Chapter 1

Conjugacy over $\mathbb{R}, \mathbb{Q}$

- k-tuples $\underline{z} = (z_1, \ldots, x_k), \underline{w} = (w_1, \ldots, w_k) \in \mathbb{C}^k$ **conjugate** over $K \in \{\mathbb{Q}, \mathbb{R}\}$ if $\forall p \in K[t_1, \ldots, t_n], p(\underline{z}) = 0 \iff p(\underline{w}) = 0$.
- $z_1, z_2 \in \mathbb{C}$ conjugate over $\mathbb{R} \iff z_1 = z_2 \vee z_1 = \bar{z}_2$.

($\implies$): Let $z_1 = x + iy$, then root of $p(z) = (z-x)^2 + y^2$. z_1, z_2 conjugate so $p(z_2) = 0 \iff z_2 - x = \pm iy$. ($\impliedby$): z_1, z_2 conjugate. Let $z_2 = \bar{z}_1$. Complex conjugation ring homomorphism $\therefore$
$p(t) = \sum a_i t^i \implies \overline{p(t)} = \sum a_i \bar{t}^i = p(\bar{t}) \implies p(z_1) = 0 \iff \overline{p(z_1)} = \bar{0} \iff p(\bar{z}_2) = 0$

The Galois Group

Definition

- $f \in \mathbb{Q}[t]$ has roots $\alpha_1, \ldots, \alpha_k$, then $Gal(f) = \{\sigma \in S_k | (\alpha_1, \ldots, \alpha_k), (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}\ conjugate\} \leq S_k$
- S_k acts on $\mathbb{Q}[t_1, \ldots, t_k]$ via $(\sigma p)(t_1, \ldots, t_k) = p(t_{\sigma(1)}, \ldots, t_{\sigma(k)})$. $\sigma \in Gal(f)$ iff $p(\alpha_1, \ldots, \alpha_k) = 0 \iff (\sigma p)(\alpha_1, \ldots, \alpha_k) = 0$. Then $\iota \in Gal(f) \neq \emptyset$. If $\sigma \in Gal(f) \subseteq S_k$, $\sigma^{-1} p \in \mathbb{Q}[t_1, \ldots, t_k]$, so $\sigma^{-1} p = 0 \iff \sigma(\sigma^{-1} p) = 0 \iff p = 0$ so $\sigma^{-1} \in Gal(f)$. If $\sigma, \tau \in Gal(f)$, $\sigma p \in \mathbb{Q}[t_1, \ldots, t_k]$, so $\tau p = 0 \iff \tau(\sigma p) = 0$ and $\tau p = 0 \iff p = 0$, so $(\tau\sigma)p = 0 \iff p = 0$, so $\tau\sigma \in Gal(f)$

Examples for Simple Polynomials

- $f \in \mathbb{Q}[t]$ with rational roots then $Gal(f) = \{\iota\}$; if f is quadratic with non-rational roots, these are conjugate, so $Gal(f) = S_2$
- if $f = t^4 + t^3 + t^2 + t + 1$, roots are non-1 roots of unity, $Gal(f) \cong C_4 = \langle (1243) \rangle$; transpositions not part of Galois Group (use $p(t_1, t_2, t_3, t_4) = t_1^2 - t_2$)
- $f(t) = t^5 - 6t + 3$ has $Gal(f) = S_5$, so not solvable

Chapter 2

Group Actions

Definition

G acts on set X via $G \times X \to X, (g, x) \mapsto gx$ such that: 1) $\forall x \in X, 1_G x = x$, 2) $\forall g, h \in G, \forall x \in X, (gh)x = g(hx)$

Abstract Symmetry Group

- $Sym(X)$ is the set of all bijections $X \to X$. Forms a group under composition. If $X = \{1, \ldots, n\}$, $\mathrm{Sym}(X) = S_n$.
- if G acts on X, $g \in G$ leads to $\bar{g} : X \to X, \bar{g}(x) = gx$. This induces homomorphism $\Sigma : G \to \mathrm{Sym}(X)$, since $\bar{g}$ is a bijection with inverse $\overline{g^{-1}}$.

Equivalent Conditions for Faithful Actions

1. G acts faithfully on X ($\forall g, h \in G, \forall x \in X, gx = hx \implies g = h$)
2. for any $g \in G$, if $\forall x \in X, gx = x$ then $g = 1_G$
3. $\Sigma : G \to Sym(X)$ is injective / $\ker(\Sigma) = \{1_G\}$

Examples of Group Actions

1. Sym(X) acts on X via $gx = g(x)$. If $g \in \mathrm{Sym}(X)$, $\bar{g} = g$, so $\Sigma = \iota$; this is injective, so $\mathrm{Sym}(X)$ acts faithfully.
2. Aut(X) $\subseteq$ Sym(X) contains automorphisms of X. GL($\mathbb{R}; n$) acts on $X = \mathbb{R}^n$ via matrix multiplication. Σ is the inclusion $\Sigma(g) = g$, which is injective, so Aut(X) acts faithfully.
3. 48 isometries of cube (rotations + reflection) act on 6 faces, 12 edges, 8 vertices & 4 long diagonals. Action on vertices induces $\Sigma : G \to S_{12}$, $\Sigma(g) = \sigma_g$ where $gx_i = x_{\sigma_g(i)}$.

Action on faces/edges/vertices has $\ker(\Sigma) = \{e\}$, so faithful. Action on long diagonals not faithful (Σ can't be injective, as $|S_4| = 24 < 48 = |G|$)

4. the trivial action $gx = x$ is only faithful if G trivial

Sym(X) Contains a Copy of G if Faithful (Lemma 2.1.11)

If $\Sigma : G \to Sym(X)$ and G acts faithfully on X, then $G \cong \mathrm{im}(\Sigma) \leq \mathrm{Sym}(X)$.

G faithful $\therefore$ Σ injective $\therefore$ induced isomorphism between G and $\mathrm{im}(\Sigma)$.

No cube vertex isometry swaps vertices leaving the rest fixed, so $\mathrm{im}(\Sigma) \leq S_8$ contains no 2-cycles.

The Fixed Set

Definition

G acts on X, $S \subseteq G$. Define **fixed set** of S as $\mathrm{Fix}(S) = \{x \in X | \forall x \in S, sx = x\}$.

Conjugating the Fixed Set (Lemma 2.1.15)

$\forall g \in G, \mathrm{Fix}(gSg^{-1}) = g\,\mathrm{Fix}(S)$

$x \in Fix(gSg^{-1}) \iff \forall s \in S, gsg^{-1}x = x \iff \forall s \in S, s(g^{-1}x) = g^{-1}x \iff g^{-1}x \in Fix(S) \iff x \in gFix(S)$

Rings

Definition

Set $(R, +, \cdot)$, with $(R, +)$ abelian group with identity 0_R, $(R, \cdot)$ commutative monoid (multiplication associative & commutative, 1_R is multiplicative identity) and distributivity holds in R.

Ideals, Subrings and the Trivial Ring

- $I \subseteq R$ where $I \neq \emptyset$, I closed under subtraction & $\forall i \in I, \forall r \in R, ri, ir \in I$.
- if $Y \subseteq R$, $\langle Y \rangle$ is the **ideal generated** by Y (smallest ideal containing Y; either intersection of all ideals containing Y, or $\langle Y \rangle = \{\sum a_i r_i | r_i \in I, a_i \in R\}$, since if $Y \subseteq J$, then $r_i \in J$, and any $R-$linear combination must be in J by ideal closure, so $\langle Y \rangle \subseteq J$).
- a **principal ideal** is an ideal generated by one element $\langle r \rangle, r \in R$
- $S \subseteq R$ where $0_R, 1_R \in S$ and S closed under subtraction and multiplication.
- the only subring which is also an ideal is R itself (if $1_R \in I$, then $I = R$)
- any intersection of subrings/ideals of R is a subring/ideal of R.
- $R = \{0_R\}$ is the **trivial ring**, where $0_R = 1_R$; the only such ring (if S has $0_S = 1_S$, $s \in S \setminus \{0_S\}$, then $s \cdot 0_S = s \cdot 1_S \implies s = 0_S$).

Ring Homomorphisms

- Mapping $\varphi : R \to S$ such that if $r_1, r_2 \in R$, 1) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$, 2) $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$, 3) $\varphi(1_R) = 1_S$. From these, we get 4) $\varphi(0_R) = 0_S$, 5) $\varphi(-r) = -\varphi(r)$.
- $\ker(\varphi)$ is an ideal of R, and $\mathrm{im}(\varphi)$ is a subring of S.

The Characteristic Homomorphism: From $\mathbb{Z}$ to R

$\exists! \chi : \mathbb{Z} \to \mathbb{R}$, where $\chi(n) = n \cdot 1_R = \sum_n 1_R$ or recursively $\chi(0) = 0_R$, if $n > 0$, $\chi(n) = \chi(n-1) + 1_R$, if $n < 0$, $\chi(n) = -\chi(-n)$.

$\chi(0) = 0_R, \chi(1) = 1_R$ immediate, $\chi(n+m) = \chi(n) + \chi(m)$ immdiate.
$\chi(nm) = \sum_{i=1}^n 1_R \cdot \left[\sum_{j=1}^m 1_R\right] = \chi(n)\chi(m)$. If $\exists \varphi : \mathbb{Z} \to \mathbb{R}$ with $\chi \neq \varphi$, since both homomorphisms, they preserve identity; inductively assume $\chi(n) = \varphi(n)$, then for $n > 0$ $\varphi(n+1) = 1_R + \varphi(n) = 1_R + \chi(n) = \chi(n+1)$, and result follows for $n < 0$, so χ unique.

The Universal Property of Factor Rings

Let $I \triangleleft R$. A **factor ring** is a ring R/I, whose elements are cosets $r + I = \{r + i | i \in I\}$. Canonical homomorphism $\pi_I : R \to R/I$ by $r \mapsto r + I$.

1. π_I is surjective & $\ker(\pi_I) = I$
2. if $\varphi : R \to S$ ring homomorphism & $\varphi(I) = \{0_S\}$ ($I \subseteq \ker(\varphi)$), then $\exists! \bar{\varphi} : R/I \to S$ via $\varphi = \bar{\varphi} \circ \pi_I$.

The **First Isomorphism Theorem**: if $\ker(\varphi) = I$, then $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Integral Domains

- ring where $0_R \neq 1_R$ & $\forall r_1, r_2 \in R$, if $r_1 r_2 = 0_R$ then $r_1 = 0_R$ or $r_2 = 0_R$
- the cancellation law applies: $r_1 s = r_2 s \implies r_1 = r_2 \vee s = 0_R$
- a **principal ideal domain** (PID) is an ID where every ideal is principal
- $\mathbb{Z}$ is PID: it is ID; if $I \triangleleft \mathbb{Z}$, let $n \in I$ be smallest non-zero integer. If $b \in I$, by division algorithm, $b = nq + r, q, r \in \mathbb{Z}, r < n$ so $r = b - nq \in I$. But $r < n$ and n is smallest $\therefore$ $r = 0$ so $b = nq \implies I = \langle n \rangle$

Units in Rings

- a unit $u \in R$ has a multiplicative inverse
- $u \in R$ is a unit $\iff \langle u \rangle = R$ (if unit, $u(u^{-1}r) = r \in \langle u \rangle$ for any $r \in R$; else if $\langle u \rangle = R$, then $1_R \in \langle u \rangle$ so $\exists r \in R : 1_R = ur$ and $r = u^{-1} \in R$)
- if $r, s \in R$, r divides s ($r|s$) if $\exists a \in R : s = ar$ (equivalently: $s \in \langle r \rangle$ or $\langle s \rangle \subseteq \langle r \rangle$)
- $r, s \in R$ are **coprime** if $\forall a \in R$ such that $a|r, a|s$, a is a unit
- set of units in R form a **group** $R^\times$ under mutliplication

Bezout's Identity (Proposition 2.2.16)

If R is PID and $r, s \in R$, then r, s coprime $\iff \exists a, b \in R : ar + bs = 1_R$.

($\implies$): R is PID $\therefore \exists u \in R : \langle r, s \rangle = \langle u \rangle$. $r \in \langle u \rangle, s \in \langle u \rangle$, so $u|r, u|s$. r, s coprime $\therefore u$ is unit $\therefore R = \langle u \rangle = \langle r, s \rangle \therefore \exists a, b \in R : ar + bs = 1_R$. ($\impliedby$): if $u|r$, $u|s$, then $u|ar + bs$ $u|1_R \therefore \exists x \in R : ux = 1_R \therefore u$ unit $\therefore r, s$ coprime.

Mutual Divisibility in Integral Domains (Exercise 2.2.15)

If $r, s \in R$ PID and u unit, then $r|s|r \iff \langle r \rangle = \langle s \rangle \iff s = ur$.

$r|s|r \iff \langle s \rangle \subseteq \langle r \rangle \wedge \langle r \rangle \subseteq \langle s \rangle \iff \langle r \rangle = \langle s \rangle \iff \exists u, w \in R : s = ur$, $r = ws \iff s = uws \iff uw = 1_R \iff u$ unit.

