Delta(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Note: $\Delta(f)$ is symmetric in the roots of f, so is a polynomial in the coefficients of f.

Group Theory Basics

Def'n: A group $(G, \cdot)$ is a set G with a binary operation $\cdot : G \times G \longrightarrow G$, $(g, h) \longmapsto g \cdot h$ such that

1) The operation is associative.
2) $\exists e \in G$ such that $\forall g \in G$, $e \cdot g = g \cdot e = g$.
3) $\forall g \in G\ \exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Def'n: Let $(G, \cdot)$ be a group. If $\forall g, h \in G$, $g \cdot h = h \cdot g$, we call G abelian.

Def'n: Let K be a field. We define the automorphism group of K as

$\mathrm{Aut}(K) := \{\sigma : K \to K \mid \sigma \text{ is a field isomorphism}\}$

Def'n: Let $F \to K$ be an extension. The Galois Group of K over F is

$\mathrm{Gal}(K/F) := \{\sigma \in \mathrm{Aut}(K) \mid \sigma|_F = \mathrm{id}_F\}$.

Remark: If F is the prime subfield of K, then $\mathrm{Gal}(K/F) = \mathrm{Aut}(K)$.

Proposition: Let $F \to K$ be an extension. Consider $f \in F[x]$ and suppose $\alpha \in K$ is a root of f.

Then $\forall \sigma \in \mathrm{Gal}(K/F)$, $\sigma(\alpha)$ is a root of f. That is, any $\sigma \in \mathrm{Gal}(K/F)$ maps roots of f to roots of f.

Pf: Write $f = \sum_{j=0}^{n} c_j x^j \in F[x]$. Since σ is a field isomorphism with $\sigma|_F = \mathrm{id}_F$,

$\forall a,b \in K$, $\sigma(a+b) = \sigma(a)+\sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$, and if $a \in F$, $\sigma(a) = a$. Thus,

$$0 = \sigma(0) = \sigma(f(\alpha)) = \sigma\left(\sum_{j=0}^{n} c_j \alpha^j\right) = \sum_{j=0}^{n} \sigma(c_j)\sigma(\alpha^j) = \sum_{j=0}^{n} c_j (\sigma(\alpha))^j = f(\sigma(\alpha)).$$

So $\sigma(\alpha)$ is a root of f. $\square$

Theorem: Let G be a group. Then

1) The identity element is unique
2) The inverse of each $g \in G$ is unique
3) $\forall a,b,c \in G$, $ac = bc$ implies $a = b$, $ca = cb$ implies $a = b$.

Pf: 1) Suppose $e, e' \in G$ are both the identity. Fix $g \in G$. Then $e = gg^{-1} = e'$.

2) Suppose $g \in G$ has inverses $h, h' \in G$. Then $h = h(gh') = (hg)h' = h'$.

3) Follows immediately by multiplication by inverses. $\square$

Def'n: Let G be a group. A subgroup of G is a set $H \subseteq G$ such that H is a group. If H is a subgroup of G, we write $H \leq G$.

Def'n: Let G be a group and $X \subseteq G$. Then the subgroup generated by X is

$\langle X \rangle :=$ the smallest subgroup of G containing X.

Def'n: Let G be a group. Then the center of G is $Z(G) := \{g \in G \mid \forall x \in G, gx = xg\}$.

Proposition: Let G be a group. Then $Z(G) \leq G$.

Pf: Consider $g, h \in Z(G)$.

i) Fix $x \in G$. Then $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$, so $gh \in Z(G)$.

ii) Fix $x \in G$. Then $gx = xg$, so $g^{-1}(gx)g^{-1} = g^{-1}(xg)g^{-1}$, and thus $xg^{-1} = g^{-1}x$, so $g^{-1} \in Z(G)$.

Also, it is clear $e \in Z(G)$, so $Z(G) \leq G$. $\square$

Group Actions

Def'n: Let G be a group and X a set. An action of G on X is a map

$G \times X \longrightarrow X$, where $(g,x) \in G \times X$ is mapped to $g.x \in X$ such that

1) $\forall x \in X$, $e.x = x$
2) $\forall g,h \in G, \forall x \in X$, $g.(h.x) = (gh).x$.

Def'n: Let $G \times X \longrightarrow X$ be an action. The orbit of $x \in X$ is

$$G.x := \{g.x \mid g \in G\} \subseteq X$$

Def'n: Let $G \times X \to X$ be an action. The stabilizer of $x \in X$ is

$$G_x := \{g \in G \mid g.x = x\} \subseteq G$$

Proposition: Let $G \times X \to X$ be an action. Take $x, y \in X$. Then

1) $x \in G.x$
2) $y \in G.x$ if and only if $G.x = G.y$

Pf: 1) is immediate as $e.x = e$.

2) Suppose $y \in G.x$. We show $G.x = G.y$.

Since $y \in G.x$, there is $h \in G$ such that $y = h.x$. In particular, we see that $h^{-1}.y = h^{-1}.(h.x) = (h^{-1}h).x = x$.

Consider any $z \in G.x$. Then $z = g.x$, for some $g \in G$. But then $z = g.(h^{-1}.y) = (gh^{-1}).y \in G.y$, so $G.x \subseteq G.y$.

Consider any $z \in G.y$. Then $z = g.y$, for some $g \in G$. But then $z = g.(h.x) = (gh).x \in G.x$, so $G.y \subseteq G.x$.

Overall, we have $G.x = G.y$.

Conversely, if $G.x = G.y$, then 1) gives $y \in G.x$. $\square$

Remark: If $G.x \cap G.y \neq \emptyset$, then $G.x = G.y$.

Pf: Let $z \in G.x \cap G.y$. Then $z \in G.x$ and $z \in G.y$. The above proposition gives $G.x = G.z = G.y$ $\square$

Def'n: Let $G \times X \to X$ be an action. Define $X/G := \{G.x \mid x \in X\}$, the set of all orbits.

Theorem: X/G partitions X.

Pf: Follows from the above proposition/remark.

Def'n: Let G be a group and $H \leq G$. Define the action $\begin{aligned} H \times G &\longrightarrow G \\ (h,g) &\longmapsto gh^{-1} \end{aligned}$.

The orbits of the action are $H.g = \{gh^{-1} \mid g \in G\} = \{gh' \mid h' \in H\} = gH$.

We say an orbit of this action is a left coset of H in G.

We define G/H to be the set of left cosets of H.

Remark: The above theorem tells us that G/H partitions G.

Theorem: Let G be a group, $H \leq G$. Consider $g, k \in G$. Then

1) If $gH \subseteq kH$, then $gH = kH$

2) If $gH \cap kH \neq \emptyset$, then $gH = kH$

3) $gH = kH$ if and only if $g^{-1}k \in H$

Pf: 1) and 2) hold as left cosets partition G (noted above).

We have $gH = kH$ if and only if $g \in kH$ if and only if there is $h \in H$ so that $g = kh$.

But this holds if and only if $h = k^{-1}g \in H$, so 3) holds. $\square$

Def'n: Let G be a group, $H \leq G$. The index of H in G is $[G:H] := \#G/H$.

Def'n: Let G be a group, $H \leq G$. Consider the action $\begin{aligned} H \times G &\longrightarrow G \\ (h,g) &\longmapsto hgh^{-1} \end{aligned}$. We call the orbits of this action the conjugacy classes of G under conjugacy by H.

Remark: $H.g = H.g'$ if and only if $\exists h \in H$ such that $ghg^{-1} = g'$.

Remark: If $x \in Z(G)$, the conjugacy class of x is $\{x\}$

Pf: $\forall g \in G$, $gxg^{-1} = gg^{-1}x = ex = x$, so $G.x = \{x\}$ $\square$

Remark: Since orbits are a partition of G, the conjugacy classes of G partition G.

Proposition: Let $G \times X \to X$ be an action, $x \in X$. Then $G_x \leq G$.

Pf: Consider any $g, h \in G_x$.

i) $g.x = x$, and $h.x = x$, so $(gh).x = g.(h.x) = g.x = x$. Thus, $gh \in G_x$.

ii) $g.x = x$, so $x = e.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.x$. Thus, $g^{-1} \in G_x$.

It is clear $e \in G_x$, so $G_x \leq G$. $\square$

Theorem (Orbit-Stabilizer Theorem):

Let $G \times X \to X$ be an action. Consider $x \in X$. Then there is a bijection $\varphi: G.x \to G/G_x$.

Pf: Consider $\varphi: G \to G.x$ This is a surjective map. Assume $\varphi(g) = \varphi(h)$ for some $g, h \in G$. We show $gG_x = hG_x$

Let $G\times X \to X$ be an action. Consider $x\in X$. Then there is a bijection $\Psi: G.x \to G/G_x$.

Pf: Consider $\begin{array}{l}\varphi: G \to G.x \\ \quad g \mapsto g.x\end{array}$. This is a surjective map. Assume $\varphi(g)=\varphi(h)$ for some $g,h\in G$. We show $gG_x = hG_x$.

We have $\varphi(g)=\varphi(h)$ if and only if $g.x = h.x$ if and only if $(g^{-1}h).x = x$ if and only if $g^{-1}h \in G_x$.

But by the theorem on cosets, this holds if and only if $gG_x = hG_x$, as desired. Thus, we define

$\Psi: G/G_x \to G.x$ where $\Psi(gG_x) = g.x$. The above gives that this map is well-defined.

Also, if $\Psi(gG_x) = \Psi(hG_x)$, then $g.x = h.x$ so by above $gG_x = hG_x$ $\therefore$ Ψ is injective.

Furthermore, if $g.x\in G.x$, then $gG_x \mapsto g.x$ so the map is indeed a bijection. $\square$

Theorem (Lagrange): Let G be a finite group, $H\le G$. Then $\#G = [G:H]\#H$.

Pf: G/H partitions G, so $\#G = \sum_{C\in G/H} \#C$. We show $\#C = \#H$ for all $C\in G/H$.

Recall, gH is an orbit of G under the action $\begin{array}{l}H\times G \to G \\ (h,g)\mapsto gh^{-1}\end{array}$.

By the Orbit-Stabilizer Theorem, $\#gH = \#H.g = \#H/H_g$.

But $H_g = \{h\in H \mid gh^{-1} = g\} = \{e\}$. Hence, each left coset has size $\#H$. This gives

$\#G = \sum_{C\in G/H} \#C = [G:H]\#H$. $\square$

Corollary: Let G be a finite group and $G\times X\to X$ an action. Let $x\in X$. Then $\#G.x = [G:G_x] = \frac{\#G}{\#G_x}$.

Pf: $\#G.x = [G:G_x]$ by the Orbit-Stabilizer Theorem. But $G_x \le G$ and G is finite, so the claim holds by Lagrange. $\square$

Corollary (Class Equation): Let G be a finite group, and $\begin{array}{l}G\times G \to G \\ (g,h)\mapsto ghg^{-1}\end{array}$.

Then $\#G = \sum_{\substack{\text{conjugacy} \\ \text{classes } C}} [G:G_{x_C}] = \#Z(G) + \sum_{\substack{\text{non-central} \\ \text{conjugacy} \\ \text{classes, } C}} [G:G_{x_C}]$. Where $x_C \in C$. (Note: $\#C = [G:G_{x_C}]$ by Orbit-Stabilizer Theorem).

Pf: Recall, if $x\in Z(G)$, the conjugacy class of x is $\{x\}$. We have

$\#G = \sum_{\substack{\text{conjugacy} \\ \text{classes, } C}} \#C = \#Z(G) + \sum_{\substack{C \text{ non-} \\ \text{central}}} \#C = \#Z(G) + \sum [G:G_{x_C}]$, by Orbit-Stabilizer Theorem. $\square$

Group Homomorphisms and Normal Subgroups

Def'n: A homomorphism from a group G to a group H is a map $\varphi: G\to H$ such that $\forall a,b\in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.

We say a homomorphism is an isomorphism if φ is bijective.

Remark: If $\varphi: G\to H$ is a group isomorphism, then so is $\varphi^{-1}: H\to G$.

Def'n: The kernel of a homomorphism $\varphi: G\to H$ is $\ker\varphi := \{g\in G \mid \varphi(g) = e_H\}$.

Remark: $\ker\varphi \le G$.

Def'n: Let G be a group, $H\le G$. We say H is normal if $\forall g\in G\ \forall h\in H$, $ghg^{-1}\in H$.

If H is normal, we write $H \trianglelefteq G$.

Theorem: Let G be a group, $H\le G$. Then the following are equivalent:

1) H is normal $(H\trianglelefteq G)$
2) $\forall g\in G$, $gHg^{-1} \subseteq H$
3) $\forall g\in G$, $gHg^{-1} = H$
4) $\forall g\in G$, $gH = Hg$

Pf:

1) $\Longrightarrow$ 2) This follows from the definition of $H\trianglelefteq G$ ($\forall g\in G, \forall h\in H$, $ghg^{-1}\in H$).

2) $\Longrightarrow$ 3) Suppose $gHg^{-1} \subseteq H$, for any $g\in G$. Then since $g^{-1}\in G$, $g^{-1}Hg \subseteq H$.

1) $\Longrightarrow$ 2) This follows from the definition of $H \trianglelefteq G$ ($\forall g \in G, \forall h \in H$, $ghg^{-1} \in H$).

2) $\Longrightarrow$ 3) Suppose $gHg^{-1} \subseteq H$, for any $g \in G$. Then since $g^{-1} \in G$, $g^{-1}Hg \subseteq H$.

Also, if $ghg^{-1} \in gHg^{-1}$, $\exists h' \in H$ so that $ghg^{-1} = h'$. Hence, $h = g^{-1}h'g \in g^{-1}Hg$.

Thus, $g^{-1}Hg = H$, so $H = gHg^{-1}$.

3) $\Longrightarrow$ 4) If $\forall g \in G$, $gHg^{-1} = H$, then $gH = \{gh \mid h \in H\} = \{(ghg^{-1})g \mid h \in H\} = (gHg^{-1})g = Hg$.

4) $\Longrightarrow$ 3) If $gH = Hg$ $\forall g \in G$, then $gHg^{-1} = (gH)g^{-1} = (Hg)g^{-1} = H(gg^{-1}) = H$.

4) $\Longrightarrow$ 1) From above, $\forall g \in G$, $gH = Hg$ implies $H = gHg^{-1}$ $\forall g \in G$. Hence, $\forall h \in H$, $ghg^{-1} \in H$ so $H \trianglelefteq G$. □

Theorem: Let G be a group, $H \leq G$. If H is normal, then G/H is a group, with operation

$$(gH)(kH) = (gk)H$$

Pf: We need to show that if $x, y, x', y' \in G$ so that $xH = x'H$, $yH = y'H$, then $xyH = x'y'H$.

Note, $x'H = xH$, $y'H = yH$ imply $(x')^{-1}x, (y')^{-1}y \in H$. Thus, $x'y'H = x'y'((y')^{-1}y)H = x'(y'y'^{-1})y = x'yH = x'Hy$

Now, $x'Hy = x'(x'^{-1}x)Hy = xHy = xyH$, so the operation is well-defined.

Associativity follows from associativity in G, H is the neutral element, and $(gH)^{-1} = g^{-1}H$. □

Proposition: Let $\varphi: G \to K$ be a group homomorphism. Then $\ker(\varphi) \trianglelefteq G$.

Pf: Previous theorem gives $\ker(\varphi) \leq G$. Fix $g \in G, h \in \ker(\varphi)$. Then

$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e_H$, so $ghg^{-1} \in \ker(\varphi)$. i.e., $\ker(\varphi) \trianglelefteq G$. □

Proposition: Let G be a group. Then if $H \trianglelefteq G$, there exists a homomorphism $\pi: G \to G/H$ with $\ker(\pi) = H$. We call this the natural homomorphism.

Pf: Define $\pi: G \to G/H$, $g \mapsto gH$. This is well-defined. Also, if $g, h \in G$, $\pi(gh) = (gh)H = (gH)(hH) = \pi(g)\pi(h)$, as H is normal. Thus, π is a homomorphism. $\ker(\pi) = \{g \in G \mid \pi(g) = gH = H\} = H$. □

Theorem (First Isomorphism Theorem for Groups): Let $\varphi: G \to H$ be a group homomorphism.

Then there is a map $\psi: G/\ker(\varphi) \to H$ such that ψ induces an isomorphism between $G/\ker(\varphi)$ and $\mathrm{im}(\varphi)$.

Proof: See lecture notes.

Proposition: A group action $\rho: G \times X \to X$ is equivalent to a homomorphism $\varphi: G \to S_X$, where $\varphi(g) = [x \mapsto \rho(g,x)]$, $\rho(g,x) = \varphi(g)(x)$.

Theorem (Cayley): Every finite group is isomorphic to a subgroup of S_n, for some $n \in \mathbb{N}$.

Pf: Let G be a finite group. Consider the action $G \times G \to G$, $(g,h) \mapsto gh$. This induces a homomorphism $\varphi: G \to S_G$, $g \mapsto [h \mapsto gh]$. We have that $\ker(\varphi) = \{g \in G \mid \forall h \in G, gh = h\} = \{e\}$.

Thus, φ is injective. Let $n = \#G$. Then $S_n \cong S_G$. By the first isomorphism theorem, $G \cong \mathrm{im}(\varphi)$. But the image of a homomorphism is a subgroup of the codomain. □

Normal Field Extensions

Def'n: Let F be a field, $S = \{f_\alpha\}_{\alpha \in I}$, $f_\alpha \in F[x]$. A splitting field of S over F is an extension $F \to K$ such that K is generated over F by all the roots (in $\overline{F}$) of the f_α.

Lemma (Extension Lemma): Let $F \to K$, $F \to K'$ be extensions. Assume $\sigma: K \to K'$ is an isomorphism.

Also let $\rho: K \to L$ be an algebraic extension and $\rho': K' \to \overline{F}$ be an extension. Then there is an

ρ' algebraic

Lemma (Extension Lemma): Let $F \to K$, $F \to K'$ be extensions. Assume $\sigma : K \to K'$ is an isomorphism. Also let $\rho : K \to L$ be an algebraic extension and $\rho' : K' \to \bar{F}$ be an extension. Then there is an extension $\varphi : L \to \bar{F}$ such that $\varphi \circ \rho = \rho' \circ \sigma$. Pictorally, we have

$$\begin{tikzcd} & K \arrow[r, "\rho - \text{algebraic}"] \arrow[d, "\sigma"', "\wr"] & L \arrow[d, dashed, "\varphi"] \\ F \arrow[ur] \arrow[dr] & & \\ & K' \arrow[r, "\rho'"] & \bar{F} \end{tikzcd}$$

Pf: See lecture notes for sketch.

Def'n: An extension $F \to K$ is normal if $m_{\alpha,F}$ splits in $K[x]$ for every $\alpha \in K$.

Theorem: Let $F \to K$ be an algebraic extension, $K \subseteq \bar{F}$. The following are equivalent:

1) K is a splitting field
2) Every $\sigma : K \to \bar{F}$ which fixes F induces an automorphism of K.
3) K is normal

Pf: 1) $\Longrightarrow$ 2) Assume K is a splitting field of $S \subseteq F[x]$. Consider $\sigma : K \to \bar{F}$ fixing F. K is a splitting field, so K is generated by $\{\alpha \mid \alpha \in \bar{F}$ is a root of $f \in S\}$. But $\sigma(\alpha)$ must be a root of f (for any α), so $\sigma(\alpha) \in K$. Thus, $\sigma(K) \subseteq K$.

We show σ is surjective. It suffices to show that $\forall f \in S$, if α is a root of f, then $\alpha \in \sigma(K)$. Since σ permutes roots of f, and there are only finitely many roots, we have that any root of f is in $\sigma(K)$. Thus, since K is the splitting field of S, $K \subseteq \sigma(K)$, so $K = \sigma(K)$.

3) $\Longrightarrow$ 1) Let $S = \{m_{\alpha,F} \mid \alpha \in K\}$. Then K is the splitting field of S.

2) $\Longrightarrow$ 3) Let $\alpha \in K$ and $\alpha' \in \bar{F}$ be a root of $m_{\alpha,F}$. We have

$$\begin{tikzcd} & F(\alpha) \arrow[r] \arrow[d, "\wr"] & K \\ F \arrow[ur] \arrow[dr] & & \\ & F(\alpha') \arrow[r, hook] & \bar{F} \end{tikzcd}$$

$F(\alpha) \to K$ is algebraic, so by the extension lemma, there is $\varphi : K \to \bar{F}$ fixing F. By 2), $\varphi(K) = K$, so $\varphi(\alpha) = \alpha' \in K$. Hence, any other root of $m_{\alpha,F}$ is in K, so $m_{\alpha,F}$ splits completely in $K[x]$. Thus, K is normal. $\square$

Proposition: Let $S \subseteq F[x]$. Let K, K' be splitting fields for S over F. Then $K \cong K'$.

Pf: See lecture notes.

Remark: If $F \hookrightarrow K$, $F \hookrightarrow K'$ are normal extensions with $K, K' \subseteq L$, L a field. Then KK' is normal over F.

Pf: Since K, K' are normal over F, there are $S, S' \subseteq F[x]$ such that $K = SF(S)$, $K' = SF(S')$. Then $KK' = SF(S \cup S')$, so KK' is normal over F. $\square$

Remark: Let $F \to K \to L$ be extensions. If L is normal over F, then L is normal over K.

Pf: Since L is normal over F, $\exists S \subseteq F[x]$ so that $L = SF_F(S)$. But $SF_F(S) = SF_K(S)$. Hence, L is normal over K. $\square$

Def'n: The normal closure, K^{norm}, of K over F is the subfield of $\bar{F}$ generated by all $\sigma(K)$, where $\sigma : K \to \bar{F}$ fixes F.

Remark: This is the smallest normal subfield of $\bar{F}$ containing K.

Separable Extensions

Def'n: Let $F \to K$ be an algebraic extension. Define the separable degree of K over F as

$[K:F]_s := \#\{\sigma: K \to \overline{F} \mid \sigma|_F = \text{inclusion}\}$

Lemma: Suppose $\phi: F \to F' \subseteq \overline{F}$ is an isomorphism. Let K be algebraic over F. Then

$$[K:F]_s = \#\{\sigma: K \to \overline{F} \mid \sigma|_F = \phi\}$$

Pf: See lecture notes.

Theorem: Let $F \to K \to L$ be algebraic extensions. Then $[L:F]_s = [L:K]_s [K:F]_s$

Pf: Assume all quantities are finite. We have that

$$[L:F]_s = \#\{\sigma: L \to \overline{F} \mid \sigma|_F = id\} = \sum_{\substack{\tau: K \to \overline{F} \\ \tau|_F = id}} \#\{\sigma: L \to \overline{F} \mid \sigma|_K = \tau\}$$

$$= \sum_{\substack{\tau: K \to \overline{F} \\ \tau|_F = id}} [L:K]_s = [K:F]_s [L:K]_s$$

$\square$

Theorem: Let $F \to K$ be algebraic. Then $[K:F]_s \leq [K:F]$.