Fields

Definition and Properties of Fields

- a field is a commutative ring R where $0_R \neq 1_R$ and $\forall r \in R$ r is a unit (so if $R^\times = R \setminus \{0_R\}$, then R is a field).
- every field is an integral domain; and every **finite** integral domain is a field (i.e $\mathbb{Z}$ not a field)
- fields only have **trivial ideals**: $\{0_R\}, R$ (ideals generated by units are the whole ring)
- **subfields** are subrings which are also fields
- $\mathbb{Z}_m$ is a field $\iff m$ is prime

The Field of Rational Expressions

- if K is a field, $K(t)$ (set of rational expressions $f/g, f, g \in K[t]$) is a field
- $f_1/g_1, f_2/g_2 \in K(t)$ are equal if $f_1 g_2 = f_2 g_1$

Field Homomorphisms are Injective (Lemma 2.3.3)

If $\varphi : K \to L$, $\ker(\varphi) \triangleleft K$, $\therefore \ker(\varphi) = \{0_K\}$ or $\ker(\varphi) = K$. φ homomorphism $\therefore$ $\varphi(1_K) = 1_L \neq 0_L$ (L is field) $\therefore \ker(\varphi) = \{0_K\} \therefore \varphi$ injective.

Subfields from Field Homomorphisms (Lemma 2.3.6)

Let $\varphi : K \to L$. Then, if $A \leq K$, $\varphi(A) \leq L$. If $B \leq L$, $\varphi^{-1}(B) \leq K$.

φ ring homomorphism $\therefore \varphi(A) \leq L$. A subfield, so $a, a^{-1} \in A$ and $\varphi(a^{-1}) = \varphi(a)^{-1} \in \varphi(A)$, so $\varphi(A)$ subfield.

Equalisers and Subfields (Lemma 2.3.8)

- X, Y sets, $S \subseteq \{f : X \to Y\}$, $Eq(S) = \{x \in X | \forall f, g \in S, f(x) = g(x)\}$
- if K, L fields and S subset of homomorphisms $K \to L$, $Eq(S) \leq K$
- for example, $S = \{\mathrm{id}_\mathbb{C}, \kappa\}$, κ complex conjugation, then $Eq(S) = \mathbb{R} \leq \mathbb{C}$.

$0_K, 1_K \in Eq(S)$ & $0_K \neq 1_K$, since $\varphi \in S$ field homomorphism. If $a, b \in Eq(S)$, let $\varphi, \theta \in Eq(S)$. Then $\varphi(a - b) = \varphi(a) - \varphi(b) = \theta(a) - \theta(b) = \theta(a - b) \therefore a - b \in Eq(S)$. Similarly, $ab, a^{-1} \in Eq(S)$.

The Characteristic of a Ring

Definition

- the characteristic of R is smallest $n \in \mathbb{N}$ such that $n \cdot 1_R = 0_R$ (if no such n, $\mathrm{char}(R) = 0$. Alternatively, $\mathbb{Z}$ is PID, so $\exists n \geq 0 : \ker(\chi) = \langle n \rangle$; $\mathrm{char}(R) = n$.
- $\mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{C}) = 0$, whereas $\mathrm{char}(\mathbb{Z}_p) = p$
- if K field, then $\mathrm{char}(K) = \mathrm{char}(K(t))$

Characteristic in Integral Domains (Lemma 2.3.11)

If K is ID (like fields), then $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ (p prime).

Let R ID. If $\mathrm{char}(R) = 0$, done; assume $\mathrm{char}(R) = n \geq 1$. $n = 1 \implies 1 \cdot 1_R = 0_R$ but in ID $1_R \neq 0_R$, so $n \geq 2$. $\exists k, m > 0 : km = n \therefore \chi(k)\chi(m) = \chi(n) = 0_R$. R is ID: WLOG $\chi(k) = 0_R$. Then, $k \in \ker(\chi) = \langle n \rangle \therefore n | k$. But $km = n \therefore k | n \therefore n = k \therefore n$ prime.

Field Homomorphisms and Characteristic (Lemma 2.3.12)

If $\varphi : K \to L$ field homomorphism, $\mathrm{char}(K) = \mathrm{char}(L)$.

$\varphi(n \cdot 1_K) = n \cdot 1_L = \chi_L(n)$. φ field homomorphism $\therefore$ injective $\therefore$ $n \cdot 1_L = 0_L \iff n \cdot 1_K = 0_K \iff \mathrm{char}(K) = \mathrm{char}(L)$.

Prime Subfields

Definition

- the smallest subfield of K (any other subfield contains it)
- either: intersection of all subfields of K, or $\{(m \cdot 1_K)/(n \cdot 1_K) | m, n \in \mathbb{Z}, n \cdot 1_K \neq 0_K\}$ (subfields contain 1_K, must contain any $n \cdot 1_K$ and closed under products and inverses $1/(m \cdot 1_K)$).

Number of Prime Subfields (Lemma 2.3.16)

Let K field. If $\mathrm{char}(K) = 0$, prime subfield is $\cong \mathbb{Q}$. If $\mathrm{char}(K) = p$ prime, prime subfield is $\cong \mathbb{F}_p$.

If $\mathrm{char}(K) = 0$, $n \cdot 1_K \neq 0$. Define field homomorphism $\varphi : \mathbb{Q} \to K$, $m/n \mapsto (m \cdot 1_K)/(n \cdot 1_K)$. φ injective induces isomorphism $\mathbb{Q} \cong \mathrm{im}(\varphi)$. $\mathbb{Q}$ has no proper subfields $\therefore \mathrm{im}(\varphi)$ no proper subfields $\therefore \mathrm{im}(\varphi) \leq K$ smallest subfield. If $\mathrm{char}(K) = p$, $\ker(\chi) = \langle p \rangle$. By FIT, $\mathrm{im}(\chi) \cong \mathbb{Z}/\langle p \rangle \cong \mathbb{F}_p$. $\mathbb{F}_p$ no proper subfields (Lagrange), so $\mathrm{im}(\chi)$ doesn't have proper subfields $\therefore \mathrm{im}(\chi) \leq K$ smallest subfield.

Finite Fields Have Positive Characteristic (Lemma 2.3.17)

If K finite & $\mathrm{char}(K) = 0$, $\mathbb{Q}$ prime subfield; but $\mathbb{Q}$ infinite, so contradiction.

Rings of Prime Characteristic

The Frobenius Map (Proposition 2.3.20)

Let $\mathrm{char}(R) = p$ prime. $\theta : R \to R, r \mapsto r^p$ is homomorphism. If R field, θ injective; if R finite field, θ automorphism.

$\theta(0_R) = 0_R, \theta(1_R) = 1_R, \theta(rs) = \theta(r)\theta(s)$. For additivity, $\theta(r + s) = (r + s)^p = \sum_{i=0}^p \binom{p}{i} r^i s^{p-i}$. From definition: $\binom{p}{i} = \frac{p!}{(p-i)!i!} \therefore p! = i!(p-i)! \binom{p}{i}$. Then, $p | p!$, $p \not| i!$, $p \not| (p-i)! \therefore p \left| \binom{p}{i} \right.$. $\mathrm{char}(R) = p$, so $\theta(r + s) = r^p + s^p = \theta(r) + \theta(s)$. If $|R| < \infty$, injectivity induces bijectivity.

pth Roots in Fields of Characteristic p (Corollary 2.3.22)

Let $\mathrm{char}(R) = p$ prime. If R field, every $a \in R$ has at most 1 pth root. If R finite field, every $a \in R$ has exactly 1 pth root.

Frobenius map θ injective for fields, $a \in R$ maps to unique $a^p \therefore x^p$ has at most 1 root. If R finite, θ is automorphism, so for each $x \in R$, $x = a^p$.

Examples of pth Roots

- in $\mathbb{Z}_p$, using FLT, $\theta(a) = a^p = a^{p-1}a = a$
- if $\mathrm{char}(R) = 2$, there is at most 1 square root
- over $\mathbb{C}$, p pth roots of unity; if $\mathrm{char}(K) = p$, only 1 (1_K)
- $t \in \mathbb{F}_p(t)$ has no pth root

Irreducible Ring Elements

Irreducibles and Reducibles

- $r \in R$ irreducible if $r \neq 0_R$, r not unit & $\forall a, b \in R$ if $ab = r$, then a or b is a unit (think of irreducibles as primes in $\mathbb{Z}$)
- $r \in R$ reducible if $r \neq 0_R$, r not unit and r not irreducible
- 0_R and units are neither reducible nor irreducible
- there are no irreducibles in fields (every $r \in R$ is unit)

Fields from Irreducibles in PIDs (Proposition 2.3.26)

Let R be PID, and $0_R \neq r \in R$. r irreducible $\iff R/\langle r \rangle$ field.

($\implies$): let r irreducible, & F be the ring $R/\langle r \rangle$. Let $\pi : R \to R/\langle r \rangle$ canonical map. $\ker(\pi) = \langle r \rangle$; r not a unit, so $1_R \notin \langle r \rangle \therefore \pi(1_R) = 1_F \neq 0_F$. F field if every $0_F \neq s \in F$ is unit. $\langle r \rangle \neq R$, so let $s \in R \setminus \langle r \rangle$. $s \notin \langle r \rangle \therefore r \not| s$. r only divisibly by units (since irreducible), so if $a|r$ and $a|s$, a is unit $\ r, s$ coprime $\therefore$ by Bezout (2.2.16) $\exists a, b \in R : ar + bs = 1_R$. Then,
$\pi(a)\pi(r) + \pi(b)\pi(s) = 1_F \implies \pi(b)\pi(s) = 1_F \iff \pi(s)^{-1} = \pi(b) \therefore \pi(s)$ unit $\therefore$ non-zero elements of F are units. ($\impliedby$): let $F = R/\langle r \rangle$ field. Then, $0_F \neq 1_F \therefore$ $\pi(1_R) \neq 0_F \therefore 1_R \notin \ker(\pi) = \langle r \rangle \therefore r \not| 1_R \therefore r$ no inverse. Assume $r = ab$. Then, $\pi(a)\pi(b) = 0_F$. R is PID; WLOG $\pi(a) = 0_F \therefore a \in \langle r \rangle \therefore a = rz \therefore r = ab = rzb$. By Cancellation Law, $zb = 1_R \therefore b$ unit.

Chapter 3

The Ring of Polynomials

Definition

- R ring generates ring $R[t]$ of polynomials over R $(a_0, a_1, \ldots)$ where $|\{i | a_i \neq 0\}| < \infty$.
- additive identity: $(0_R, 0_R, \ldots)$; multiplicative identity: $(1_R, 0_R, \ldots)$
- the **degree** $\deg(f) = n$ is largest n such that $a_n \neq 0$; if $f = 0_R, \deg(f) = -\infty$.

Polynomials Induce Ring Endomorphisms

- if $r \in R$ ring and $f \in R[t]$, f leads to endomorphism $r \mapsto \sum_i a_i r^i$
- if R is finite, finitely many endomorphisms but infinitely many polynomials $\therefore$ encomorphism isn't unique (i.e in $\mathbb{F}_2$, $f = t$ and $g = t^2$ generate same endomorphism, since $0^2 = 0$ & $1^2 = 1$, but $f \neq g$).

Homomorphisms Over Polynomial Rings

Universal Property of the Polynomial Ring (Proposition 3.1.6)

Let R, B rings, $\varphi : R \to B$ and $b \in B$. $\exists! \theta : R[t] \to B$ such that $\forall a \in R, \theta(a) = \varphi(a)$ & $\theta(t) = b$.

If θ satisfies above, $\theta\left(\sum_i a_i t^i\right) = \sum_i \varphi(a_i) b^i$, so θ uniquely determined by $\varphi(a_i), b^i$ $\therefore$ at most 1 such θ exists. Define $\theta\left(\sum_i a_i t^i\right) = \sum_i \varphi(a_i) b^i$. θ satisfies conditions, and is homomorphism $\therefore$ at least 1 such θ exists.

The Induced Homomorphism

$\varphi : R \to S$ induces **unique** homomorphism $\varphi_* : R[t] \to S[t]$ where $\forall a \in R, \varphi_*(a) = \varphi(a), \varphi_*(t) = t$.

The Evaluation Homomorphism

Evaluation induces a **unique** homomorphism $\mathrm{ev}_r : R[t] \to R$, where $r \in R$ and $\forall a \in R, \mathrm{ev}_r(a) = a, \mathrm{ev}_r(t) = r$.

The Substitution Homomorphism

There is **unique** homomorphism $\theta : R[t] \to R[u]$ such that $\forall a \in R, \theta(a) = a, \theta(t) = u + c$, where $c \in R$. This is an **isomorphism** ($\theta^{-1}(u) = t - c$), so $f(t)$ irreducible $\iff f(t - c)$ irreducible.