Pf: Without loss of generality, assume $[K:F]$ is finite. $F \to K$ is algebraic, so we have

$F = F_0 \to F(\alpha_1) = F_1 \to F_1(\alpha_2) = F_2 \to \dots \to F_m = K$, and so

$[K:F] = \prod_{i=1}^{m} [F_i : F_{i-1}]$, $[K:F]_s = \prod_{i=1}^{m} [F_i : F_{i-1}]_s$. Thus, it suffices to show $[F_i : F_{i-1}] \geq [F_i : F_{i-1}]_s, \forall i \in \{1, \dots, m\}$.

Consider $F \to F(\alpha) \subseteq \overline{F}$ algebraic. Then any $\sigma: F(\alpha) \to \overline{F}$ fixing F must map a root of $m_{\alpha,F}$ to a root of $m_{\alpha,F}$. That is, $[F(\alpha):F]_s = \#$ distinct roots of $m_{\alpha,F} \leq \deg(m_{\alpha,F}) = [F(\alpha):F]$. $\square$

Def'n: A finite extension $F \to K$ is separable if $[K:F]_s = [K:F]$.

Theorem: Let $F \to K$ be normal, separable, and finite. Then $\#Gal(K/F) = [K:F]$.

Pf: Recall, $Gal(K/F) = \{\sigma: K \to K \mid \sigma|_F = id\}$. Consider any $\sigma: K \to \overline{F}$ such that $\sigma|_F = id$.

Then since $F \to K$ is normal, $\sigma(K) = K$. Thus,

$[K:F] = [K:F]_s = \#\{\sigma: K \to \overline{F} \mid \sigma|_F = id\} = \#\{\sigma: K \to K \mid \sigma|_F = id\} = \#Gal(K/F)$. $\square$

Def'n: Let $F \to K \subseteq \overline{F}$ be an extension. We say $\alpha \in K$ is separable over F if $m_{\alpha,F}$ has no multiple roots.

Remark: This is equivalent to saying $F \to F(\alpha)$ is separable.

Proposition: Let $F \to K$ be a finite extension. Then $F \to K$ is separable if and only if $\forall \alpha \in K$, α is separable.

Pf: Suppose $F \to K$ is separable. Consider any $\alpha \in K$. Then

$[K:F] = [K:F]_s = [K:F(\alpha)]_s [F(\alpha):F]_s \leq [K:F(\alpha)][F(\alpha):K] = [K:F]$

Thus, $[K:F(\alpha)]_s = [K:F(\alpha)]$, and $[F(\alpha):F]_s = [F(\alpha):F]$, so α is separable.

Suppose instead each $\alpha \in K$ is separable. Then $F \to K$ is the tower

$F \to F(\alpha_1) \to F(\alpha_1)(\alpha_2) \to \dots \to K$.

But each individual extension is separable, so $[K:F]_s = [K:F(\alpha_1, \dots, \alpha_m)]_s \cdot \ldots \cdot [F(\alpha_1):F]_s = [K:F(\alpha_1, \dots, a_m)] \cdot \ldots \cdot [F(\alpha):F] = [K:F]$.

Thus, $F \to K$ is separable. $\square$

Remark: If F has characteristic zero, and $F \to K$ is an extension, then every $\alpha \in K$ is separable.

Pf: Consider any $\alpha \in K$ and let $f = m_{\alpha,F} \in F[x]$. Set $g = f'$. f is irreducible, so $\deg(f) \geq 1$. Let $f = a_0 + \dots + a_d x^d$.

Then $g = a_1 + \dots + dx^{d-1} \neq 0$. If f has a repeated root at $\beta \in K$, then $f(\beta) = g(\beta) = 0$. But then

$m_{\beta,F} \mid g$. However, $m_{\beta,F} \mid f$ as well, but f is irreducible so $\deg(m_{\beta,F}) = \deg(f) > \deg(g)$, a contradiction.

Thus, f has no repeated roots, so α is separable over F. $\square$

Theorem (Theorem of the Primitive Element): Let $F \to K$ be a finite and separable extension. Then there is $\alpha \in K$ such that $K = F(\alpha)$.

Pf: For now, assume F is infinite. We proceed by induction on $d = [K:F]$.

If $d=1$ we are done. Assume $d>1$. Consider any $\alpha \in K \setminus F$. Then we have $[K:F] = [K:F(\alpha)][F(\alpha):F] = d_2 d_1 = d$. We have $d_2 < d$, so by induction $\exists \beta \in K$ such that $F(\alpha)(\beta) = F(\alpha,\beta) = K$. Let $\sigma_i : K \to \bar{F}$, $i \in \{1,\dots,d\}$ be the d embeddings of K into $\bar{F}$ fixing F. Each σ_i is determined by what $\sigma_i(\alpha)$ and $\sigma_i(\beta)$ are.

If $i \neq j$, then $\sigma_i \neq \sigma_j$, so $\exists c_{ij} \in F$ such that $\sigma_i(\alpha) + c_{ij}\sigma_i(\beta) \neq \sigma_j(\alpha) + c_{ij}\sigma_j(\beta)$.

Let $P(x) := \prod_{i \neq j} (\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta)) \in \bar{F}[x]$.

Note, $P(x) \neq 0$, so $\exists c \in F$ such that $P(c) \neq 0$. Then $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$, for all $i \neq j$.

i.e., the $\sigma_i(\alpha + c\beta)$ are all distinct. Let $\gamma = \alpha + c\beta$. Notice, if $i \neq j$, then $\sigma_i|_{F(\gamma)} \neq \sigma_j|_{F(\gamma)}$, since $\sigma_i(\gamma) \neq \sigma_j(\gamma)$.

Thus, there are d distinct embeddings of $F(\gamma)$ into $\bar{F}$ fixing F.

Thus, $d \leq [F(\gamma):F]_s \leq d$, so $F \to F(\gamma)$ is separable.

In particular, we have that $K = F(\gamma)$, as K and $F(\gamma)$ are both d-dimensional vector spaces over F, and $F(\gamma) \subseteq K$. $\square$

Finite Fields

Def'n: We define the finite field with p elements (p prime) to be $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Recall, if F is a finite field, $\mathrm{Char}(F) = p$, for p prime.

Remark: Let F be a finite field. Then $\#F = p^n$ for some p prime, $n \in \mathbb{N}$.

Pf: Let $\mathbb{F}_p$ be the prime subfield of F. Then F is an $\mathbb{F}_p$-vector space. If $[F:\mathbb{F}_p] = n$, then $F \cong (\mathbb{F}_p)^n$. Thus, $\#F = \#(\mathbb{F}_p)^n = p^n$. (alternatively, let $\{\alpha_1,\dots,\alpha_n\}$ be an $\mathbb{F}_p$-basis of F. Then $\alpha \in F$ can be written as $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n$, $a_i \in \mathbb{F}_p$. There are p choices for a_i, so p^n total $\alpha \in F$). $\square$

Proposition: Let $F = \mathbb{F}_{p^n} \subseteq \bar{\mathbb{F}}_p$. Then F is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

Pf: Let $G = (F \setminus \{0\}, \cdot)$. Then G is a group of order $p^n - 1$. Consider $\alpha \in G$. Then $\langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{k-1}\} \subseteq G$. By Lagrange, $o(\alpha) = k \mid p^n - 1$, so $\alpha^{p^n-1} = 1$. Thus, $\forall \alpha \in G$, $\alpha^{p^n-1} = 1$, so α is a root of $x^{p^n-1} - 1$. Hence, any $\alpha \in F$ is a root of $x^{p^n} - x$, so $F = SF(x^{p^n} - x)$. $\square$

Remark: This gives that, up to isomorphism, there is at most one field of order p^n.

Remark: F is normal and separable over $\mathbb{F}_p$.

Pf: F is a splitting field, so is normal over $\mathbb{F}_p$. Let $f = x^{p^n} - x$. Then $f' = p^n x^{p^n-1} - 1 = -1$.

Hence, f and f' never share a root, so f is separable. Thus, $\forall \alpha \in F$, α is separable, so F is separable over $\mathbb{F}_p$. $\square$

Remark: If $F \to K$ is an extension of finite fields, then K is normal and separable over F.

Pf: We have $\mathbb{F}_p \to F \to K$, but $\mathbb{F}_p \to K$ is normal, so $F \to K$ is normal by previous result.

The separability proof is similar to the proof above. $\square$

Theorem: For any $n \in \mathbb{N}$, there is a finite field of order p^n.

Pf: Let $f = x^{p^n-1} - 1 \in \mathbb{F}_p[x]$. Take $F = SF(f(x))$. We show $\#F = p^n$.

Notice $f' = (p^n-1)x^{p^n-2} = -x^{p^n-2}$, so $f'(x) = 0$ if and only if $x = 0$. But $f(0) \neq 0$.

Pf: Let $f = x^{p^n-1} - 1 \in \mathbb{F}_p[x]$. Take $F = SF(f(x))$. We show $\#F = p^n$.

Notice, $f' = (p^n-1)x^{p^n-2} = -x^{p^n-2}$, so $f'(x) = 0$ if and only if $x = 0$. But $f(0) \neq 0$,

so f and f' do not share a root. In particular, we have that f has $p^n - 1$ distinct roots,

all of which are in F. Let F' be the set of all roots of $x^{p^n} - x$. We show F' is a field.

Consider any $\alpha, \beta \in F'$, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$, so $\alpha+\beta$ is a root of $x^{p^n} - x$. Thus, $\alpha + \beta \in F'$.

Also, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, so $\alpha\beta \in F'$. The other axioms similarly hold. Thus, F' is a field, but

$F = SF(x^{p^n} - x)$, so $F = F'$, and $\#F = \#F' = p^n$. $\square$

Remark: We define the map $\varphi: \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$, $\alpha \mapsto \alpha^p$. This is an endomorphism. We call it the Frobenius Endomorphism.

Remark: φ restricts to endomorphisms. That is, $\varphi|_{\mathbb{F}_q}: \mathbb{F}_q \to \mathbb{F}_q$ is an endomorphism.

Theorem: Let $G = \mathbb{F}_q^* = \mathbb{F}_{p^n}^*$. Then there is $\alpha \in G$ such that $G = \langle \alpha \rangle$. i.e., G is cyclic.

Pf: Consider $\alpha \in G$ of order k. Let $H = \langle \alpha \rangle = \{1, \alpha, \dots, \alpha^{k-1}\}$. Notice, each $\beta \in H$ is a root of $x^k - 1$.

i.e., all k'th roots in $\overline{\mathbb{F}_q}$ are in H. Let φ be the Euler Phi Function. Then the number of elements

of G of order k is either 0, or $\varphi(k)$. We have that $q - 1 = \#G \leq \sum_{k \mid q-1} \varphi(k)$ (note, $\alpha^{q-1} = 1, \forall \alpha \in G$).

We show this inequality is in fact an equality.

Let $G' = \mathbb{Z}/(q-1)\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{q-2}\} = \langle \overline{1} \rangle$. In G', the number of elements of order $k \mid q-1$

is exactly $\varphi(k)$. Thus, $q - 1 = \#G = \#G' = \sum_{k \mid q-1} \varphi(k)$. But then there is at least one element in G of

order $q-1$, say $\beta \in \mathbb{F}_q$. Hence, $\langle \beta \rangle = \{1, \beta, \dots, \beta^{q-2}\} = \mathbb{F}_q^*$. $\square$

Proposition: $Gal(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, where $q = p^n$.

Pf: Let α be a generator of $\mathbb{F}_q^*$. Then $\alpha^k = 1$ if and only if $p < q - 1 \mid k$.

Assume $n > 1$. Let φ denote the Frobenius endomorphism. We claim $\alpha, \varphi(\alpha) = \alpha^p, \dots, \varphi^{n-1}(\alpha) = \alpha^{p^{n-1}}$ are all distinct.

We have $\alpha^{p^k} = \alpha$ if and only if $\alpha^{p^k - 1} = 1$, which is true when $p^n - 1 = q - 1 \mid p^k - 1$. But we assume $k < n$,

so these elements are all distinct. Thus, $n = \#\langle \varphi \rangle$, and $\#Gal(\mathbb{F}_q/\mathbb{F}_p) = n$, so $Gal(\mathbb{F}_q/\mathbb{F}_p) = \langle \varphi \rangle \cong \mathbb{Z}/n\mathbb{Z}$. $\square$

Remark: $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, where $\langle \alpha \rangle = \mathbb{F}_q^*$.

Proposition: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$.

Pf: If $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is an $\mathbb{F}_{p^m}$-vector space, so $\exists k \in \mathbb{N}$ so that $\mathbb{F}_{p^n} = (\mathbb{F}_{p^m})^k$. Thus, $p^n = p^{mk}$, so $m \mid n$.

Suppose instead $m \mid n$. Every element of $\mathbb{F}_{p^m}$ satisfies $\varphi^m(\alpha) = \alpha$, $\alpha \in \mathbb{F}_{p^m}$. Note, $\beta \in \mathbb{F}_{p^n}$ if and only if $\varphi^n(\beta) = \beta$.

Suppose $n = km$, for some $k \in \mathbb{N}$. Then if $\alpha \in \mathbb{F}_{p^m}$, $\alpha^{p^n} = \alpha^{p^{mk}} = \alpha^{p^{\overbrace{m + \dots + m}^{k \text{ times}}}} = (\alpha^{p^m})^{\cdot^{\cdot^{\cdot^{p^m}}}} = \alpha$, so $\alpha \in \mathbb{F}_{p^n}$.

Thus, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. $\square$

Proposition: $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$, where $m \mid n$.

Galois Correspondence

Def'n: An algebraic extension $F \to K$ is Galois if it is normal and separable.

Remark: If $F \to K$ is finite Galois, then $|Gal(K/F)| = [K:F]$

Pf: $[K:F] \overset{\text{separable}}{=} [K:F]_s = \# \{\sigma: K \to \overline{F} \mid \sigma|_F = id\} \overset{\text{normality}}{=} \# \{\sigma: K \to K \mid \sigma|_F = id\} = \# Gal(K/F)$.

Theorem: Let $F \subseteq K$ be finite Galois, $G = Gal(K/F)$. Then there is an inclusion reversing bijection between subgroups of G and subfields of K containing F, where $H \leq G \longmapsto K^H$ and if $F \subseteq L \subseteq K$, then $L \longmapsto Gal(K/L) \leq G$.

Pf: Let $F \subseteq K' \subseteq K$. We show $K' = K^{Gal(K/K')}$. Recall, $K^{Gal(K/K')} = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma: K \to K \text{ s.t. } \sigma|_{K'} = id\}$. Clearly, $K' \subseteq K^{Gal(K/K')}$.

Take $\alpha \in K \setminus K'$. Then $m_{\alpha,K'}$ has degree ≥ 2 and distinct roots as $F \to K$ is separable. Let $\alpha' \neq \alpha$ be another root of $m_{\alpha,K'}$.

We have

$$\begin{tikzcd} K' \arrow[r] \arrow[dr] & K'(\alpha) \arrow[r] \arrow[d, "?"] & K \arrow[d, dashed] \\ & K'(\alpha') \arrow[r] & K \end{tikzcd}$$

exists by extension lemma + normality. i.e., $\exists \sigma: K \to K$ s.t. $\sigma(\alpha) = \alpha'$.

Hence, $\alpha' \notin K^{Gal(K/K')}$, so $K' = K^{Gal(K/K')}$.

Conversely, let $H \leq G = Gal(K/F)$. We show $Gal(K/K^H) = H$.

Notice, $Gal(K/K^H) = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall \alpha \text{ s.t. } \tau(\alpha) = \alpha \ \forall \tau \in H\}$. Thus, $H \leq Gal(K/K^H)$.

By Thm. of the primitive element, there is $\alpha \in K$ so that $K = F(\alpha)$. Set $X = H.\alpha = \{\alpha_1, \dots, \alpha_k\}$, where each $\alpha_i \in K$.

Now, $m_{\alpha,K^H} \mid p(x) := \prod_{i=1}^{k} (x - \alpha_i) \in K[x]$. But $\forall \tau \in H$, $\tau.p(x) = p(x)$ as τ permutes the $\alpha_1, \dots, \alpha_k$. That is, $p(x) \in K^H[x]$.

But then $\# Gal(K/K^H) = [K:K^H] = \deg(m_{\alpha,K^H}) \leq \# H$. Hence, $Gal(K/K^H) = H$.

We have established the bijection. For inclusion reversing, if $H \leq H' \leq G$, we want $K^{H'} \subseteq K^H$.

If $\alpha \in K^{H'}$, then $\forall \sigma \in H'$, $\sigma(\alpha) = \alpha$. But then $\forall \tau \in H$ $\tau(\alpha) = \alpha$ so $\alpha \in K^H$.

If instead $F \subseteq F_1 \subseteq F_2 \subseteq K$, we want $Gal(K/F_2) \leq Gal(K/F_1)$. Let $\sigma \in Gal(K/F_2)$. Then $\sigma|_{F_2} = id$.

But $F_1 \subseteq F_2$, so $\sigma|_{F_1} = id$. In particular, $\sigma \in Gal(K/F_1)$. $\square$

Quadratic Extensions - Galois Correspondence

Let F be a field with char $F \neq 2$. Let $f = x^2 + bx + c \in F[x]$ be irreducible. Then f has 2 distinct roots (quadratic formula).

The splitting field of f, K, has $[K:F] = 2$, and $F \to K$ is separable (as f is separable). In particular, $F \to K$ is finite Galois.

$Gal(K/F) = \{e, \sigma\}$, where σ permutes the 2 roots of f. Also, there are no intermediate fields.

Finite Fields - Galois Correspondence

Let p be prime, $n \in \mathbb{N}$, $q = p^n$. Then $\mathbb{F}_p \to \mathbb{F}_q$ is finite Galois with $Gal(\mathbb{F}_q/\mathbb{F}_p) \cong \langle \varphi \rangle \cong \mathbb{Z}/(q-1)\mathbb{Z}$ (φ the Frobenius endomorphism).

$G = Gal(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic, with one subgroup for each divisor d of $q-1$, $\langle \varphi^d \rangle$ has order $q-1/d$.

$\mathbb{F}_q^{\langle \varphi^d \rangle} = \{\alpha \in \mathbb{F}_q \mid \alpha^{p^d} = \alpha\} = \mathbb{F}_{p^d}$.

Cubic Extensions

Assume char $F \neq 2, 3$. Take $f \in F[x]$ irreducible with roots $\alpha_1, \alpha_2, \alpha_3$. Let $K = F(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of f.

Since char $F \neq 3$, f is separable (e.g. formal derivative) so $F \to K$ is finite Galois, and $G = Gal(K/F) \leq S_3$ as $\sigma \in G$ acts on the α_i.

We have $[F(\alpha_1):F] = 3 \leq [K:F]$, so $|G| = 6$ or $|G| = 3$, and hence $G \cong S_3$ or $G \cong A_3$.

Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \sqrt{\Delta(f)}$ and let $\sigma = (123)$ (so $A_3 = \langle \sigma \rangle$). δ is fixed by δ but not $(12), (13)$, or (23),

so $\delta \in K^G = F$ if and only if $G = A_3$. i.e., $G = \begin{cases} S_3, & \sqrt{\Delta(f)} \notin F \\ A_3, & \sqrt{\Delta(f)} \in F \end{cases}$ (one real root implies Δ not square - midterm).

Second Part of Galois Correspondence

Theorem: Let $F \subseteq K$ be finite Galois and $H \leq Gal(K/F) = G$. Then $H \trianglelefteq G$ iff $F \subseteq K^H$ is normal, and $Gal(K^H/F) \cong G/H$.

Second Part of Galois Correspondence

Theorem: Let $F \subseteq K$ be finite Galois and $H \leq Gal(K/F) = G$. Then $H \trianglelefteq G$ iff $F \subseteq K^H$ is normal, and $Gal(K^H/F) \cong G/H$.

Pf: Assume $F \to K^H$ normal. Then any $\sigma : K^H \to \bar{F}$ fixing F induces some $\sigma \in Gal(K^H/F)$, so there is a homomorphism $\varphi : Gal(K/F) \to Gal(K^H/F)$.

By the extension lemma, this is surjective, and $\ker(\varphi) = \{\sigma : K \to K \mid \sigma|_{K^H} = id\} = Gal(K/K^H) = H$. Hence, $H \trianglelefteq G$ and $Gal(K^H/F) \cong G/H$.

Conversely, let $H \trianglelefteq G$. Let $\sigma : K^H \to \bar{F}$ fix F. Any such σ lifts to $\tilde{\sigma} : K \to K$ fixing F via extension lemma and normality of $F \to K$.

Now let $\alpha \in K^H$, $\tau \in H$. Then $\tau(\tilde{\sigma}(\alpha)) = (\tau\tilde{\sigma})(\alpha) = (\tilde{\sigma}\tau)(\alpha) = \tilde{\sigma}(\alpha)$, by normality of H and since $\alpha \in K^H$, so $\tilde{\sigma}(\alpha) \in K^H$, and $\sigma(K^H) \subseteq K^H$. $\square$

Note: Let $F \subseteq K, L \subseteq \bar{F}$ be fields and L finite over F. Then if $F \to L$ is Galois, $K \cap L \to L$ and $K \to KL$ are Galois.

Pf: $K \cap L \to L$ finite Galois is immediate. $K \to KL$ is finite Galois since it is generated by normal and separable elements (from L).

Theorem (Base change Theorem): Let K, L be as above. Then $Gal(KL/K) \cong Gal(L/K \cap L)$.

Pf: Take $\varphi : Gal(KL/K) \to Gal(L/K \cap L)$ where $\varphi(\sigma) = \sigma|_L$. This is a well-defined homomorphism.

We show injective and surjective. Since $\sigma \in Gal(KL/K)$ is determined by its behaviour on K (constant) and L, φ is injective.

Let $H = \operatorname{im}\varphi$. Then $L^H = K \cap L$, so $H = Gal(L/K \cap L)$ and φ is surjective. $\square$

First Sylow Theorem + Pre-requisites.

Proposition: Let G be abelian and $p \mid |G|$. Then G has a subgroup of order p.

Pf: By induction on $|G|$. The base case is trivial. Assume $|G| > 1$ and the result is true for smaller groups.

Assume $\forall x \in G \setminus \{e\}, p \nmid |\langle x \rangle|$ (else we are done). Then G is abelian so $G/\langle x \rangle$ is a group, and is abelian.

Since $p \nmid |\langle x \rangle|$ and $p \mid |G|$, we have $p \mid |G/\langle x \rangle|$. Hence, $\exists \bar{y} \in G/\langle x \rangle$ of order p. Now, if y is in the pre-image in natural homomorphism then $y \notin \langle x \rangle$ but $y^p \in \langle x \rangle$ as $o(\bar{y}) = p$. But $y^m \in \langle x \rangle$ if and only if $p \mid m$, so $p \mid o(y)$ and we are done by induction. $\square$

Theorem (First Sylow Theorem): Let G be a finite group with $|G| = mp^k$ for some p prime, $m \in \mathbb{N}$, $k \in \mathbb{Z}_{\geq 0}$, $\gcd(p, m) = 1$.