Properties of Polynomials

Polynomials Over Integral Domains (Lemma 3.1.11)

If R ID, $R[t]$ ID, & $\forall f, g \in R[t]$, $\deg(fg) = \deg(f) + \deg(g)$.

t has no pth Root in $\mathbb{F}_p(t)$ (Exercise 3.1.13)

If t has pth root, $\exists f, g \in \mathbb{F}_p(t) : f^p/g^p = t \therefore f^p = tg^p$. $\mathbb{F}_p(t)$ ID $\therefore$ $\deg(f^p) = \deg(t) + \deg(g^p) \therefore p \deg(f) = 1 + p \deg(g)$.

Irreducible Polynomials Over Fields (Lemma 3.1.14)

If K field, units in $K[t]$ are non-zero constants, and $f \in K[t]$ **irreducible** $\iff f$ non-constant & f isn't product of 2 non-constant polynomials.

If $f \in K[t]$ unit, $\deg(ff^{-1}) = \deg(1_K) \therefore \deg(f) + \deg(f^{-1}) = 0 \therefore \deg(f) = 0 \therefore f$ is constant & $f \in K$ has inverse if $f \neq 0_K$.

Polynomial Remainders (Proposition 3.2.1)

Let K field, $f, g \neq 0_K \in K[t]$. $\exists! q, r \in K[t] : f = gq + r$ & $\deg(r) < \deg(g)$.

Polynomials Over Fields as PIDs (Proposition 3.2.2)

If K is a field, then $K[t]$ is a PID.

K is ID by (3.1.11). Let $I \triangleleft K[t]$. If $I = \{0_K\}$ then $I = \langle 0_K \rangle$. Else, let $d = \min\{deg(f) \mid 0_K \neq f \in I\}$ and $g \in I : deg(g) = d$. Claim: $I = \langle g \rangle \iff$ $\forall f \in I$, $g | f$. By (3.2.1) $\exists! q, r \in K[t] : f = gq + r$, $deg(r) < deg(g) = d$. $q \in K[t] \therefore$ $gq \in I \therefore r = f - gq \in I$ g has minimal degree & $deg(r) < d \therefore r = 0 \therefore f = gq \therefore g | f$.

If K field, $K[t]$ PID, but $K[t_1, \ldots, t_n]$ is only ID & need not be PID (for example, $\langle t_1, t_2 \rangle$ not principal in $\mathbb{Q}[t_1, t_2]$). If K not a field in (3.2.2), then $\langle 2, t \rangle$ not principal in $\mathbb{Z}[t]$ (where $\mathbb{Z}$ is PID but not field). Note, $\langle 2, t \rangle = \{2f + tg | f, g \in \mathbb{Z}[t]\}$. If principal, $\exists h \in \mathbb{Z}[t] : \langle h \rangle = \langle 2, t \rangle \therefore \exists a, b \in \mathbb{Z}[t] : 2 = ha, t = hb \therefore \deg(h) + \deg(a) = 0 \therefore h \neq 0 \in \mathbb{Z}$. $t = hb \therefore h = \pm 1 \therefore h$ is unit $\therefore \langle h \rangle = \mathbb{Z}[t]$. But $1 \notin \langle 2, t \rangle \therefore$ contradiction & not principal.

Factorising Polynomials

Non-Constant Polynomials Divisible by Irreducibles (Lemma 3.2.6)

Let K field, $f \in K[t]$ non-constant. f is divisible by irreducible in $K[t]$.

Irreducibles Divide Elements of Product (Lemma 3.2.7)

Let K field, $f, g, h \in K[t]$. If f irreducible & $f|gh$, then $f|g$ or $f|h$.

Polynomials Over Fields Factorise Uniquely (Theorem 3.2.8)

Let K field, $0_K \neq f \in K[t]$. Then $f = af_1 \dots f_n$, where $n \geq 0$, $a \in K$, $f_1, \dots, f_n \in K[t]$ monic irreducible. n, a uniquely determined by f; $f_1, \dots, f_n$ uniquely determined up to reordering.

Linear Factors and Roots (Lemma 3.2.9)

Let K field, $f \in K[t]$, $a \in K$. Then, $f(a) = 0_K \iff (t-a)|f$.

Factorisation in Algebraically Closed Fields (Lemma 3.2.10)

- K **algebraically closed** if every non-constant polynomial has at least 1 root in K
- if K algebraically closed, $0_K \neq f \in K[t]$, then $f(t) = c(t-a_1)^{m_1} \dots (t-a_k)^{m_k}$, where $a_1, \dots, a_k$ are distinct roots of f in K, $m_1, \dots, m_k \geq 1$.

Irreducibility in Polynomials

Fields from Irreducible Polynomials

Let K field, $0_K \neq f \in K[t]$. Then, f irreducible $\iff K[t]/\langle f \rangle$ is field.

Primitive Polynomials

$p \in \mathbb{Z}[t]$ is primitive if its coefficients have no common divisor, except ± 1.

From Primitives to Rational Polynomials (Lemma 3.3.7)

If $f \in \mathbb{Q}[t]$, $\exists F \in \mathbb{Z}[t], \alpha \in \mathbb{Q}$ (with F **primitive**) such that $f = \alpha F$.

Gauss's Lemma (Lemma 3.3.8)

1. Product of primitive polynomials over $\mathbb{Z}[t]$ is primitive
2. If non-constant $p \in \mathbb{Z}[t]$ irreducible over $\mathbb{Z}$, it is irreducible over $\mathbb{Q}$.

Irreducibility from Degree & Roots (Lemma 3.3.1)

Let K field, $f \in K[t]$. Then:

1. If f constant, then f not irreducible.
2. If $\deg(f) = 1$, f irreducible.
3. If $\deg(f) \geq 2$ & f has root, f reducible.
4. If $\deg(f) \in \{2, 3\}$ & f has no root, f irreducible.

- $f = \sum_{i=0}^{p-1} t^i$ reducible in $\mathbb{Z}_p[t]$, as $f(1) = 0$.
- $f = t^3 - 10 \in \mathbb{Q}[t]$ has no root in $\mathbb{Q}$ & $\deg(f) = 3 \therefore$ irreducible.
- over **algebraically closed** fields, the irreducibles are linear.

Mod-p Method (Proposition 3.3.9)

Let $f = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t]$. Define $\pi : \mathbb{Z} \to \mathbb{Z}_p$, $\pi_* : \mathbb{Z}[t] \to \mathbb{Z}_p[t]$, p prime. If $p \nmid a_n$ & $\bar{f} \in \mathbb{Z}_p[t]$ irreducible, then f irreducible over $\mathbb{Q}$.

- $f = 9 + 14t - 8t^3 \in \mathbb{Z}[t]$ reduces to $\bar{f} = 2 - t^3$ in $\mathbb{Z}_7$. No roots & cubic $\therefore$ irreducible in $\mathbb{Z}_7 \therefore$ irreducible in $\mathbb{Q}$.
- in $\mathbb{Z}_3$, $\bar{f} = t(t^2 - 1)$ is reducible, but this doesn't imply reducibility in $\mathbb{Q}$.
- condition $p \nmid a_n$ necessary: $f = 6t^2 + t$ reducible, but in $\mathbb{Z}_3$, $\bar{f} = t$ irreducible.

Eisenstein's Criterion (Proposition 3.3.12)

Let $f = \sum_{i=1}^{n} a_i t^i \in \mathbb{Z}[t], n \geq 1$. f irreducible over $\mathbb{Q}$ if $\exists p$ prime, such that:

1. $p \nmid a_n$ 2. $\forall i \in [0, n-1], p|a_i$ 3. $p^2 \nmid a_0$

- $g = \frac{2}{9}t^5 - \frac{5}{3}t^4 + t^3 + \frac{1}{3}$; by Gauss (3.3.8), g irreducible over $\mathbb{Q} \iff 9g$ irreducible over $\mathbb{Q}$; $9g$ irreducible by Eisenstein with $p = 3$.
- pth **cyclotomic polynomial** is $\Phi_p(t) = 1 + t + \dots + t^{p-1} = \frac{t^p - 1}{t-1}$. Can't apply Eisenstein on $\Phi_p(t)$ immediately; but $\Phi_p(t+1) = \frac{1}{t}\sum_{i=1}^{p} \binom{p}{i} t^i$, which is irreducible by Eisenstein with p.

Chapter 4

Field Extensions

Definition

- a field extension (FE) of **field** K is field M alongside homomorphism $\iota : K \to M$. Written $M : K$.
- $K(t)$ extends K with trivial homomorphism $\iota(a) = a/1$; $\mathbb{Q}$ trivially extends itself; $\mathbb{R}$ extends $\mathbb{Q}$, again through the inclusion homomorphism.

Generating Subfields

- let K field, $X \subseteq K$. The subfield of K **generated by** X is intersection of all K subfields containing X (smallest subfield containing X)
- if $M : K$ FE & $Y \subseteq M$, $K(Y)$ = subfield of M generated by $K \cup Y$ (subfield generated by Y over K, K with Y adjoined).
- $K(Y)$ is the smallest subfield containing K & Y
- subfield of K generated by $\emptyset$ is prime subfield; subfield of $\mathbb{C}$ generated by $\{i\}$ is $\mathbb{Q}(i)$, since $\mathbb{Q}$ is prime subfield.

Algebraic and Transcendental Elements

Definition

- let $M : K$ FE & $\alpha \in M$. α **algebraic over** K if $\exists 0_K \neq f \in K[t] : f(\alpha) = 0_K$. If no such f exists, α **transcendental**
- π, e transcendental/algebraic over $\mathbb{Q}/\mathbb{R}$; $e^{2\pi i/n}$ algebraic over $\mathbb{Q}$ (root of $f = t^n - 1$); $t \in K(t)$ transcendental over K, as $f(t) = 0_K \iff f = 0_K$.

The Minimal Polynomial

Definition (Lemma 4.2.6)

- if $M : K$ FE, **annihilating polynomial** (AP) of $\alpha \in M$ is $f \in K[t] : f(\alpha) = 0$.
- if $M : K$ FE & $\alpha \in M$, $\exists m \in K[t] : \langle m \rangle = \{$APs of α over $K\}$. m is **minimal polynomial** (MP) of α over K.
- if α transcendental over K, $m = 0_K$; if algebraic, m is unique & monic.

By Universal Property of Polynomial Rings (3.1.6), unique evaluation homomorphism $\theta : K[t] \to M$ evaluates at α, so $\ker(\theta) = \{$APs of α over $K\}$. By (3.2.2), $K[t]$ PID $\therefore$ $\exists m \in K[t] : \langle m \rangle = \ker(\theta)$. If α transcendental, $\ker(\theta) = \{0_K\}$, so $m = 0_K$. Else, multiply m by $0_k \neq k \in K$ & $\langle m \rangle$ doesn't change $\therefore$ assume monic. If $\langle \tilde{m} \rangle = \ker(\theta)$, $\tilde{m} = cm$, but $\tilde{m}, m$ monic $\therefore c = 1$.

Equivalent Conditions for Minimal Polynomial (Lemma 4.2.10)

Let $M : K$ FE, $\alpha \in M$ algebraic over K, $m \in K[t]$ monic. Equivalent:

1. m is MP of α over K
2. $(\alpha) = 0_K$ & $m|f$, $\forall$ APs $f \in K[t]$ of α.
3. $m(\alpha) = 0$ & $\deg(m) \leq \deg(f)$, $\forall$ APs $0_k \neq f \in K[t]$ of α
4. $m(\alpha) = 0$ & m irreducible over K.

Field Extensions from Polynomials (Lemma 4.3.1)

Let K field.

1. Let $m \in K[t]$ monic, irreducible, $\pi : K[t] \to K[t]/\langle m \rangle$ canonical homomorphism. Write $\pi(t) = \alpha \in K[t]/\langle m \rangle$. Then, m is MP of α over K, and $K[t]/\langle m \rangle \cong K(\alpha)$.
2. $t \in K(t)$ is transcendental over K, and $K(t)$ generated by t over K.

---

1. Let $M = K[t]/\langle m \rangle$. $\pi\left(\sum_i a_i t^i\right) = \sum a_i \alpha^i \therefore ker(\pi) = \langle m \rangle$ contains APs of α over K $\therefore m$ MP of α over K. If $L \leq M$ & L contains K, α, then contains every polynomial in α over $K \therefore M \leq L \therefore L = M \therefore M = K(\alpha)$.
2. t transcendental in $K(t)$. Let $L \leq K(t)$ contain K, t. If $f, g \in K[t]$ are in L, then $f/g \in L \therefore L = M \therefore M = K(t)$.

Homomorphisms Over Fields

Definition

- let K field with extensions $\iota_1 : K \to M_1, \iota_2 : K \to M_2$. Homomorphism $\varphi : M_1 \to M_2$ is **homomorphism over** K if $\forall a \in K, \varphi(\iota_1(a)) = \iota_2(a)$
- if ι_1, ι_2 inclusions, $\forall a \in K, \varphi(a) = a$

Homomorphisms Over Fields Defined by Subsets (Lemma 4.3.6)

Let $M_1 : K, M_2 : K$ FE, $\varphi, \psi : M_1 \to M_2$ homomorphisms over K. Let $Y \subseteq M_1$: $M_1 = K(Y)$. If $\forall a \in Y$ $\varphi(a) = \psi(a)$, then $\varphi = \psi$.