Then there is a subgroup $H \leq G$ such that $|H| = p^k$.

Pf: By induction on $|G|$. Base case is trivial. Assume $p \mid [G:H]$ $\forall H \lneq G$.

By the class equation, $|G| = |Z(G)| + \sum' [G:H] \equiv |Z(G)| \equiv 0 \pmod{p}$, so $Z(G) \neq \{e\}$.

By proposition, $Z(G)$ has a subgroup H of order p. Since $H \leq Z(G)$, $H \trianglelefteq G$, $|G/H| = mp^{k-1}$.

By induction, $\exists K \leq G/H$ of order p^{k-1}. Pre-image is subgroup of order $|H| \cdot |K| = p \cdot p^{k-1} = p^k$. $\square$

Corollary: Let G be a finite group and p a prime dividing $|G|$. Then there exists $H \leq G$ with $|H| = p$.

Pf: By Sylow's (First) Theorem, G has a subgroup of order p^k for maximal $k \in \mathbb{N}$ such that $p^k \mid |G|$. By Homework, $|Z(H)|$ is non-trivial, so by the proposition has a subgroup of order p. $\square$

Theorem: Let p be prime, $f \in \mathbb{Q}[x]$ be irreducible of degree p with splitting field K. If f has exactly 2 real roots then $Gal(K/\mathbb{Q}) \cong S_p$.

Pf: By Homework 7 Question 6(d), S_p is generated by any transposition and the cycle $(1 2 \ldots p)$. Recall, $G = Gal(K/\mathbb{Q}) \leq S_p$. Also, $p \mid |G|$ as $\deg(f) = p$, and f is irreducible. Let $G \cong H \leq S_p$. Then H has a p-cycle as $p \mid H$ and so H has a subgroup of order p. Let $\tau : K \to K$ be given by $\tau(\alpha) = \bar{\alpha}$, the complex conjugate of α. Then since f has exactly 2 non-real roots, and any $\beta \in \mathbb{R}$ is fixed under τ, H has a transposition so we are done. $\square$

Fundamental Theorem of Algebra

$\square$

Theorem: Every finite extension of $\mathbb{C} = \mathbb{R}(i)$ is $\mathbb{C}$.

Pf: Let K be a finite extension of $\mathbb{C}$. Then the normal closure $\tilde{K}$ of K is finite Galois over $\mathbb{C}$.

Then $G = Gal(\tilde{K}/\mathbb{R})$ has order divisible by 2. Let $H \leq G$ be a Sylow 2-subgroup of G.

Then $[G:H] = |G|/|H|$ is odd, and so $[\tilde{K}^H : \mathbb{R}]$ is odd. By IVT, ... odd degree polynomial over $\mathbb{R}$ has a root in $\mathbb{R}$

Then $G = \mathrm{Gal}(\tilde{K}/\mathbb{R})$ has order divisible by 2. Let $H \leq G$ be a Sylow 2-subgroup of G.

Then $[G:H] = |G|/|H|$ is odd, and so $[\tilde{K}^H : \mathbb{R}]$ is odd. By IVT, any odd degree polynomial over $\mathbb{R}$ has a root in $\mathbb{R}$.

Hence, $\tilde{K}^H = \mathbb{R}$, so G is a 2-group. Let $G' := \mathrm{Gal}(\tilde{K}/\mathbb{C})$. Then G' is a 2-group.

If $|G'| \neq 1$, then (by HW) there is an index 2 subgroup $H' \leq G'$. Then $[\tilde{K}^{H'} : \mathbb{C}] = 2$.

But $\mathbb{C}$ has no quadratic extension by the quadratic formula, a contradiction. Thus, $G' = \{e\}$, so $\tilde{K} = \mathbb{C}$.

Solvable Groups

Def'n: A group G is simple if $H \trianglelefteq G$ implies $H = \{e\}$ or $H = G$.

Def'n: A composition series of a finite group G is a sequence of subgroups $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_m = G$ so that each G_{i+1}/G_i is simple.

Theorem: Every finite group G has a composition series.

Pf: By induction on $|G|$. The base case is trivial. Suppose any group of size $< |G|$ has a composition series.

If G is simple we are done. Assume not. Then $\exists H \trianglelefteq G$ such that $H \neq \{e\}$ and $H \neq G$ and H is of maximal size among normal subgroups of G. Since $|H| < |G|$, H has a composition series. We need only show G/H is simple.

Let $K \trianglelefteq G/H$ and take $\pi : G \to G/H$ to be the natural homomorphism. Since $K \trianglelefteq G/H$, $\pi^{-1}(K) \trianglelefteq G$.

However, $H \subseteq \pi^{-1}(K)$ so since $H \trianglelefteq G$, $H \trianglelefteq \pi^{-1}(K)$. But H is maximal, so $\pi^{-1}(K) = H$ or $\pi^{-1}(K) = G$.

In either case, $K = H = e_{G/H}$ or $K = G/H$, so G/H is simple. $\square$

Def'n: A finite group is solvable if it has a composition series with abelian factors.

Proposition: Let G be a finite simple group. If G is abelian, then $G \cong \mathbb{Z}_p$ for some prime p.

Pf: G is abelian so any subgroup of G is normal. Let p be a prime dividing $|G|$. Then G has a subgroup H of order p.

But then G must have order p. $\square$

Proposition: Let G be a finite solvable group. If G is simple, then G is abelian.

Pf: Since G is simple, the only composition series is $\{e\} \trianglelefteq G$, and by solvability $G \cong G/\{e\}$ is abelian. $\square$

Theorem: Let G be a finite group and $H \trianglelefteq G$. Then G is solvable if and only if H and G/H are solvable.

Pf: Homework 8, Question 3.

Corollary: G is solvable if and only if any composition series of G has abelian factors.

Pf: The only if direction follows immediately by definition and an above theorem.

Suppose G is solvable. We go by induction on $|G|$. The base case is trivial.

Let $G_0 \trianglelefteq \dots \trianglelefteq G_{m-1} \trianglelefteq G_m = G$ be a composition series of G. By theorem, G_{m-1} and G/G_{m-1} are solvable.

Furthermore, G/G_{m-1} is simple, so solvability implies G/G_{m-1} is abelian (by proposition).

Also, by induction any composition series of G_{m-1} has abelian factors. $\square$

Def'n: Let $G \leq S_n$ act on $K[x_1, \dots, x_n]$ by permuting the x_i, where K is a field. Let $f = \prod_{i<j}(x_i - x_j)$. Define $A_n := \mathrm{Stab}(f) = \{\sigma \in S_n \mid \sigma(f) = f\}$.

Remarks:
- $A_n \leq S_n$ as stabilizers are subgroups.
- $\mathrm{Orb}(f) = \{f, -f\}$, so by Orbit-Stabilizer Theorem, $[S_n : A_n] = 2$, so by Homework 4 Question 8, $A_n \trianglelefteq S_n$.
- Homework 8/11 give additional properties / characterizations of A_n.

Lemma: A_n is generated by 3-cycles.

Pf: For all $\sigma \in A_n$, σ is the product of an even number of transpositions. Hence, it suffices to show the product of 2 transpositions is a product of 3-cycles. Notice, $(ij)(jk) = (jki)$ and $(ij)(kl) = (ij)(ik)(ik)(kl) = (ikj)(kli)$.

Pf. for all $\sigma \in A_n$, σ is the product of an even number of transpositions. Hence, it suffices to show the product of 2 transpositions is a product of 3-cycles. Notice, $(ij)(jk) = (jki)$ and $(ij)(k\ell) = (ij)(ik)(ik)(k\ell) = (ikj)(k\ell i)$.

Thus, any 3-cycle is in A_n and any $\sigma \in A_n$ can be written as the product of 3-cycles. □

Remark: Let $(a_1 \dots a_k) \in S_n$ be a k-cycle and $\sigma \in S_n$. Then $\sigma (a_1 \dots a_k) \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$.

Lemma: All 3-cycles in A_n are conjugate in A_n for $n \geq 5$.

Pf: Let $(ijk) \in A_n$ be a 3-cycle. Take $\sigma \in S_n$ to send i to 1, j to 2, and k to 3.

Then $\sigma (ijk) \sigma^{-1} = (123)$. So all 3-cycles are conjugate to (123) and hence conjugate in S_n.

We need $\sigma \in A_n$. If $\sigma \in A_n$ we are done. Assume not. Then since $n \geq 5$, choose $r, s \notin \{i, j, k\}$.

Then set $\sigma' = \sigma (rs)$. Then $\sigma' (123) \sigma' = (123)$ and $\sigma' \in A_n$. □

Theorem: A_n is simple if $n \geq 5$.

Pf: Let $n \geq 5$ and take $\{e\} \subsetneq H \trianglelefteq A_n$. We show H has a 3-cycle. If this is the case, then by the lemmas and normality, $H = A_n$. Pick $\sigma \in H$ fixing a maximal number of elements of $\{1, 2, \dots, n\}$, $\sigma \neq \{e\}$.

First case: Suppose σ is the disjoint product of 2-cycles. Write $\sigma = (ij)(k\ell)\dots$ and choose $r \notin \{i, j, k, \ell\}$.

Set $\tau = (k\ell r)$. Then let $\rho = \tau \sigma \tau^{-1} \sigma^{-1}$. Then $\rho \in H$ by normality and $\rho \neq e$. Suppose $x \in \{1, 2, \dots, n\}$ satisfies $\sigma(x) = x$.

Then if $x \neq r$, $\rho(x) = x$. But then $\rho(i) = i$, $\rho(j) = j$, so ρ fixes more elements than σ, a contradiction.

Second case: Suppose σ is the disjoint product of cycles $\sigma = (ijk\dots)\dots$. If $\sigma = (ijk)$ we are done. Assume not.

Then $\exists r, s \in \{1, \dots, n\} \setminus \{i, j, k\}$ so that $\sigma(r) \neq r$, $\sigma(s) \neq s$. Let $\tau = (krs) \in A_n$ and take $\rho = \tau \sigma \tau^{-1} \sigma^{-1} \in H$ (by normality).

Choose x such that $\sigma(x) = x$. Then $\rho(x) = x$, $\rho(j) = j$, and $\rho \neq e$ as $\rho(k) = r$, a contradiction.

Thus, σ is a 3-cycle. □

Corollary: For $n \geq 5$, A_n (and hence S_n) is not solvable.

Pf: If A_n were solvable, then A_n would be abelian, which is false. □

Solvable Extensions

Def'n: A field extension $F \to K$ is a principal radical extension if there is $\alpha \in K$, $m \in \mathbb{N}$ so that $K = F(\alpha)$ and $\alpha^m \in F$.

Def'n: A field extension $F \to K$ is called radical if it is the composition of finitely many principal radical extensions.

i.e. there is a tower $F = F_0 \to F_1 \to \dots \to F_k = F$ so that each $F_i \to F_{i+1}$ is a principal radical extension.

Def'n: A field extension $F \to K$ is solvable if there is a field K' such that $K \subseteq K'$ and $F \to K'$ is radical.

Theorem: Let $F \to L$ be finite Galois and assume $\operatorname{char} F = 0$. Then $F \to L$ is solvable if and only if $\mathrm{Gal}(L/F)$ is solvable.

Pf: Assume $F \to L$ is solvable. Then there is a field M containing L such that $F \to M$ is radical.

Let M' be the normal closure of M. We claim $F \to M'$ is still radical.

Since $F \to M$ is radical, we have a tower $F \to F_1 = F(\alpha_1) \to F_2 = F_1(\alpha_2) \to \dots \to M$ such that $\forall \alpha_i\ \exists m_i \in \mathbb{N}$ such that $\alpha_i^{m_i} \in F_{i-1}$. Now consider the tower $F \to SF(m_{\alpha_1,F}) = \widetilde{F}_1 \to SF(m_{\alpha_2,\widetilde{F}_1}) = \widetilde{F}_2 \to \dots \to M'$.

Then each $\widetilde{F}_{i-1} \to \widetilde{F}_i$ is radical as $\alpha_i \in F_i$ is a root of $x^{m_i} - \alpha_i^{m_i} \in F_{i-1}[x]$.

Thus, $F \to M'$ is radical. Now $F \to M'$ is Galois as $F \to L$ is normal and $L \to M'$ is normal and F has characteristic 0.

Furthermore, $\mathrm{Gal}(M'/L) \trianglelefteq \mathrm{Gal}(M'/F)$ and $\mathrm{Gal}(M'/F)/\mathrm{Gal}(M'/L) \cong \mathrm{Gal}(L/F)$ by the Second part of Galois Correspondence.

Now, by solvability theorem, if $\mathrm{Gal}(M'/F)$ is solvable, so is $\mathrm{Gal}(L/F)$. Hence, we need only show that a Galois and radical extension $F \to L$ has solvable Galois group.

Observe: Let α be a primitive m'th root of unity. Then $F \to F(\alpha)$ is Galois with abelian Galois group.

and radical extension $F \to L$ has solvable Galois group.

Observe: Let α be a primitive m'th root of unity. Then $F \to F(\alpha)$ is Galois with abelian Galois group.

To see this, let $f(x) = x^m - 1$. Then $\{1, \alpha, \dots, \alpha^{m-1}\}$ are all roots of f, so $F(\alpha)$ is a splitting field and so $F \to F(\alpha)$ is Galois (separability from char $F = 0$).

Notice, if instead char $F \nmid m$ the result holds as $\gcd(f, f') = 1$ so f is separable.

Let $G = Gal(F(\alpha)/F)$ and take $\sigma, \tau \in G$. Then σ and τ are determined by $\sigma(\alpha) = \alpha^i$, $\tau(\alpha) = \alpha^j$ (as α is a primitive m'th root of unity).

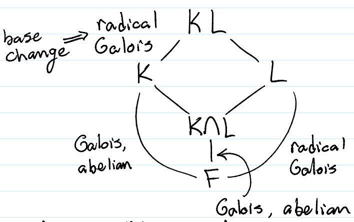
Thus, $\sigma\tau(\alpha) = \tau\sigma(\alpha)$ so $\sigma\tau = \tau\sigma$ and G is abelian.

Now let $F \to K$ be the extension of F by adjoining all m'th roots of unity. Then $F \to K$ is Galois with $Gal(K/F)$ abelian.

Furthermore, by the base change theorem $K \to KL$ is Galois, and note it is also radical. Also, $Gal(KL/K) \cong Gal(L/K \cap L)$.

So if $Gal(KL/K)$ is solvable, so is $Gal(L/K \cap L)$. But $Gal(L/K\cap L) \trianglelefteq Gal(L/F)$ and $Gal(L/F)/_{Gal(L/K\cap L)} \cong Gal(K \cap L/F)$.

But $Gal(K\cap L/F)$ is abelian since $Gal(K/F)$ is abelian. Hence, $Gal(L/K)$ would be solvable by solvability theorem.



Thus, if $Gal(KL/K)$ is solvable, then $Gal(L/F)$ is solvable.

Without loss of generality, we may assume $F \to L$ is radical Galois, and F has all m'th roots of unity needed.

Now we have $F = F_0 \to F_1 \to \dots \to F_k = L$ where $F_i = F_{i-1}(\alpha_i)$ for some α_i satisfying $\alpha_i^{m_i} \in F_{i-1}$ for some $m_i \in \mathbb{N}$. We may assume m_i is prime. We claim $F_{i-1} \to F_i$ is Galois with cyclic Galois group.

To see this, we have that α_i is a root of $x^{m_i} - \beta_i$ where $\beta_i = \alpha_i^{m_i}$. Let ζ be an m_i'th root of unity. Then $\zeta\alpha_i \in F_i$ is also a root of $x^{m_i} - \beta_i$. Hence, $x^{m_i} - \beta_i$ splits in $F_i[x]$, so $F_{i-1} \to F_i$ is Galois.

Furthermore, Homework 9 Question 1 gives $Gal(F_i/F_{i-1})$ is cyclic.

Set $G_i = Gal(L/F_i)$. Then each $G_{i-1} \trianglelefteq G_i$ by normality of extensions and G_{i+1}/G_i is abelian $\forall i$ by construction.

Thus, $G_0 = Gal(L/F)$ is solvable.

Conversely, suppose $Gal(L/F)$ is solvable. We show $F \to L$ is solvable.

We first prove a lemma:

Lemma: Let $F \to K$ be Galois, $Gal(K/F) \cong \mathbb{Z}_p$ for some prime p, and assume F has all p'th roots of unity.
Then $F \to K$ is a principal radical extension.

Pf of lemma: Let $\beta \in K \setminus F$ be such that $K = F(\beta)$ (by Theorem of the Primitive Element).

Let ζ be a primitive p'th root of unity and σ a generator of $Gal(K/F)$. We use Lagrange Resolvents.

For all $i \in \{0, \dots, p-1\}$ define $\alpha_i = \sum_{j=0}^{p-1} \zeta^{-ij}\sigma^j(\beta)$.

We have $\alpha_0 = \beta + \sigma(\beta) + \dots + \sigma^{p-1}(\beta)$, and $\sigma(\alpha_0) = \sigma(\beta) + \sigma^2(\beta) + \dots + \beta = \alpha_0$, so $\alpha_0 \in K^{\langle\sigma\rangle} = F$.

More generally, $\alpha_i = \beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \dots + \zeta^{-(p-1)i}\sigma^{p-1}(\beta)$ and $\zeta^{-i}\sigma(\alpha_i) = \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \dots + \beta = \alpha_i$.

Hence, $\sigma(\alpha_i) = \zeta^i\alpha_i$ and so $\sigma(\alpha_i^p) = \sigma(\alpha_i)^p = (\zeta^i\alpha_i)^p = \alpha_i^p$, so $\alpha_i^p \in K^{\langle\sigma\rangle} = F$, $\forall i \in \{0, \dots, p-1\}$.

We need to show there is i such that $\alpha_i \notin F$. But $\zeta^i \neq 1$ $\forall 1 \le i \le p-1$ so $\sigma(\alpha_i) \neq \alpha_i$ and hence $\alpha_i \notin F$ unless $\alpha_i = 0$.

Assume, for a contradiction, that $\alpha_1 = \alpha_2 = \dots = \alpha_{p-1} = 0$. Then

$$\begin{aligned}
\alpha_0 = \alpha_0 + \alpha_1 + \dots + \alpha_{p-1} &= \beta + \sigma(\beta) + \sigma^2(\beta) + \dots + \sigma^{p-1}(\beta) \\
&+ \beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma(\beta) + \dots + \zeta^{-(p-1)}\sigma^{p-1}(\beta) \\
&+ \beta + \zeta^{-2}\sigma(\beta) + \zeta^{-2\cdot 2}\sigma(\beta) + \dots + \zeta^{-(p-1)\cdot 2}\sigma^{p-1}(\beta) + \dots \\
&= p\beta + (1 + \zeta^{-1} + \dots + \zeta^{-(p-1)})\sigma(\beta) + \dots + (1 + \zeta^{-j} + \dots + \zeta^{-j(p-1)})\sigma^j(\beta) + \dots \\
&= p\beta + 0\sigma(\beta) + \dots + 0\sigma^{p-1}(\beta) = p\beta.
\end{aligned}$$

$$= p\beta + (1+\zeta^{-1}+\dots+\zeta^{-(p-1)})\sigma(\beta)+\dots+(1+\zeta^{-j}+\dots+\zeta^{-j(p-1)})\sigma^j(\beta)+\dots$$
$$= p\beta + 0\sigma(\beta)+\dots+0\sigma^{p-1}(\beta) = p\beta.$$

But $\beta \notin F$ so this is impossible. Hence, there is $1 \le i \le p-1$ such that $\alpha_i \in K\setminus F$.

But $[K:F]=p$ so $F(\beta)=F(\alpha_i)$, and $\alpha_i^p \in F$, so $F \to F(\beta)$ is a principal radical extension.

Note the $\sum_{i=0}^{p-1} \zeta^{ij} = 0$ as it is the coefficient of a term in $x^p - 1$. //

Now $G = Gal(L/F)$ is solvable so let $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_m = G$ be a composition series of G. Then G_{i+1}/G_i is simple and abelian for all i. Hence, $G_{i+1}/G_i \cong \mathbb{Z}_p$ for some prime p.

Define $L_i = L^{G_i}$ for each $i \in \{0,\dots,m\}$. Now we have $F = L_m \to L_{m-1} \to \dots \to L_0 = L$ where each $L_i \to L_{i-1}$ is Galois and has Galois group isomorphic to $\mathbb{Z}_{p_i}$ for some prime p_i. We can almost apply the lemma. Let $F \to K$ be given by adjoining all p_i'th roots of unity. We have

$$\begin{tikzcd}[column sep=small]
& KL_{i-1} \arrow[dl, dash] \arrow[dr, dash] & \\
KL_i \arrow[dr, dash] \arrow[ddr, dash] & & L_{i-1} \arrow[dl, dash] \arrow[ddl, dash] \\
& KL_i \cap L_{i-1} \arrow[d, dash] & \\
& L_i &
\end{tikzcd}$$

and $KL_i \to KL_{i-1}$ is Galois by the base change theorem. Also, $Gal(KL_{i-1}/KL_i) \cong Gal(L_{i-1}/L_{i-1}\cap KL_i) \le Gal(L_{i-1}/L_i) \cong \mathbb{Z}_p$, so $Gal(KL_{i-1}/KL_i)$ is isomorphic to either $\{e\}$ or $\mathbb{Z}_p$. Now, $F \to K$ is radical, so $F \to KL$ is radical, and $L \subseteq KL$, so $F \to L$ is solvable. $\square$

Constructibility

Def'n: A number is constructible if it is the x or y coordinate of a point which can be made by starting with points $(0,0)$ and $(1,0)$ and iteratively either drawing a line between two points or making a circle at a point with radius the distance between any two previously obtained points.

Theorem: Let $K = \{\alpha \in \mathbb{R} \mid \alpha \text{ is constructible}\}$. Then K is a field.

Pf: See constructible notes.

Lemma: If $\alpha \in \mathbb{R}$ then $\sqrt{|\alpha|}$ is constructible.

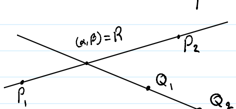
Pf: Homework 10 Question 2.

Theorem: Let $\alpha \in K$. Then α is constructible if and only if there is a tower $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n$, each $F_i \subseteq \mathbb{R}$ and $[F_i : F_{i-1}] = 2$, $\alpha \in F_n$.

Pf: Suppose $\alpha \in K$. We go by induction on the number of steps to construct α. There are 3 cases for the final step:

Case 1: α is the coordinate of a point gotten by intersecting two lines.

We have

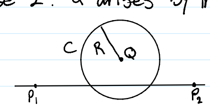


$P_1 = (a_1, b_1)$, $P_2 = (a_2, b_2)$, $Q_1 = (c_1, d_1)$, $Q_2 = (c_2, d_2)$.