$\varphi = \psi$ on $K \cup Y \therefore K \cup Y \subseteq \{\varphi, \psi\}$. By (2.3.8), $\{\varphi, \psi\} \leq M$ containing $K \cup Y$; $K(Y)$ smallest such subfield $\therefore \{\varphi, \psi\} = K(Y) = M$.

Universal Properties of $K[t]/\langle m \rangle, K(t)$ (Proposition 4.3.7)

Let K field.

1. Let $m \in K[t]$ monic, irreducible, $L : K$ FE, $\beta \in L$ with MP $m \in K[t]$, $\alpha = \pi(t)$. $\exists!$ homomorphism $\varphi : K[t]/\langle m \rangle \to L$ over K, such that $\varphi(\alpha) = \beta$.
2. $L : K$ FE, $\beta \in L$ transcendental. $\exists!$ homomorphism $\varphi : K(t) \to L$ over K such that $\varphi(t) = \beta$.

---

1. There is at least 1 homomorphism $\varphi : K[t]/\langle m \rangle \to L$ over K with $\varphi(\alpha) = \beta$. By (3.1.6), $\exists!$ homomorphism $\theta : K[t] \to L$ with $\forall a \in K, \theta(a) = a$ & $\theta(t) = \beta$). Then, $\theta(m(t)) = \theta(m(\beta)) = 0 \therefore \langle m \rangle \subseteq \ker(\theta) \therefore$ by Universal Property of Quotient Rings, $\exists!$ homomorphism $\varphi : K[t]/\langle m \rangle \to L$ with $\theta = \varphi \circ \pi$. φ is homomorphism over K, since $\forall a \in K, \varphi(a) = \varphi(\pi(a)) = \theta(a) = a$. Moreover, $\varphi(a) = \varphi(\pi(t)) = \theta(t) = \beta$. There is at most 1 homomorphism as the one described. Assume there are 2 such homomorphisms $\varphi\varphi'$. Then, $\varphi\alpha) = \varphi'(\alpha)$. By (4.3.1, i), $K(\alpha) = K[t]/\langle m \rangle$, so $\varphi = \varphi'$ by (4.3.6).
2. There is at least one homomorphism $\varphi : K(t) \to L$ over K with $\varphi(t) = \beta$. Elements in $K(t)$ are of form f/g where $f, g \in K[t], g \neq 0_K$. β transcendental over $K \therefore g(\beta) \neq 0_K \therefore$ $f(\beta)/g(\beta) \in L$ well defined. This defines homomorphism $\varphi : K(t) \to L, f/g \mapsto f(\beta)/g(\beta)$. φ homomorphism over K & $\varphi(t) = \beta$ as required. At most one such φ similar to 1) above.

Isomorphisms Over Fields

Definition

$M_1 : K, M_2 : K$ FE. $\varphi : M_1 \to M_2$ is **isomorphism over** K if its homomorphism over K & isomorphism. M_1, M_2 can be isomorphic, but not isomorphic over K.

Corollary to Universal Property (Corollary 4.3.11)

Let K field.

1. Let $m \in K[t]$ monic, irreducible, $L : K$ FE, $\beta \in L$ with MP $m \in K[t]$, $L = K(\beta)$, $\alpha = \pi(t)$. $\exists!$ isomorphism $\varphi : K[t]/\langle m \rangle \to L$ over K, st $\varphi(\alpha) = \beta$.
2. $L : K$ FE, $\beta \in L$ transcendental, $L = K(\beta)$. $\exists!$ isomorphism $\varphi : K(t) \to L$ over K st $\varphi(t) = \beta$.

---

1. (4.3.7,i) implies $\exists!$ homomorphism $\varphi : K[t]/\langle m \rangle \to L$ over K with $\varphi(\alpha) = \beta$. φ isomorphism if surjective (since φ homomorphism of fields $\therefore$ injective). By (2.3.6, i) $\text{im}(\varphi) \leq L$ & φ homomorphism over $K \therefore K \subseteq \text{im}(\varphi)$ & $\beta \in \text{im}(\varphi)$ (since $\varphi(\alpha) = \beta$) $\therefore$ $\text{im}(\varphi) = K(\beta) = L$
2. Similar to above.

Simple Field Extensions

Definition

- $M : K$ simple if $\exists \alpha \in M$ st $M = K(\alpha)$
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ simple: computing $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ shows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Classification of Simple Extensions (Theorem 4.3.16)

Let K **field**.

1. Let $m \in K[t]$ monic, irreducible. $\exists M : K, \exists \alpha \in M : M = K(\alpha)$ where α algebraic with MP m. If (M_1, α_1), (M_2, α_2) are 2 such pairs, $\exists!$ isomorphism $\varphi : M_1 \to M_2$ over K st $\varphi(\alpha_1) = \alpha_2$.
2. There exists FE $M : K$, $\alpha \in M$ transcendental st $M = K(\alpha)$ If (M_1, α_1), (M_2, α_2) are 2 such pairs, $\exists!$ isomorphism $\varphi : M_1 \to M_2$ over K st $\varphi(\alpha_1) = \alpha_2$.

Take $M = K[t]/\langle m \rangle, \alpha = \pi(t)$. By (4.3.1, i), α has MP $m \in K[t]$ & $M = K(\alpha)$ Lastly, use (4.3.11, i). For 2) use (4.3.1, ii), (4.3.11, ii).

Chapter 5

The Degree of an Extension

Definition

- Degree of $M : K$ is $[M : K]$: dimension of M as **vector space** over K.
- $M : K$ is **finite** if $[M : K] < \infty$. $\mathbb{C} : \mathbb{R}$ finite ($\{1, i\}$ basis); $K(t) : K$ infinite ($\{1, t, t^2, \dots\}$ infinite basis).

Extensions of Degree 1 (Example 5.1.3, i)

$[M : K] = 1 \iff M = K$

If $M = K$, $\{1_K\}$ basis. If $[M : K] = 1$, $\{1_K\}$ basis $\therefore m = 1_K \cdot k$.

Basis for Simple Extensions (Theorem 5.1.5)

Let $K(\alpha) : K$ simple FE.

1. Let $\alpha \in M$ algebraic with MP $m \in K[t]$, $n = \deg(m)$. $\{1, \alpha, \dots, \alpha^{n-1}\}$ basis for $K(\alpha) : K \therefore [K(\alpha) : K] = \deg(m)$.
2. Let $\alpha \in M$ transcendental over K. $\{1, \alpha, \dots\}$ LiD & $[K(\alpha) : K] = \infty$.

---

1. α algebraic $\therefore 1, \alpha, \dots, \alpha^{n-1}$ LiD (else $\deg(m) < n$). By (4,3,1,i) & (4.3.16, i), $K(\alpha) = K[t]/\langle m \rangle, \alpha = \pi(t)$. π surjective $\therefore \forall x \in K(\alpha), \exists f \in K[t] : \pi(f) = x$. By (3.2.1), $\exists! q, r \in K[t] : f = qm + r$, $\deg(r) < n \therefore r$ unique polynomial st $f - r \in \langle m \rangle \therefore$ $\pi(f) = \pi(r)$. Then, unique a_i st $\pi(f) = \pi\left(\sum_{i=0}^{n-1} a_i t^i\right) = \sum_{i=0}^{n-1} a_i \alpha^i \therefore 1, \dots, \alpha^{n-1}$ is spanning set.
2. (4.3.16, ii) implies $K(\alpha) \cong K(t)$ over K & $K(t) : K$ infinite.

Field Extension with Cube Root of 2

$\sqrt[3]{2}$ has MP $t^3 - 2 \therefore [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \therefore \{1, 2^{1/3}, 2^{2/3}\}$ is a basis. This shows that $2^{2/3}$ can't be written as $\mathbb{Q}$-linear combination of $1, 2^{1/3}$.

Degree of Field Elements

Definition

Let $M : K$ FE, $\alpha \in M$ with MP $m \in K[t]$. $\deg_K(\alpha) = [K(\alpha) : K] = \deg(m)$

Degree of Algebraic Field Elements (Corollary 5.1.10)

Let $M : K$ FE, $\alpha \in M$. $\deg_K(\alpha) < \infty \iff \alpha$ **algebraic** over K.

Adjoining Elements to Chained Extensions (Corollary 5.1.12)

Let $M : L : K$ FE, $\beta \in M$. Then, $[L(\beta) : L] \leq [K(\beta) : K]$.

If β transcendental, $[K(\beta) : K] = \infty$ & follows. If β algebraic over K, let $m \in K[t]$ be MP. $L : K \therefore m$ AP of β over $L \therefore$ degree of MP p of β over L is at most $deg(m) \therefore$ $[L(\beta) : L] = deg(p) \leq deg(m) = [K(\beta) : K]$

Generating Field Elements from Algebraics (Corollary 5.1.14)

Let $M : K$ FE, $\alpha_1, \dots, \alpha_n \in M$ algebraic over K with $\deg_K(\alpha_i) = d_i$. Then: $\forall \alpha \in K(\alpha_1, \dots, \alpha_n), \exists c_{r_1, \dots, r_n} \in K : \alpha = \sum_{r_1, \dots, r_n} c_{r_1, \dots, r_n} \prod_{i=1}^{n} \alpha_i^{r_i}$ where: $r_i \in [0, d_i - 1]$.

Apply induction. Base Case: $K(\alpha) : K$. For inductive step, $\alpha \in K(\alpha_1, \dots, \alpha_n) \therefore$ $\alpha \in (K(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n) \therefore \alpha$ algebraic in simple extension and can use inductive hypothesis.

The Tower Law

Tower Law (Theorem 5.1.17)

Let $M : L : K$ FE.

1. If $(\alpha_i)_{i \in I}$ basis L over K, $(\beta_j)_{j \in J}$ basis M over L, then $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ basis of M over K.
2. $M : K$ finite $\iff M : L, L : K$ finite
3. $[M : K] = [M : L][L : K]$

Prove 1, then 2,3 follow. Let $(c_{ij})_{(i,j) \in I \times J} \subseteq K$ st $\sum_{i,j} c_{ij} \alpha_i \beta_j = 0$ where $\forall j \in J$, $\sum_i c_{ij} \alpha_i \in L$ (α_i basis of L over K). $(\beta_j)_{j \in J}$ is LiD over $L \therefore \sum_{i,j} c_{ij} \alpha_i \beta_j = 0 \iff$ $\sum_i c_{ij} \alpha_i = 0$. But $(\alpha_i)_{i \in I}$ LiD over $K \therefore \forall i \in I, \forall j \in J,\ c_{ij} = 0 \therefore$ $\sum_{i,j} c_{ij} \alpha_i \beta_j = 0 \iff c_{ij} = 0 \therefore (\alpha_i \beta_j)_{(i,j) \in I \times J}$ LiD over K. Let $e \in M$. $(\beta_j)_{j \in J}$ spans M over $L \therefore e = \sum_j d_j \beta_j$, $(d_j)_{j \in J} \subseteq L$. But $(\alpha_i)_{i \in I}$ spans L over K, so $\forall j \in J$, $d_j = \sum_i c_{ij} \alpha_i$, $(c_{ij})_{i \in I} \subseteq K$. Hence, $e = \sum_j \sum_i c_{ij} \alpha_i \beta_j$

Corollary I (Corollary 5.1.19)

Let $M : L_1 : L_2 : K$ FE. $[M : K] < \infty$, then $[L_1 : L_2] | [M : K]$.

Corollary II (Corollary 5.1.21)

Let $M : K$ FE, $\alpha_1, \dots, \alpha_n \in M$. Then, $K(\alpha_1, \dots, \alpha_n) : K] \leq [K(\alpha_1) : K] \dots [K(\alpha_n) : K]$.

Tower Law & (5.1.12) $\therefore [K(\alpha_1, \dots, \alpha_k) : K(\alpha_1, \dots, \alpha_{k-1})] \leq [K(\alpha_k) : K]$.

Finiteness Conditions in Extensions

Finitely Generated Field Extensions

$M : K$ finitely generated if $\exists Y \subseteq M : |Y| < \infty \wedge M = K(Y)$.

Algebraic Field Extensions

$M : K$ algebraic if $\forall \alpha \in M$, α algebraic over K.

Finite FE are Finitely Generated & Algebraic (Proposition 5.2.4)

Let $M : K$ FE. Then, the following are equivalent:

1. $M : K$ finite 2. $M : K$ **finitely generated** and **algebraic**
3. $\exists \{\alpha_1, \dots, \alpha_n\}$ of algebraic elements of M over K with $M = K(\alpha_1, \dots, \alpha_n)$

(1 ⇒ 2): $M : K$ finite, so has basis $\alpha_1, \dots, \alpha_n$. If $L \leq M, K \subseteq L$, L $K-$linear subspace $\therefore \alpha_1, \dots, \alpha_n \in L \Rightarrow$L = M$\therefore M$ only subfield with $K \cup \{\alpha_1, \dots, \alpha_n\} \therefore$ $M = K(\alpha_1, \dots, \alpha_n)$. Let $\alpha \in M$. $M : K$ finite & by Tower Law, $[M : K] = [M : K(\alpha)][K(\alpha) : K] \therefore [K(\alpha) : K]$ finite $\therefore$ by (5.1.10) α algebraic. **(2 ⇒ 3)**: immediate. **(3 ⇒ 1)**: let α_i algebraic over K with $M = K(\alpha_1, \dots, \alpha_n)$. By (5.1.21), $[M : K] \leq [K(\alpha_1) : K] \dots [K(\alpha_n) : K]$. α_i algebraic $\therefore [K(\alpha_i) : K] < \infty \therefore [M : K] < \infty$.

Finite, Simple Extensions are Algebraic (Corollary 5.2.6)

Let $K(\alpha) : K$ be a **simple extension**. The following are equivalent:

1. $[K(\alpha) : K] < \infty$ 2. $K(\alpha) : K$ algebraic 3. α algebraic over K

Set of Algebraics is Subfield (Proposition 5.2.7)

The set $\overline{\mathbb{Q}}$ of algebraic numbers over $\mathbb{Q}$ is a subfield of $\mathbb{C}$.

By (5.2.6), if $\mathbb{Q}(\alpha) : \mathbb{Q}$ finite, then algebraic $\therefore \overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} | [\mathbb{Q}(\alpha) : \mathbb{Q} < \infty\}$. Let $\alpha, \beta \in \overline{\mathbb{Q}}$: by (5.1.21), $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] < \infty \therefore \mathbb{Q}(\alpha, \beta)$ finite. $\alpha - \beta \in \mathbb{Q}(\alpha, \beta) \therefore$ $[\mathbb{Q}(\alpha - \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < \infty \therefore \mathbb{Q}(\alpha - \beta) : \mathbb{Q}$ finite, simple field extension $\therefore$ by (5.2.6), $\alpha - \beta$ algebraic. By same argument, $0, 1, \alpha\beta \in \overline{\mathbb{Q}} \therefore \overline{\mathbb{Q}}$ subring of $\mathbb{C}$. $\mathbb{Q}(\alpha)$ is a field $\therefore$ $[\mathbb{Q}(1/\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty \therefore 1/\alpha$ algebraic. Hence, $\overline{Q}$ subring & each α unit $\therefore$ subfield.

Ruler and Compass Constructions

Constructible Points

- let Σ subset of plane. A point is **immediately constructible** from Σ if its point of intersection between 2 lines/2 circles/line & circle
- $C \in \Sigma$ is **constructible** if $\exists C_1, \dots, C_n = C$, st C_i immediately constructible from $\Sigma \cup \{C_1, \dots, C_{i-1}\}$

Iterated Quadratics and Compositums

Iterated Quadratic Extensions

- let $K \leq \mathbb{R}$ subfield. $K : \mathbb{Q}$ **iterated quadratic** if $\exists$ finite subfield sequence $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = k$ st $\forall i \in [|, n], [K_i : K_{i-1}] = 2$.
- for example, $\mathbb{Q}\left(\sqrt{\sqrt{2} + \sqrt{3}}\right) : \mathbb{Q}$ is **iterated quadratic**:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}\left(\sqrt{\sqrt{2} + \sqrt{3}}\right)$$

Compositum of Fields

Let L_1, L_2 subfields of M. The **compositum** $L_1 L_2 = L_1(L_2) = L_2(L_1)$ is **subfield** of M, generated by $L_1 \cup L_2$.

Degree of Compositum (Lemma 5.3.6)

Let $M : K$ FE, L_1, L_2 subfields of M containing K. Then, if $[L_1 : K] = 2$, then $[L_1 L_2 : L_2] \in \{1, 2\}$. Generally, $[L_1 L_2 : L_2] \leq [L_1 : K]$.

Prove general case. If $[L_1 : K]$ infinite, inequality trivial. Else, $[L_1 : K]$ finite $\therefore$ by (5.2.4), $\exists \beta_1, \dots, \beta_n \in L_1$ spanning L_1 over K & algebraic, so that $L_1 = K(\beta_1, \dots, \beta_n)$. Firstly, assume $\exists \beta \in L_1 \setminus K : L_1 = K(\beta)$. $L_1 L_2$ smallest subfield of M containing L_1, L_2 & L_1 smallest subfield of M containing $K, \beta \therefore L_1 L_2$ smallest subfield of M containing L_2, K, β. $K \subseteq L_2 \therefore L_1 L_2$ smallest subfield containing $L_2, \beta \therefore$ $L_1 L_2 = L_2(\beta)$. By (5.1.12), $[L_2(\beta) : L_2] \leq [K(\beta) : K] \therefore [L_1 L_2 : L_2] \leq [L_1 : K]$. Now, assume that $L_1 = K(\beta_1, \dots, \beta_n)$, β_i algebraic. Similar argument to above shows $L_1 L_2 = L_1(\beta_1, \dots, \beta_n)$. By Tower Law, $[L_1 L_2 : L_2] = \prod_{j=1}^{n} [L_2(\beta_1, \dots, \beta_j) : L_2(\beta_1, \dots, \beta_{j-1})]$. By (5.1.12), $[L_1 L_2 : L_2] \leq \prod_{j=1}^{n} [K(\beta_1, \dots, \beta_j) : K(\beta_1, \dots, \beta_{j-1})]]$. By Tower Law, $[L_1 L_2 : L_2] \leq [L_1 : K]$.

Generating iterated Quadratic Subfields (Lemma 5.3.8)
Let K, L subfields of $\mathbb{R}$, such that $K:\mathbb{Q}, L:\mathbb{Q}$ **iterated quadratic**. Exists subfield M of $\mathbb{R}$ st $M:\mathbb{Q}$ iterated quadratic & $K, L \subseteq M$.

$\exists K_i, L_i$ st $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n = K \subseteq \mathbb{R}$,
$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_m = K \subseteq \mathbb{R}$ where $\forall i,j,\ [K_i : K_{i-1}] = 2 = [L_j : L_{j-1}]$
Consider chain of subfields of $\mathbb{R}$:
$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K = KL_0 \subseteq KL_1 \subseteq \ldots \subseteq KL_m = KL$ Claim: $M = KL$ is iterated quadratic extension of $\mathbb{Q}$ ($K, L \subseteq KL$ clearly). L_j, KL_{j-1} subfields of $\mathbb{R}$ containing L_{j-1}. By (5.3.6), $[L_j : L_{j-1}] = 2 \therefore$
$[KL_j : KL_{j-1}] = [L_j(KL_{j-1}) : KL_{j-1}] \in \{1,2\}$ Successive degrees in subfield chain are 1 or 2. If degree 1, equality $\therefore$ ignore. Thus, $KL:\mathbb{Q}$ iterated quadratic extension containing K, L.

Iterated Quadratic Extensions Contain Constructible Points (Proposition 5.3.9)
Let $(x,y) \in \mathbb{R}^2$. If (x,y) constructible from $\Sigma = \{(0,0),(1,0)\}$ then $\exists$ iterated quadratic extension of $\mathbb{Q}$ containing both x, y.

Induction on steps n to construct (x,y). If $n = 0$, $(x,y) \in \Sigma \therefore x, y \in \mathbb{Q}$ (iterated quadratic over itself). Suppose (x,y) constructible in $\leq k$ steps lie in iterated quadratic extension of $\mathbb{Q}$. Let (x,y) constructible in $k+1$ steps from Σ. (x,y) intersection of lines/circles through points constructible in $\leq k$ steps $\therefore$ by inductive hypothesis, intermediate points lie in iterated quadratic extension $\therefore$ by (5.3.8) there is iterated quadratic extension L of $\mathbb{Q}$ containing all intermediate points. If x, y satisfy line equation: $ax + by + c = 0$; if satisfy circle equation: $x^2 + y^2 + dx + ey + f = 0$. If x, y intersection of 2 lines, x satisfies linear equation $\therefore x \in L \therefore \deg_L(x) = 1$. If x, y intersection of line & circle, x satisfies linear or quadratic over L, so $\deg_L(x) \in \{1,2\}$. If x, y intersection of 2 circles, reduces to case of line, circle intersection, so $\deg_L(x) \in \{1,2\}$. Hence, $[L(x) : L] \in \{1,2\} \therefore$ either L or $L(x)$ iterated quadratic extension of $\mathbb{Q}$ containing x. Same applies to y. Combining these with (5.3.8) yields iterated quadratic extension containing x, y.

Constructible, Algebraic Points Have Power of 2 Degree (Theorem 5.3.10)
Let $(x,y) \in \mathbb{R}^2$. If (x,y) constructible from $\Sigma = \{(0,0),(1,0)\}$ then:
1. x, y algebraic over $\mathbb{Q}$ 2. their degrees over $\mathbb{Q}$ are powers of 2

By (5.3.9), $\exists$ iterated quadratic extension M of $\mathbb{Q}$ with $x \in M$. By Tower Law:
$\exists n \geq 0 : [M : \mathbb{Q}] = 2^n$. Again by Tower Law: $[M:\mathbb{Q}] = [M:\mathbb{Q}(x)][\mathbb{Q}(x):\mathbb{Q}] \therefore$
$[\mathbb{Q}(x):\mathbb{Q}] \mid 2^n \therefore \deg_{\mathbb{Q}}(x) < \infty$ (so x algebraic), and power of 2.

The Problems Which Stumped the Greeks

Can't Trisect Angles by Ruler & Compass (Proposition 5.3.11)
If possible, construct triangle with vertices at $(0,0)$ & $(1,0)$. Trisect angle at $(0,0)$. Let (x,y) be intersection of trisector & circle (centre $(0,0)$, radius 1). Then, $x = \cos(\pi/9)$. But MP x is $t^3 - \frac{3}{4}t - \frac{1}{6}$ (use DeMoivre for identity of $\cos(3x)$ & Mod-p method with $p = 5$), so $\deg_{\mathbb{Q}}(\cos(\pi/9)) = 3$, but if x constructible, degree power of 2 by (5.3.10).

Can't Duplicate Cube by Ruler and Compass (Proposition 5.3.12)
If possible, if A, B distance 1 apart, can construct A', B' distance $\sqrt[3]{2}$ apart $\therefore (\sqrt[3]{2}, 0)$ constructible. MP of $\sqrt[3]{2}$ is $t^3 - 2 \therefore$ not power of 2, so can't be constructible by (5.3.10).

Can't Square Circle by Ruler and Compass (Proposition 5.3.13)
If true, given circle of radius 1 with centre $(0,0)$ (with area π), construct square with side length $\sqrt{\pi} \therefore (\sqrt{\pi}, 0)$ constructible. By (5.3.10), $\sqrt{\pi}$ algebraic over $\mathbb{Q} \therefore \pi$ algebraic over $\mathbb{Q}$ ($\overline{\mathbb{Q}}$ subfield), but it's transcendental.

Fermat Primes
A regular n-polygon is constructible $\iff n = 2^r p_1 \ldots p_k$ where $r, k \geq 0$ & p_i is a **Fermat Prime** ($p_i = 2^u + 1$; 3,5,17,257,65537, ...).

Chapter 6

Homomorphism Extensions

Definition
- let $\iota_1 : K_1 \to M_1, \iota : K_2 \to M_2$ FE, $\psi : K_2 \to K_2$ field homomomorphism. $\varphi : M_1 \to M_2$ extends ψ if $\varphi \circ \iota_1 = \iota_2 \circ \psi$. If ι_1, ι_2 inclusions, φ extends ψ if $\forall a \in K_1$, $\varphi(a) = \psi(a)$.
- if $M_1 : K, M_2 : K$ & $\varphi : M_1 \to M_2$ extends id_K, φ is homomorphism over K

Homomorphism Extensions Preserve Roots (Lemma 6.1.3)
Let $M_1 : K_1, M_2 : K_2$ FE, $\psi : K_1 \to K_2$ homomorphism, $\varphi : M_1 \to M_2$ homomorphism extending ψ, $\psi_* : K_1[t] \to K_2[t]$ induced homomorphism. Let $\alpha \in M_1, f \in K_1[t]$. Then, $f(\alpha) = 0_{K_1} \iff (\psi_* f)(\varphi(\alpha)) = 0_{K_2}$

$f = \sum_i a_i t^i \therefore \psi_* f = \sum_i \psi(a_i) t^i \therefore (\psi_* f)(\varphi(\alpha)) = \sum_i \psi(a_i)\varphi(\alpha)^i = \sum_i \varphi(a_i)\varphi(\alpha)^i$ $= \varphi(f(\alpha))$, using that φ equal to ψ on K_1. φ field homomorphism $\therefore$ injective by (2.3.3), so $f(\alpha) = 0 \iff \varphi(f(\alpha)) = 0$.