The lines are then given by $y_1 - b_1 = \frac{b_2 - b_1}{a_2 - a_1}\cdot(x - a_1)$ and $y_2 - d_1 = \frac{d_2 - d_1}{c_2 - c_1}(x - c_1)$.

Take $F = \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2)$. Then $\alpha, \beta \in F$ and we are done.

Case 2: α arises by intersecting a line and a circle.



$L = P_1P_2$, $Q = (x_0, y_0)$. We write L as $y = mx + b$, $m, b \in F$ (assume all coordinates lie in previously attained tower).

For C, we have equation $(x-x_0)^2 + (y-y_0)^2 = R^2$. Now, α is a coordinate of a solution to the quadratic $(x-x_0)^2 + (mx+b-y_0)^2 = R^2$.

By quadratic formula, α is in a real quadratic extension of F.

Case 3: α arises by intersecting two circles.

We find circles $(x-a)^2 + (y-b)^2 = R_1^2$, $(x-c)^2 + (y-d)^2 = R_2^2$. Taking the difference gives a linear equation in x and y.

Now we are back in case 2.

Conversely, assume we have $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \mathbb{R}$ where each $[F_{i+1} : F_i] = 2$ and $\alpha \in F_n$.

By induction. If $n = 0$ we are done as $\mathbb{Q} \subseteq K$.

Now assume each $F_i \subseteq K$ and $F_{i+1} = F_i(\sqrt{\alpha_i})$ for some $\alpha_i \in F_i$ not a square. By lemma, $\sqrt{\alpha_i} \in K$ so each $F_i \subseteq K$ $\forall i$. $\square$

Corollary: $\alpha \in K$ implies $\deg_{\mathbb{Q}}(\alpha)$ is a power of 2 [Converse not true - see homework 10].

Consequences:

1) You cannot square a circle:

If C is a circle with radius 1, then C has area π. If you could square a circle, then the square would have sidelength $\sqrt{\pi}$.

But π is not algebraic so $\sqrt{\pi}$ is not algebraic. No such tower exists so by theorem a circle cannot be squared.

2) Cannot trisect an arbitrary angle.

We show we cannot trisect a $60°$ angle. If we could, we could construct $\alpha = \cos 20°$.

We have $\cos 60° = 4\alpha^3 - 3\alpha$ by identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Hence, $4\alpha^3 - 3\alpha - 1/2 = 0$.

But this polynomial in $\mathbb{Q}[x]$ is irreducible so $\deg_{\mathbb{Q}}(\alpha) = 3$. By theorem α is not constructible.

Remark: We can define $\tilde{K} = \{a + ib \mid a, b \in K\}$. This is a subfield of $\mathbb{C}$ and consists of constructible complex numbers.

Theorem: $\alpha \in \tilde{K}$ if and only α is contained in some $K_n \subseteq \mathbb{C}$ where $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ and each $[K_i : K_{i-1}] = 2$.

Pf: If $\alpha \in \tilde{K}$, then $a, b \in K$ where $\alpha = a + ib$, $a, b \in \mathbb{R}$. Now by previous theorem a, b are in quadratic towers.

Combining these and adjoining i gives a quadratic tower for α.

If instead a tower exists, then since $\tilde{K}$ is closed under quadratic extensions (by quadratic formula) we are done. $\square$

Theorem: $\alpha \in \tilde{K}$ if and only if the splitting field of $m_{\alpha,\mathbb{Q}}$ has degree a power of 2 over $\mathbb{Q}$.

Pf: Consider $\alpha \in \tilde{K}$. Then there is a tower $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n \subseteq \mathbb{C}$ with $\alpha \in K_n$ and $[K_i : K_{i-1}] = 2$ $\forall 1 \le i \le n$.

Let L be the normal closure of K_n. So $L = \prod_i \sigma_i(K_n)$, where $\sigma_i : K_n \to \mathbb{C}$ is an embedding fixing $\mathbb{Q}$.

Now we have $K_0 \overset{2}{\subseteq} K_1 \overset{2}{\subseteq} \dots \overset{2}{\subseteq} K_n \overset{1 \text{ or } 2}{\subseteq} K_n\sigma_1(K_0) \overset{1 \text{ or } 2}{\subseteq} K_n\sigma_1(K_1) \overset{1 \text{ or } 2}{\subseteq} \dots \overset{1 \text{ or } 2}{\subseteq} K_n\sigma_1(K_n) = K_n\sigma_1(K_n)\sigma_2(K_0) \overset{1 \text{ or } 2}{\subseteq} \dots \overset{1 \text{ or } 2}{\subseteq} L$.

The total degree is a power of 2. Since $SF(m_{\alpha,\mathbb{Q}}) \subseteq L$, it must also be a power of 2 by tower law.

Conversely, let $L' = SF(m_{\alpha,\mathbb{Q}})$ and assume $\exists m \in \mathbb{Z}_{\ge 0}$ such that $[L' : \mathbb{Q}] = |Gal(L'/\mathbb{Q})| = 2^m$.

Then there is a chain $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_m = G$ where $[G_i : G_{i-1}] = 2$ for each $1 \le i \le m$.

Now there is a tower of quadratic extensions (fixed fields) containing α so $\alpha \in \tilde{K}$ by theorem. $\square$

Cyclotomic Polynomials and Constructing a Regular n-gon

Observation: A regular n-gon is constructible if and only if $\tilde{K}$ contains a primitive n'th root of unity.

Remark: Let α be a primitive m'th root of unity. Then $\mathbb{Q}(\alpha)$ is the splitting field of $m_{\alpha,\mathbb{Q}}$.

Hence, $\alpha \in \tilde{K}$ if and only if $\deg(m_{\alpha,\mathbb{Q}})$ is a power of 2.

Def'n: The n'th cyclotomic polynomial is $\Phi_n := \prod_{\mu}(x - \mu)$ where μ ranges over the primitive n'th roots of unity.

Def'n: Let $f = \sum_{i=0}^{n} c_i x^i \in \mathbb{Z}[x]$. We say f is primitive if $\gcd(c_0, c_1, \dots, c_n) = 1$.

Lemma: If $f, g \in \mathbb{Z}[x]$ are primitive, then so is $f \cdot g$.

Pf: Write $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$. Let p be a prime not dividing all a_i and not dividing all b_j such that $p \mid a_0, \dots, a_i$ and $p \mid b_0, \dots, b_j$ but $p \nmid a_{i+1}, b_{j+1}$.

Then the coefficient of x^{i+j+2} in $f \cdot g$ is $c = \underbrace{a_0 b_{i+j+2} + a_1 b_{i+j+1} + \dots + a_i b_{j+2}}_{\text{divisible by } p} + \underbrace{a_{i+1} b_{j+1}}_{\text{not divisible by } p} + \underbrace{\dots + a_{i+j+2} b_0}_{\text{divisible by } p.}$

Thus, $p \nmid c$ and p divides all other coefficients, so $f \cdot g$ is primitive. $\square$

Corollary: Let $f \in \mathbb{Z}[x]$, $g, h \in \mathbb{Q}[x]$ monic such that $f = gh$. Then $g, h \in \mathbb{Z}[x]$.

Pf: There are $\lambda_g, \lambda_h \in \mathbb{Z}$ such that $\tilde{g} = \lambda_g g$, $\tilde{h} = \lambda_h h \in \mathbb{Z}[x]$ are primitive.

Then $\lambda_g \lambda_h gh = \lambda_g \lambda_h f$ is primitive. Thus, $\lambda_g = \lambda_h = \pm 1$ so $g, h \in \mathbb{Z}[x]$. $\square$

Pf: There are $\lambda_g, \lambda_h \in \mathbb{Z}$ such that $\tilde{g} = \lambda_g g$, $h = \lambda_h h \in \mathbb{Z}[x]$ are primitive.

Then $\lambda_g \lambda_h gh = \lambda_g \lambda_h f$ is primitive. Thus, $\lambda_g = \lambda_h = \pm 1$ so $g, h \in \mathbb{Z}[x]$. $\square$

Theorem: $\Phi_n = m_{\alpha,\mathbb{Q}} \in \mathbb{Q}[x]$, where α is a primitive n'th root of unity.

Pf: Note α is a root of $x^n - 1$, so $m_{\alpha,\mathbb{Q}} \mid x^n - 1$.

By the corollary, $m_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x]$ as there is $h \in \mathbb{Q}[x]$ so that $x^n - 1 = h \cdot m_{\alpha,\mathbb{Q}}$.

We claim that if p is a prime and $p \nmid n$, then $m_{\alpha,\mathbb{Q}}(\alpha^p) = 0$.

If we can show this, then since $m_{\alpha,\mathbb{Q}}$ only has primitive n'th roots of unity as roots, we can conclude that the theorem holds.

The primitive n'th roots of unity are given by α^k such that $\gcd(k,n) = 1$. Now, if $k = p_1 \dots p_\ell$ is the prime factorization of k, then each $p_i \nmid n$. Hence, $\alpha^k = (\alpha^{p_2 \dots p_\ell})^{p_1}$ is a root by an inductive argument.

Thus, we need only show the claim.

Assume α^p is not a root. Then α^p is a root of h. Now $h(x^p)$ has α as a root so $m_{\alpha,\mathbb{Q}} \mid h(x^p)$.

Hence, there is $g \in \mathbb{Q}[x]$ such that $h(x^p) = g \cdot m_{\alpha,\mathbb{Q}}$. By corollary, $g \in \mathbb{Z}[x]$. Now lets instead look in $\mathbb{Z}/p\mathbb{Z}\,[x]$.

Set $\bar{g} = g$, $\bar{h} = h$, $\bar{m}_\alpha = m_{\alpha,\mathbb{Q}} \pmod p$. We have $\bar{h}(x^p) = [\bar{h}(x)]^p$ as $[\bar{h}(x)]^p = (\sum_i \gamma_i x^i)^p = \sum_i \gamma_i^p x^{ip} = \sum_i \gamma_i (x^p)^i = \bar{h}(x^p)$ ($\gamma_i^p = \gamma_i$ by Frobenius).

Thus, $\bar{h}(x^p) = \bar{g}\,\bar{m}_\alpha = (\bar{h}(x))^p$ and so $\bar{h}$ and $\bar{m}_\alpha$ share a root (mod p).

But $\overline{x^n - 1} = \bar{h} \cdot \bar{m}_\alpha$ is separable (take formal derivative, note $p \nmid n$), a contradiction. $\square$

Corollary: $\deg(\alpha) = \deg(\Phi_n) = \phi(n) = |\{k \in \mathbb{N} \mid \gcd(k,n) = 1\}|$.

Theorem: Properties of $\phi(n)$:

1) If p is prime, $\phi(p) = p - 1$.

2) If p is prime, $\phi(p^k) = p^{k-1}(p-1)$

3) If p_i are distinct primes and $e_i \in \mathbb{Z}_{>0}$, then $\phi(p_1^{e_1} \dots p_r^{e_r}) = \phi(p_1^{e_1}) \cdot \ldots \cdot \phi(p_r^{e_r})$.

Proposition: The regular n-gon is constructible if and only if for $n = p_1^{e_1} \dots p_r^{e_r}$, p_i distinct primes, $e_i \in \mathbb{Z}_{>0}$, then $p_i = 2$ or $p_i = 2^k + 1$ and $e_i = 1$.

Pf: If the regular n-gon is constructible, then $\phi(n)$ is a power of 2. Then $p_i = 2$ or $p_i = 2^k + 1$ and $e_i = 1$.

Conversely, we have that $\phi(n)$ is a power of 2 so we are done. $\square$

Remark: For $3 \le n \le 20$, the regular n-gon is constructible if $n \in \{3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20\}$.