Homomorphisms Over Fields Preserve APs (Example 6.1.4)
Let $M_1 : K, M_2 : K$ FE, $\varphi : M_1 \to M_2$ homomorphism over K. AP of $\alpha \in M_1$ same as $\varphi(\alpha) \in M_2$.

Apply (6.1.3) with $\psi = \mathrm{id}_K$, then $f(\alpha) = 0_K \iff f(\varphi(\alpha)) = 0_K$.

Isomorphism Extensions Over Simple Fields (Proposition 6.1.6)
Let $\psi : K_1 \to K_2$ field isomorphism, $K_1(\alpha_1) : K_1$ simple extension (α_1 with MP $m \in K_1[t]$), $K_2(\alpha_2) : K_2$ simple extension (α_2 with MP $\psi_* m \in K_2[t]$). Then, $\exists!$ isomorphism $\varphi : K_1(\alpha_1) \to K_2(\alpha_2)$ extending ψ & $\varphi(\alpha_1) = \alpha_2$.

View $K_2(\alpha_2)$ as FE of K_1: $K_1 \mapsto K_2 \mapsto K_2(\alpha_2) \therefore$ MP of α_2 over K_1 is m. By (4.3.16), $\exists!$ isomorphism $\varphi : K_1(\alpha_1) \to K_2(\alpha_2)$ over K_1 with $\varphi(\alpha_1) = \alpha_2$.

Splitting Fields of Polynomials

Definition
- $f \in M[t]$ **splits** in M if irreducible factors linear: $f = \beta(t - \alpha_1)\ldots(t - \alpha_n)$ with $n \geq 0, \beta, \alpha_i \in M$.
- **splitting field** of $0_K \neq f \in K[t]$ is extension $M : K$ st:

1. f splits in M 2. $M = K(\alpha_1, \ldots \alpha_n)$, α_i roots of f in M

Bounding Degree of Splitting Field (Theorem 6.2.10)
Let $0_K \neq f \in K[t]$. $\exists$ splitting field M of f over K st $[M:K] \leq \deg(f)!$.

Induction on $deg(f) = n$. If $\deg(f) = 0$, $f \in K$ so $M = K$ is SF (irreducible factors linear), so $[M:K] = 1 \leq 0!$. Assume $\deg(f) \leq k!$, then $[M:K] \leq k!$. Let $f \in K[t]$ with $\deg(f) = k+1$. Let $m \in K[t]$ irreducible factor of f. By (4.3.16), $\exists K(\alpha) : K$ where $m(\alpha) = 0$. In $K(\alpha)[t]$, $t - \alpha | f \therefore$ let $g = f/(t-\alpha) \in K(\alpha)[t]$. $\deg(g) = k < k+1 \therefore$ by inductive hypothesis, $M : K(\alpha)$ is SF of g & $[M : K(\alpha)] \leq k!$. Since $\alpha \in M$ & g splits in M, $f = (t-\alpha)g$ splits over M. By Tower Law,
$[M:K] = [M:K(\alpha)][K(\alpha):K] \leq k! \deg(m) \leq (k+1)!$.

Isomorphisms Between Splitting Fields (Proposition 6.2.11)
Let $\psi : K_1 \to K_2$ field isomorphism, $0_{K_1} \neq f \in K_1[t]$, M_1 a SF of f over K_1, M_2 a SF of $\psi_* f$ over K_2. Then, there are at most $[M:K]$ isomorphisms $\varphi : M_1 \to M_2$ extending ψ.

Uniqueness of Splitting Fields (Theorem 6.2.13)
Let $0_K \neq f \in K[t]$, K field. Then:
1. there exists a SF of f over K 2. any 2 SFs of f are **isomorphic** over K 3. if M SF of f over K, # automorphisms of M over $K \leq [M:K] \leq \deg(f)!$

1. (6.2.10) 2. (6.2.11) with $K_1 = K_2, \psi = \mathrm{id}_K$ 3. (6.2.11) & (6.2.10)

We denote **the** splitting field of f over K with $SF_K(f)$.

Splitting Fields from Subsets (Lemma 6.2.14)
1. Let $M : S : K$ FE, $0_K \neq f \in K[t]$, $Y \subseteq M$. If $S = SF_K(f)$, then $S(Y) = SF_{K(Y)}(f)$.
2. Let $0_K \neq f \in K[t]$, L subfield $SF_K(f)$ with $K \subseteq K$ (so $SF_K(f) : L : K$). Then, $SF_K(f) = SF_L(f)$.

1. f splits in $S \therefore$ splits in $S(Y)$. If X roots of f, $S = K(X) \therefore$
$S(Y) = K(X)(Y) = K(X \cup Y) = K(Y)(X) = SF_{K(Y)}(f)$.
2. By 1., $S(L) = S$ is SF of f over $K(L) = L$, so $SF_K(f) = SF_L(f)$.

The Galois Group

Galois Group of Field Extension
- let $M : K$ FE. The **Galois Group** of $M : K$, $Gal(M:K)$, is the **group of automorphisms** of M over K (composition as group operation).
- if $\theta \in Gal(M:K)$, then $\theta : M \to M$ automorphism & $\forall a \in K, \theta(a) = a$.

Galois Group of Polynomial
- let $0_K \neq f \in K[t]$. The **Galois Group** of f over K is $Gal_K(f) = Gal(SF_K(f) : K)$.
- by (6.2.13), $|Gal_K(f)| \leq [SF_K(f) : K] \leq \deg(f)!$ so $Gal_K(f)$ always finite.

Action of the Galois Group

Galois Group Restricts to Action on Roots (Lemma 6.3.7)
Let $0_K \neq f \in K[t]$, K field. The action of $Gal_K(f)$ on $SF_K(f)$ restricts to action on the set of roots of f in $SF_K(f)$ (if $X \subseteq SF_K(f)$ set of roots,
$\forall g \in Gal_K(f), \forall x \in X, gx = g(x) \in X$).

Let $\theta \in Gal_K(f)$. By (6.1.4), if $\alpha \in SF_K(f)$ root, $\theta(\alpha) \in SF_K(f)$ also root.

Galois Group Acts Faithfully (Lemma 6.3.8)
Let $0_K \neq f \in K[t]$, K field. Action of $Gal_K f)$ on roots of f is faithful.

Let $X \subseteq SF_K(f)$ be roots of f, $\theta \in Gal_K(f)$. Then, $SF_K(f) = K(X)$. If $\forall x \in X, \theta(x) = x$, by (4.3.6), $\theta = \mathrm{id}_K$, so θ faithful.

In other words, elements in $Gal_K(f)$ completely determined by how they permute roots of f. If roots $\alpha_1, \ldots, \alpha_k$, for each $\theta \in Gal_K(f)$, there is $\sigma_\theta \in S_k$ defined by $\theta(\alpha_i) = \alpha_{\sigma_\theta(i)}$. $\theta \mapsto \sigma_\theta$ is isomorphism & $Gal_K(f) \cong \{\sigma_\theta | \theta \in Gal_K(f)\} \leq S_k$.

Galois Group Isomorphic to Subgroup of S_k

Conjugacy Over Field Extensions
Let $M : K$ FE. Consider k-tuples of elements of M: $k \geq 0$, $(\alpha_1, \ldots, \alpha_k)$, $(\alpha'_1, \ldots, \alpha'_k)$
These tuples are **conjugate over** K if $\forall p \in K[t_1, \ldots, t_k]$ $p(\alpha_1, \ldots, \alpha_k) = 0 \iff p(\alpha'_1, \ldots, \alpha'_k)$.

Equivalence of Galois Group Definitions (Proposition 6.3.10)
Let $0_K \neq f \in K[t]$, K field., with k **distinct roots** $\alpha_1, \ldots, \alpha_k \in SF_K(f)$ Then:
$\{\sigma \mid \sigma \in S_k,\ (\alpha_1, \ldots, \alpha_k)\ and\ (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)})$ are conjugate over $K\} \leq S_k$ is isomorphic to $Gal_K(f)$.

Galois Subgroups from Extensions (Corollary 6.3.12)
Let $L : K$ FE and $0 \neq f \in K[t]$. $Gal_L(f)$ isomorphic to subgroup of $Gal_K(f)$.

$K \subseteq L \therefore$ if tuples conjugate over L, conjugate over $K \therefore Gal_L(f) \subseteq Gal_K(f)$. Gal isomorphic to subgroup of $S_k \therefore Gal_L(f) \leq Gal_K(f)$.

Order of Galois Group Divides $k!$ (Corollary 6.3.14)
Let $0_K \neq f \in K[t]$ have k distinct roots in $SF_K(f)$. $Gal_K(f)$ isomorphic to subgroup of S_k, so by Lagrange's Theorem, $|Gal_K(f)| | k!$.

Chapter 7

Normal Field Extension

Definition
- **algebraic** FE $M : K$ is **normal** if $\forall \alpha \in M$, MP of α splits in M.
- all SFs are normal; $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ prototypical example of non-normality: $t^3 - 2$ doesn't split, since $i \notin \mathbb{Q}(\sqrt[3]{2})$.

Normality from Irreducible Polynomials (Lemma 7.1.2)
Let $M : K$ algebraic FE. $M : K$ normal $\iff$ every irreducible $f \in K[t]$ either has no roots in M or splits in M.

($\Longrightarrow$): let $f \in K[t]$ irreducible with root $\alpha \in M$. f is irreducible $\therefore$ MP of α is f/c ($c \in K$ lead coefficient of f). $M : K$ normal $\therefore f/c$ splits in $M \therefore f$ splits too. ($\Longleftarrow$): let $\alpha \in M$. $M : K$ is algebraic $\therefore \alpha$ has MP $f \in K[t]$. f irreducible & has at least one root in M $(\alpha) \therefore f$ splits in $M \therefore M : K$ normal.

Extensions of Degree 2 (Workshop 4, Q4)
Every extension of degree 2 is normal.

If $[M:K] = 2$, $M : K$ finite $\therefore$ algebraic. Let $\alpha \in M$. By Tower Law, either $M = K(\alpha)$ or $K(\alpha) = K$. If $K(\alpha) = K$, $\alpha \in K \therefore t - \alpha$ is MP, which splits in M. If $K(\alpha) = M$, α has quadratic MP $m \in K[t]$. Since $m(\alpha) = 0$, $m = (t - \alpha)g$, with $g \in M[t]$ & $\deg(g) = 1 \therefore m$ splits in M.

Normality and Splitting Fields (Theorem 7.1.5)
Let $M : K$ FE. Then, if $0_K \neq f \in K[t]$, $M = SF_K(f) \iff M : K$ finite & normal.

($\Longleftarrow$): $M : K$ finite $\therefore$ by (5.2.4) $\exists$ basis of algebraics $\alpha_1, \ldots, \alpha_n$ of M over K with $M = K(\alpha_1, \ldots, \alpha_n)$. Let $m_i \in K[t]$ MP of α_i. $M : K$ normal $\therefore m_i$ splits over $M \therefore$ $f = m_1 m_2 \ldots m_n \in K[t]$ also splits in M. Then, set of roots of f in M contains $\{\alpha_1, \ldots, \alpha_n\}$; since $M = K(\alpha_1, \ldots, \alpha_n)$, M generated by roots of f over $K \therefore$ $M = SF_K(f)$. ($\Longrightarrow$): let $f \in K[t] : M = SF_K(f)$. Firstly, M is finite. f splits over $M = SF_K(f)$; let $\alpha_1, \ldots, \alpha_n$ be roots of f in M. Then, $M = K(\alpha_1, \ldots, \alpha_n)$ & α_i algebraic $\therefore$ by 5.2.4, $M : K$ is finite. Let $\delta \in M$ have MP $m \in K[t]$. m splits in $SF_M(m)$. Claim: if $\varepsilon \in SF_M(m)$ root of m, then $\varepsilon \in M$ (which implies that any $f \in K[t]$ splits in M). m is MP of δ over $K \therefore$ monic, irreducible over K. It annihilates $\varepsilon \therefore$ MP of ε. By (4.3.16), $\exists!$ isomorphism over K $\theta : K(\delta) \to K(\varepsilon)$ with $\theta(\delta) = \varepsilon$. By (6.2.14, ii), $M = SF_K(f) : K$. $\therefore M = SF_K(f) = SF_{K(\delta)}(f)$. Moreover,
$SF_K(f) = K(\alpha_1, \ldots, \alpha_n) \therefore$ by (6.2.14, ii) with $Y = \{\varepsilon\} \subseteq M$,
$K(\alpha_1, \ldots, \alpha_n, \varepsilon) = SF_{K(\varepsilon)}(f)$. Lastly, θ homomorphism over K, and $f \in K[t] \therefore$
$\theta_* f = f$. Since θ isomorphism from $K(\delta)$ to $K(\varepsilon)$, $0_K \neq f \in K[t] \therefore 0_K \neq f \in K(\delta)[t]$, $M_1 = M = SF_{K(\delta)}(f)$, $M_2 = K(\alpha_1, \ldots, \alpha_n, \varepsilon) = SF_{K(\varepsilon)}(f) \therefore$ by (6.2.11), $\exists$ isomorphism $\varphi : M \to K(\alpha_1, \ldots, \alpha_n, \varepsilon)$ extending θ. Since θ isomorphism over K & φ extends θ, φ also isomorphism over K. Then, $\delta \in M = K(\alpha_1, \ldots, \alpha_n)$. Since φ isomorphism over K, $\varphi(\delta) \in K(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$. φ extends $\theta \therefore$
$\varphi(\delta) = \theta(\delta) = \varepsilon \Rightarrow \varepsilon \in K(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$. By (6.1.4), α_i has AP $f \therefore \varphi(\alpha_i)$ also has AP $f \therefore f(\varphi(\alpha_i)) = 0 \Rightarrow \varphi(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\} \therefore \varepsilon \in K(\alpha_1, \ldots, \alpha_n) = M \therefore$ any root ε of f is also in M, so $M : K$ normal.

Normality of Intermediate Fields (Corollary 7.1.6)
Let $M : L : K$ FE. If $M : K$ finite & normal, $M : L$ finite & normal.

$M : K$ finite & normal $\therefore$ by (7.1.5), $M = SF_K(f)$. By (6.2.14, ii), $SF_K(f) : L : K \therefore$ $SF_K(f) = SF_L(f) \therefore M : L$ finite & normal.

$L : K$ needn't be normal: if $\omega = e^{2\pi i/3}$, consider $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$:
$\mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq SF_{\mathbb{Q}}(t^3 - 2) \therefore$ normal, but $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ not normal.

Galois Action on Normal Extensions

Galois Maps Between Conjugates (Proposition 7.1.9)
Let $M : K$ finite, normal FE & $\alpha_1, \alpha_2 \in M$. Then α_1, α_2 conjugate over $K \iff$ $\exists \varphi \in Gal(M:K) : \alpha_2 = \varphi(\alpha_1)$.

($\Longleftarrow$): assume $\exists \varphi \in Gal(M:K) : \alpha_2 = \varphi(\alpha_1)$. φ automorphism over $K \therefore$ by Example 6.1.4 α_1 and $\varphi(\alpha_1) = \alpha_2$ have same AP $\therefore \alpha_1, \alpha_2$ conjugate over K. ($\Longrightarrow$): assume α_1, α_2 conjugate over K. $M : K$ finite & normal $\therefore$ algebraic $\therefore \alpha_1, \alpha_2$ algebraic over $K \therefore$ have same MP $m \in K[t] \therefore$ by (4.3.16) $\exists!$ isomorphism $\theta : K(\alpha_1) \to K(\alpha_2)$ over K with $\theta(\alpha_1) = \alpha_2$. $M : K$ finite & normal $\therefore$ by (7.1.5), it is SF of some $0_K \neq f \in K[t]$. By (6.2.14, ii), $M = SF_K(f)$ also SF of $K(\alpha_1)$, $K(\alpha_2)$. Moreover, θ homomorphism over $K \therefore$ $\theta_* f = f \therefore$ by (6.2.11, i) $\exists$ automorphism φ of M extending θ & θ isomorphism over $K \therefore$ so is φ. $\therefore \varphi$ automorphism of M over $K \therefore \varphi \in Gal(M:K)$ with $\varphi(\alpha_1) = \theta(\alpha_1) = \alpha_2$.

Galois Acts Transitively on Roots (Corollary 7.1.11)
Let $f \in K[t]$ irreducible. Action of $Gal_K(f)$ on roots of f is **transitive** (i.e generates a single orbit $\therefore \forall x_1, x_2 \in X, \exists \theta \in Gal_K(f) : \theta(x_1) = x_2$).

f irreducible $\therefore$ roots of f in $SF_K(f)$ have same MP $\therefore$ all conjugate over K. By (7.1.5), $SF_K(f)$ finite & normal $\therefore$ by (7.1.9) $Gal_K(f)$ maps between conjugates.

Using Transitivity of Galois Group
- if f pth cyclotomic polynomial, its roots are non-trivial roots of unity $\omega, \omega^2, \ldots, \omega^{p-1}$. By (7.1.11), $\exists \varphi \in Gal_{\mathbb{Q}}(f) : \varphi(\omega) = \omega^i$. In fact, this element is unique $\varphi = \varphi_i$, and $Gal_{\mathbb{Q}}(f) = \{\varphi_1, \ldots, \varphi_{p-1}\} \cong C_{p-1}$.
- let $G = Gal_{\mathbb{Q}}(t^3 - 2)$. G acts transitively on the 3 roots $\therefore |G| \geq 3$. G isomorphic to subgroup of $S_3 \therefore G \cong C_3 = A_3$ or $G \cong S_3$. Since 2 roots are complex conjugates, G contains element of order $2 \therefore G \cong S_3$.
- doesn't work if f not irreducible: for example, in $f = (t^2 - 2)(t^2 - 3)$, by conjucacy, $\sqrt{2}$ never gets mapped to $\sqrt{3}$, so $Gal_{\mathbb{Q}}(f)$ isn't transitive.

Normal Extensions & Normal Subgroups (Theorem 7.1.15)
Let $M : L : K$ FE with $M : K$ finite & normal. Then:
1. Let $\varphi L = \{\varphi(\alpha) \mid \alpha \in L\}$. Then, $L : K$ is normal extension $\iff$ $\forall \varphi \in Gal(M:K),\ \varphi L = L$
2. If $L : K$ normal, $Gal(M:L) \triangleleft Gal(M:K)$ & $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L:K)$

1. ($\Longrightarrow$): Let $\varphi \in Gal(M:K)$ & $L : K$ normal. $M : K$ finite $\therefore L : K$ finite & normal. $\forall \alpha \in L$, $\alpha, \varphi(\alpha)$ conjugate over K by (7.1.9) $\therefore$ same MP. By normality, MP splits in $L \therefore$ $\varphi(\alpha) \in L \therefore \varphi L \subseteq L$. Same argument with φ^{-1} show $\varphi^{-1} L \subseteq L \therefore L \subseteq \therefore = L$. ($\Longleftarrow$): if $= L$, let $\alpha \in L$ have MP $m \in K[t]$. $M : K$ normal $\therefore m$ splits in M. α conjugate to every other root α' of m over K. By (7.1.9), $\exists \varphi \in Gal(M:K) : \varphi(\alpha) = \alpha' \therefore \alpha' \in \varphi L = L \therefore$ m splits in $L \therefore L : K$ must be normal
2. Let $\varphi \in Gal(M:K)$, $\theta \in Gal(M:L)$. If $Gal(M:L) \triangleleft Gal(M:K)$ then $\varphi^{-1}\theta\varphi \in Gal(M:L)$. θ automorphism over $L \therefore$ equivalent to
$\forall \alpha \in L,\quad \varphi^{-1}\theta\varphi(\alpha) = \alpha \implies \theta\varphi(\alpha) = \varphi(\alpha)$. By 1), $L : K$ normal $\therefore \varphi L = L \therefore$ $\varphi(\alpha) \in L$. Since $\theta \in Gal(M:L)$, $\theta\varphi(\alpha) = \varphi(\alpha)$. For second part, we find $\nu : Gal(M:K) \to Gal(L:K)$ with $\ker(\nu) = Gal(M:L)$. $L : K$ normal $\therefore$ any $\varphi \in Gal(M:K)$ satisfies $\varphi L = L \therefore \varphi$ permutes $L \therefore$ restricts to automorphism $\hat{\varphi}$ of L. φ automorphism of M over $K \therefore \hat{\varphi}$ is automorphism of L over $K \therefore \hat{\varphi} \in Gal(L:K)$. Thus, define $\nu(\varphi) = \hat{\varphi}$. ν group homomorphism (preserves function composition). $\ker(\nu) =$ {automorphisms fixing L} $= Gal(M:L)$. Let ψ automorphism of L over K. ν surjective if $\exists \varphi$ automorphism of M over K st $\nu(\varphi) = \psi$. Equivalently, show that we can always extend ψ to φ. Since $M : K$ normal, it is SF of some $f \in K[t]$. By (6.2.14), M also SF of f over L. Also, $\psi_* f = f$, (ψ homomorphism over K, & $f \in K[t]$). By (6.2.11), $\exists$ automorphism φ of M which extends $\psi \therefore \nu$ surjective $\therefore$ by First Isomorphism Theorem $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L:K)$.

Separable Polynomials

Definition
Let $f \in K[t]$ irreducible, K field. f separable if it has no repeated roots in SF.
Equivalently: splits into distinct linear factors, or has $\deg(f)$ distinct roots.

Simplest Example of Non-Separable Polynomials (Example 7.2.4)
- let $K = \mathbb{F}_p(u)$. Then, $f(t) = t^p - u \in K[t]$ is inseparable.
- $\mathrm{char}(K) = p$ so by (2.3.22, i) u has at most 1 pth root. f has at least one root α in SF $\therefore$ α is unique root, but $\deg(f) = p > 1$. Alternatively, by Frobenius Map on $SF_K(f)$ (2.3.20, i), $f = t^p - u = t^p - \alpha^p = (t - \alpha)^p$.
- to see f irreducible, assume f has non-trivial factorisation $f = (t-\alpha)/t - \alpha)^{p-i}$.

Coefficient of t^{i-1} in $(t-\alpha)^i$ is $-i\alpha \therefore -i\alpha \in K \therefore \alpha \in K$. But by (3.1.13), u can't have pth root in $K = \mathbb{F}_p(u)$.

The Formal Derivative

Definition
- let K field and $f(t) = \sum_{i=0}^{n} a_i t^i \in K[t]$. The **formal derivative** of f is $(Df)(t) = \sum_{i=1}^{n} i a_i t^{i-1} \in K[t]$.
- satisfies expected rules: if $f, g \in K[t], a \in K$, then $D(f+g) = Df + Dg$, $D(fg) = f \cdot Dg + Df \cdot g$, $Da = 0_K$.

Repeated Roots from Formal Derivative (Lemma 7.2.9)
Let $0_K \neq f \in K[t]$, K field. The following are equivalent:
1. f has repeated root in $SF_K(f)$. 2. f, Df have common root in $SF_K(f)$.
3. f, Df have non-constant common factor in $K[t]$.

(1 ⇒ 2): $\alpha \in SF_K(f)$ repeated root $\therefore \exists g(t) \in SF_K(f)[t],\ :\ f(t) = (t-\alpha)^2 g(t) \therefore$ $Df = (t-\alpha)(2g + (t-\alpha) \cdot Dg) \therefore \alpha \in SF_K(f)$ common root between f and Df. **(2 ⇒ 3)**: $\alpha \in SF_K(f)$ common root of f, Df. α algebraic over K ($f \neq 0_K$) $\therefore$ let $g \in K[t]$ MP. g non-constant common factor between f, Df. **(3 ⇒ 2)**: let $g \in K[t]$ non-constant common factor of f, Df. g splits in $SF_K(f)$, $\therefore$ root of g in $SF_K(f)$ common root of f, Df. **(2 ⇒ 1)**: let $\alpha \in SF_K(f)$ common root f, Df. $\exists g \in SF_K(f)[t]$, with $f(t) = (t-\alpha)g(t) \therefore$ $Df = g + (t-\alpha) \cdot Dg$. α common root $\therefore (Df)(\alpha) = 0 \Rightarrow g(\alpha) = 0 \therefore \exists h \in SF_K(f)[t] :$ $g(t) = (t-\alpha)h(t) \therefore f(t) = (t-\alpha)^2 h(t) \therefore f$ has a repeated root in $SF_K(f)$.

Separability from Formal Derivative (Proposition 7.2.10)
Let $f \in K[t]$ irreducible, K field. f inseparable $\iff Df = 0_K$.

By (7.2.9), f inseparable $\iff$ f has repeated root $\iff$ f, Df have non-constant common factor. f irreducible $\therefore f|Df$. Since $\deg(Df) < \deg(f)$, $f|Df \iff Df = 0$.

Separability from Field Characteristic (Corollary 7.2.11)
Let K field. Then:
1.If $\text{char}(K) = 0$, every irreducible $f \in K[t]$ is separable..
2.If $\text{char}(K) = p > 0$, any irreducible $f \in K[t]$ is inseparable $\iff f(t) = \sum_{i=0}^{r} b_i t^{ip}$, where $b_0, \dots, b_r \in K$.

Let $f = \sum a_i t^i \in K[t]$ irreducible. f inseparable $\iff Df = 0$ (by 7.2.10) $\iff$ $\forall i \geq 1, ia_i = 0$. When $\text{char}(K) = 0$, only follows if $\forall i \geq 1, a_i = 0 \therefore f$ constant $\therefore f$ not irreducible. $\therefore$ if $\text{char}(K)$ & f irreducible, f can't be inseparable. If $\text{char}(K) = p$, $ia_i = 0$ whenever i divides p & for remaining cases, $a_i = 0 \therefore$ polynomials in t^p. are inseparable when $\text{char}(K) = p$.