Computing Galois Groups

Motivation: Let F be a field of characteristic not equal to 2. Let $f \in F[x]$ be an irreducible cubic and K the splitting field of f.

We have shown that $\mathrm{Gal}(K/F) = \begin{cases} S_3, & \sqrt{\Delta(f)} \notin F \\ A_3, & \sqrt{\Delta(f)} \in F \end{cases}$. Can we generalize this?

Setting: Let F be a field of characteristic not equal to 2. Let $f \in F[x]$ be irreducible and separable of degree n, K its splitting field.

Let $G = \mathrm{Gal}(K/F)$. We want to compute G. Suppose f has distinct roots $\alpha_1, \dots, \alpha_n$ and let $G \cong \tilde{G} \le S_n$.

Another labelling of the roots is given by the action of any $\sigma \in S_n$ on the α_i (i.e., $\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}$ is a relabelling). In this case, G is embedded in S_n as $\sigma \tilde{G} \sigma^{-1}$. That is, we only care up to conjugation.

Def'n: A subgroup H of S_n is called transitive if $\mathrm{Orb}(i) = \{1, 2, \dots, n\}$ for all $i \in \{1, 2, \dots, n\}$ (with the permutation action on $\{1, 2, \dots, n\}$).

Proposition: Let f and K be as above. Suppose $G = \mathrm{Gal}(K/F) \cong H \le S_n$. Then H is transitive.

Pf: Consider roots of f α_i and α_j. Then $F(\alpha_i) \cong F[x]/\langle f \rangle \cong F(\alpha_j)$. We can lift this isomorphism to an automorphism of K.

Hence, $\mathrm{Orb}(i) = \{1, 2, \dots, n\}$ so H is transitive. $\square$

We follow the following steps to compute G:

Step 1: Identify all transitive subgroups of S_n (up to conjugation).

We follow the following steps to compute G:

Step 1: Identify all transitive subgroups of S_n (up to conjugation).

Step 2: Given a transitive subgroup H of S_n, identify $\varphi \in F[x_1,\dots,x_n]$ such that $\mathrm{Stab}(\varphi) = H$, under the action of S_n on $\{1,2,\dots,n\}$.

Step 3: Compute resolvents.

Define $\theta = \prod_{\sigma \in S_n/H} (y - \sigma\varphi) \in F[x_1,\dots,x_n][y]$.

This is well-defined, as if $\sigma' = \sigma \cdot h$, then $\sigma'\varphi = (\sigma h)\varphi = \sigma(h\varphi) = \sigma\varphi$, for any $h \in H$.

Notice, $\theta(y)$ is symmetric in $x_1,\dots,x_n$. To see this, let $\tau \in S_n$. Then

$\tau\theta = \tau \prod_{\sigma \in S_n/H} (y - \sigma\varphi) = \prod_{\sigma \in S_n/H} (y - \tau\sigma\varphi) = \prod_{\sigma' \in S_n/H} (y - \sigma'\varphi) = \theta$. Thus, $\theta(y) \in F[x_1,\dots,x_n]^{S_n}[y] = F[s_1,\dots,s_n][y]$.

Step 4: Use resolvents.

Substitute the coefficients of f into the s_i to get $\theta_f(y) = \theta(y)|_{x_i = \alpha_i} \in F[y]$.

Proposition: Let F be a field and $f \in F[x]$ be separable and irreducible. Let $G = \mathrm{Gal}(f)$.

Let $\varphi \in F[x_1,\dots,x_n]$, and set $\mathrm{Stab}(\varphi) = H$. Then

(1) If G is conjugate to a subgroup of H, θ_f has a root in F.

(2) If θ_f has a simple root in F, then G is conjugate to a subgroup of H.

Pf: (1) After relabelling, we may assume $G \leq H$ (so φ is fixed under G).

Notice, $\theta_f = \prod_{[\sigma] \in S_n/H} (y - \sigma\varphi(\alpha_1,\dots,\alpha_n))$ has $y - \varphi(\alpha_1,\dots,\alpha_n)$ as a factor (the α_i distinct roots of f).

Let $g \in G$. Then $g.\varphi(\alpha_1,\dots,\alpha_n) = (g\varphi)(\alpha_1,\dots,\alpha_n) = \varphi(\alpha_1,\dots,\alpha_n)$, so φ is fixed under each $g \in G$. Hence, $\varphi(\alpha_1,\dots,\alpha_n) \in F$.

That is, θ_f has a root in F.

(2) After relabelling, we may assume $\varphi(\alpha_1,\dots,\alpha_n)$ is a root of θ_f.

Suppose $G \not\leq H$, so there is $\tau \in G$ such that $\tau\varphi \neq \varphi$.

Now, $\theta = (y - \varphi)(y - \tau\varphi)\dots$, and hence $\theta_f = (y - \varphi(\alpha_1,\dots,\alpha_n))(y - \tau\varphi(\alpha_1,\dots,\alpha_n))\dots$

But we assume $\varphi(\alpha_1,\dots,\alpha_n) \in F$, so $\tau(\varphi(\alpha_1,\dots,\alpha_n)) = (\tau\varphi)(\alpha_1,\dots,\alpha_n) \in F$. But then $\tau\varphi(\alpha_1,\dots,\alpha_n) = \varphi(\alpha_1,\dots,\alpha_n)$

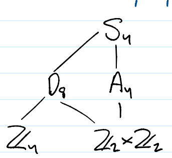
so θ_f has a non-simple root at $\varphi(\alpha_1,\dots,\alpha_n)$, a contradiction. $\square$

Remark: If all θ_f don't have multiple roots, this determines G (up to conjugation).

The Tschirnhausen transformation can transform f to a polynomial G with the same Galois group if there are multiple roots.

Galois Group of Quartics

The transitive subgroup structure of S_4 is:



$\theta = (y - (x_1x_2 + x_3x_4))(y - (x_1x_3 + x_2x_4))(y - (x_1x_4 + x_2x_3))$.

Notice $\Delta\theta_f = \Delta_f \neq 0$, so f is separable.

By proposition, $G = \mathrm{Gal}(f)$ is contained in a subgroup contained in a subgroup of S_4 isomorphic to D_8 if and only if θ_f has a root in F.

Now: $\cdot$ $G = S_4 \iff \sqrt{\Delta_f} \notin F$ and θ_f has no root in F.

$\cdot$ $G = A_4 \iff \sqrt{\Delta_f} \in F$ and θ_f has no root in F.

$\cdot$ $G \cong D_8$ or $G \cong \mathbb{Z}_4 \iff \sqrt{\Delta_f} \notin F$ and θ_f has a root in F.

$\cdot$ $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \iff \sqrt{\Delta_f} \in F$ and θ_f has a root in F.

To distinguish between D_8 and $\mathbb{Z}_4$, we can:

(1) We get $\mathbb{Z}_4$ if and only if f splits after adjoining a single root.

(2) Use a resolvent for $\mathbb{Z}_4$ (this has degree 6), and deal with multiple roots.

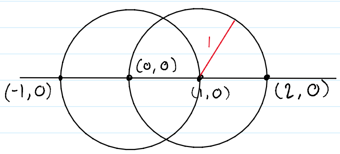
(3) Use quartic formula, which gives a complicated criterion involving roots of θ_f.

(2) Use a resolvent for $\mathbb{Z}_4$ (this has degree 6), and deal with multiple roots.

(3) Use quartic formula, which gives a complicated criterion involving roots of θ_f.

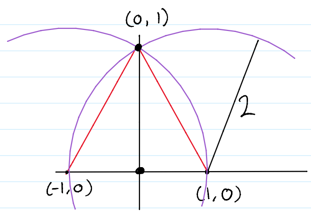
End of course notes.

Constructibility Diagrams:



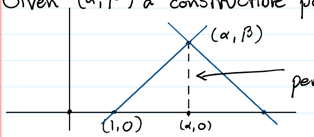
All integers are constructible.

Constructing the y-axis (namely, (0,1)):



A similar construction gives perpendicular bisectors.

Given (α,β) a constructible point, we can construct $(\alpha,0)$ and $(0,\alpha)$ by perpendicular projections onto the axes.

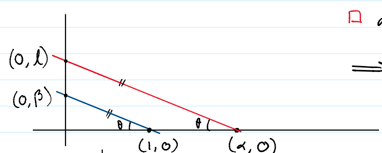


perpendicular bisector. Now, circle of radius α gives $(0,\alpha)$.

If α,β are constructible, then $\alpha+\beta$, $\beta-\alpha$, $\alpha\beta$, and β/α $[\alpha\neq 0]$ are constructible. Assume $\alpha\leq\beta$.

For $\alpha+\beta$, draw circle of radius α about $(\beta,0)$, this also gives $\beta-\alpha$.

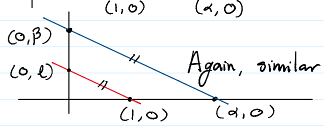
For $\alpha\beta$:



$\square$ and $\square$ are similar!

$\implies \frac{\alpha}{1}=\frac{\ell}{\beta}\implies \ell=\alpha\beta$ is constructible.

For β/α:



Again, similar triangles: $\ell/\beta = 1/\alpha$, or $\ell=\beta/\alpha$ is constructible.

Lemma: Let $F\to K$ be Galois with $Gal(K/F)\cong\mathbb{Z}_p$ for some prime p, and assume F has all p'th roots of unity.

Then $F\to K$ is a principal radical extension.

Claim: Let $F\to L$ be Galois and $Gal(L/F)$ solvable. Then $F\to L$ is solvable.

Pf of claim: Let $\{e\}=G_0\trianglelefteq G_1\trianglelefteq G_2\trianglelefteq\dots\trianglelefteq G_m=Gal(L/F)=G$ be a composition series for G with abelian quotients.

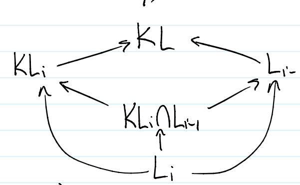
Define $L_i=L^{G_i}$ for all $0\leq i\leq m$. Then we have a tower of extensions $F=L_m\to L_{m-1}\to\dots\to L_0=L$.

Notice, G_i/G_{i-1} is simple and abelian for all i, so is thus cyclic of prime order, say $G_i/G_{i-1}\cong\mathbb{Z}_{p_i}$ for each i.

Furthermore, $Gal(L_{i-1}/L_i)\cong \frac{Gal(L/L_i)}{Gal(L/L_{i-1})}=G_i/G_{i-1}$, so $Gal(L_{i-1}/L_i)$ is cyclic of prime order.

Note this isomorphism holds as $G_{i-1}\trianglelefteq G_i$, so $L_i\to L_{i-1}$ is normal and $Gal(L_{i-1}/L_i)\cong G_i/G_{i-1}$ by the 2nd part of the Galois correspondence. Now let $F\to K$ be the extension where we adjoin all p_i'th roots of unity, for all $1\leq i\leq m$.

Now we have a tower $F\to K\to KL_m\to KL_{m-1}\to\dots\to KL_0=KL$.



Notice, $F\to K$ is radical, we show KL is radical over F. For each i, we have

Since $L_i\to L_{i-1}$ is Galois (separable by characteristic 0), the base change theorem tells us that $KL_i\to KL_{i-1}$ is Galois and $Gal(KL_{i-1}/KL_i)\cong Gal(L_{i-1}/L_{i-1}\cap KL_i)\leq Gal(L_{i-1}/L_i)\cong\mathbb{Z}_{p_i}$.

Thus, applying the lemma gives that $KL_i\to KL_{i-1}$ is a principal radical extension for each $1\leq i\leq m$.

That is, $K\to KL$ is radical. But $L\subseteq KL$, so $F\to L$ is solvable.

$\square$