In fact, irreducible polynomials over **finite fields** are separable; inseparability can only arise in infinite fields of prime characteristic.

Separable Extensions

Definition
- let $M : K$ algebraic. $\alpha \in M$ **separable** over K if its MP over K is separable.
- let $M : K$ algebraic. $M : K$ **separable** if every $\alpha \in M$ separable over K.
- any $M : K$ with $\text{char}(K) = 0$ is separable (7.2.11); any algebraic extension of finite fields is separable (by remark at end of (7.2.11).
- the SF of $t^p - u$ over $\mathbb{F}_p(u)$ inseparable, as the MP of α (root of u) is inseparable (since $t^p - u$ isn't separable).

Algebraicity of Intermediate Field (Exercise 7.2.15)
Let $M : L : K$ FE. If $M : K$ algebraic, $M : L$, $L : K$ algebraic.

If $M : K$ algebraic, $\alpha \in M$ has MP $f \in K[t]$. $L \subseteq M \therefore L : K$ algebraic. $K \subseteq L \therefore$ if α has AP $f \in K[t]$, then $f \in L[t]$ also annihilating, $\therefore M : L$ algebraic.

Separability of Intermediate Field (Lemma 7.2.16)
Let $M : L : K$ FE, $M : K$ algebraic. If $M : K$ separable, $M : L$, $L : K$ separable.

By (7.2.15), $M : L$, $L : K$ algebraic. Every $\alpha \in M$ separable over K & $L \subset M \therefore L : K$ separable. Let $\alpha \in M$ have MP m_L, m_K for L, K. m_K annihilates α over $L \therefore m_L | m_K$ in $L[t]$. $M : K$ separableV $\therefore m_K$ splits into distinct linear factors in $SF_K(m_K) \therefore$ so does $m_L \therefore m_L$ separable in $L[t] \therefore \alpha$ separable over $L \therefore L : K$ separable.

Isomorphisms Over Separable Extensions

Isomorphisms Between Separable Splitting Fields (Proposition 7.2.17)
Let $\psi : K_1 \to K_2$ field isomorphism, $0_{K_1} \neq f \in K_1[t]$, $M_1 = SF_{K_1}(f)$, $M_2 = SF_{K_2}(\psi_* f)$. If $M_2 : K_2$ separable, there are **exactly** $[M : K]$ isomorphisms $\varphi : M_1 \to M_2$ extending ψ.

Follows from (6.2.11), but in the proof separability means that there are precisely $\deg(\psi_* m)$ roots.

Order of Galois Group in Finite, Normal, Separable Extensions (Theorem 7.2.18)
For every finite, normal, separable FE $M : K$, $|Gal(M : K)| = [M : K]$.

$M : K$ finite & normal $\therefore$ by (7.1.5), $M = SF_K(f)$. Use (7.2.17) with $M_2 = M_1 = M$, $K_2 = K_1 = K$, $\psi = \text{id}_{K_1}$.

- if $\text{char}(K) = 0$, then $|Gal_K(f)| = [SF_K(f) : K]$
- separability is required: if $K = \mathbb{F}_p(u)$ & $M = SF_K(t^p - u)$, $M = K(\alpha) \therefore [M : K] = p$; but $|Gal(M : K)| = 1$, since i $Gal(M : K)$ isomorphic to subgroup of S_1.

The Fixed Field (Lemma 7.3.1)

Let $\text{Aut}(M)$ group of automorphisms of field M. If $S \subseteq \text{Aut}(M)$, $\text{Fix}(S)$ is subfield of M (known as the **fixed field of** S).

$\text{Fix}(S)$ is $(S \cup \{\text{id}_M\})$ & by (2.3.8), equaliser is subfield.

Bounding Extensions Over Fixed Fields (Theorem 7.3.3)

Let M field, $H \leq \text{Aut}(M)$, $|H| < \infty$. Then, $[M : \text{Fix}(H)] \leq |H|$.

Let $|H| = n$. If any $n+1$ elements of M are LD over $Fix(H)$, a LiD set has at most n elements $\therefore [M : Fix(H)] \leq |H|$. Define $W = \left\{(x_0, \dots, x_n) \in M^{n+1} \;\middle|\; \forall \theta \in H, \sum_{i=0}^{n} x_i \theta(\alpha_i) = 0_M\right\}$ where $\alpha_0, \dots, \alpha_n$ are $n+1$ arbitrary elements of M. W contains $n+1$-tuples in M^{n+1}. $|H| = n \therefore W$ is solutions to system of n homogeneous equations in $n+1$ variables $\therefore$ non-trivial M-linear subspace of M^{n+1}. Claim: if $(x_0, \dots, x_n) \in W$ and $\varphi \in H$, then $(\varphi(x_0), \dots, \varphi(x_n)) \in W$. Since $(x_0, \dots, x_n) \in W$ & $\varphi^{-1} \circ \theta \in H$, by definition of W, $\sum_{i=0}^{n} x_i(\varphi^{-1} \circ \theta)(\alpha_i) = 0$ Applying φ to both sides, for all $\theta \in H$ $\sum_{i=0}^{n} \varphi(x_i)\theta(\alpha_i) = 0$ $\therefore (\varphi(x_0), \dots, \varphi(x_n)) \in W$.

Now, let $\underline{x} = (x_0, \dots, x_n)$ be non-zero vector. Define its length as the unique $\ell \in [0, n]$ such that $x_\ell \neq 0$& $\forall j \in (\ell, n], x_j = 0$. W non-trivial subspace $\therefore$ there always exists an element of minimum length ℓ. W closed under scalar multiplication by elements of M $\therefore$ WLOG assume $x_\ell = 1$. Element of minimum length is of form $\underline{x} = (x_0, \dots, x_{\ell-1}, 1, 0, \dots, 0)$. $\underline{x}$ has minimal length $\therefore$ only element of W of the form $(y_0, \dots, y_{\ell-1}, 0, 0, \dots, 0)$ is $\underline{0}$. Claim: $\forall i \in [0, n], x_i \in Fix(H)$. Let $\varphi \in H \therefore$ $(x_0, \dots, x_n) \in W \Rightarrow (\varphi(x_0), \dots, \varphi(x_n)) \in W$. Define $\underline{y} = (\varphi(x_0) - x_0, \dots, \varphi(x_n) - x_n)$. By closure of subspaces $\underline{y} \in W$. φ field homomorphism $\therefore \forall i \in (\ell, n], x_i = 0 \implies \varphi(x_i) = 0$ & φ preserves the multiplicative identity $\therefore \varphi(x_\ell) = 1 \implies \varphi(x_\ell) - x_\ell = 0$. Hence, $\underline{y} = (\varphi(x_0) - x_0, \dots, \varphi(x_{\ell-1}) - x_{\ell-1}, 0, \dots, 0) \therefore \underline{y} = 0 \therefore$ $\forall i \in [0, n], \varphi(x_i) = x_i \implies x_i \in Fix(H)$. Overall, $\exists$ non-zero $\underline{x} \in Fix(H)^{n+1}$. Taking $\theta = id$ in definition of W, and using $\underline{x}$, we have found coefficients in $Fix(H)$, not all of which are 0, such that $\sum_{i=0}^{n} x_i \theta(\alpha_i) = \sum_{i=0}^{n} x_i \alpha_i = 0$. Hence, set of $n+1$ elements in M $\{\alpha_0, \dots, \alpha_n\}$ is LD over $Fix(H) \therefore [M : Fix(H)] \leq n = |H|$.

Fixed Fields as Normal Extensions (Proposition 7.3.7)

Let $M : K$ finite, normal FE & $H \triangleleft Gal(M : K)$. Then, $\text{Fix}(H)$ normal extension of K.

Every $\theta \in H$ automorphism over $K \therefore$ subfield $\text{Fix}(H) \leq M$ contains K. For any $\varphi \in Gal(M : K)$, by (2.1.15) $\varphi \,\text{Fix}(H) = \text{Fix}(\varphi H \varphi^{-1})$. Since $H \triangleleft Gal(M : K)$, $\text{Fix}(\varphi H \varphi^{-1}) = \text{Fix}(H) \therefore \varphi \,\text{Fix}(H) = \text{Fix}(H) \therefore$ by (7.1.15, i), $\text{Fix}(H) : K$ normal.

Chapter 8

The Galois Correspondence

Intermediate Fields and Galois Subgroups
- let $M : K$ be FE (view K as subfield). An **intermediate field** of $M : K$ is a subfield of M containing K. We write $\mathscr{F} = \{\text{intermediate fields of } M : K\}$.
- let $M : K$ be FE (view K as subfield). We write$\mathscr{G} = \{\text{subgroups of } Gal(M : K)\}$
- we can move from subgroups to fixed fields with $Fix : \mathscr{G} \to \mathscr{F}$ where $H \mapsto Fix(H)$ ($H \subseteq Gal(M : K) \therefore$ every element of H fixes $K \therefore K \subseteq \text{Fix}(H) \therefore \text{Fix}(H)$ intermediate field).
- we can move from fixed fields to subgroups with $Gal(M : -) : \mathscr{F} \to \mathscr{G}$ where $L \mapsto Gal(M : L)$ ($K \subseteq L \therefore$ if $\varphi \in Gal(M : L)$, φ fixes $K \therefore Gal(M : L) \leq Gal(M : K)$).

The Galois Correspondence
- the functions Fix, Gal are called the **Galois Correspondence** for $M : K$ if they are mutually inverse, so that $L = \text{Fix}(Gal(M : L))$ & $H = Gal(M : \text{Fix}(H))$
- correspondence sometimes fails: let $M : K$ be $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. $[M : K] = 3 \therefore$by Tower Law, no non-trivial intermediate fields, so $\mathscr{F} = \{M, K\}$. $G = Gal(M : K)$ trivial, so $\mathscr{G} = \{G\}$ $\therefore$ no 1-1 correspondence can exist. Indeed, $Fix(Gal(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})) = Fix(\{id_{\mathbb{Q}(\sqrt[3]{2})}\}) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.

Properties of Fix and Gal (Lemma 8.1.2)
Let $M : K$ FE. Then:
1.For $L_1, L_2 \in \mathscr{F}$, $L_1 \subseteq L_2 \Rightarrow Gal(M : L_2) \subseteq Gal(M : L_1)$. Similarly, for $H_1, H_2 \in \mathscr{G}$, $H_1 \subseteq H_2 \Rightarrow Fix(H_2) \subseteq Fix(H_1)$
2.For $L \in \mathscr{F}, H \in \mathscr{G}$, $L \subseteq Fix(H) \iff H \subseteq Gal(M : L)$
3.$\forall L \in \mathscr{F}$, $L \subseteq Fix(Gal(M : L))$. Similarly, $\forall H \in \mathscr{G}$, $H \subseteq Gal(M : Fix(H))$.

1.Let $L_1, L_2 \in \mathscr{F}$, $L_1 \subseteq L_2$. If $\varphi \in Gal(M : L_2)$, φ fixes $L_2 \therefore \varphi$ fixes $L_1 \therefore$ $Gal(M : L_2) \subseteq Gal(M : L_1)$. Similarly, let $H_1, H_2 \in \mathscr{G}$, $H_1 \subseteq H_2$. If $\alpha \in \text{Fix}(H_2)$, for any $\theta \in H_2$, $\theta(\alpha) =$. $H_1 \subseteq H_2 \therefore$ if $\theta \in H_2$, $\theta(\alpha) = \alpha \therefore \alpha \in \text{Fix}(H_1) \therefore$ $\text{Fix}(H_2) \subseteq \text{Fix}(H_1)$.
2.Both equivalent to $\forall \theta \in H, \forall \alpha \in L, \theta(\alpha) = \alpha$).
3.Follows from 2) with $H = Gal(M : L)$.

The Fundamental Theorem of Galois Theory (Theorem 8.2.1)

Let $M : K$ be a **finite, normal, separable** extension. Write $\mathscr{F} = \{\text{intermediate fields of } M : K\}$, $\mathscr{G} = \{\text{subgroups of } Gal(M : K)\}$
1.The functions:$Gal(M : -) : \mathscr{F} \to \mathscr{G}$, $Fix : \mathscr{G} \to \mathscr{F}$ are **mutually inverse**.
2.$\forall L \in \mathscr{F}, |Gal(M : L)| = [M : L]$ & $\forall H \in \mathscr{G}, [M : Fix(H)] = |H|$
3.Let $L \in \mathscr{F}$. Then, $L : K$ normal $\iff Gal(M : L) \triangleleft Gal(M : K)$. Moreover, in that case $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$.

Firstly, for $L \in \mathscr{F}$, $M : L$ is finite and normal (by (7.1.6)) and separable (by (7.2.16)). $Gal(M : K)$ finite group (by (7.2.18)), so any $H \in \mathscr{G}$ also finite. Prove 1 & 2 together. If $H \in \mathscr{G}$, then $|H| \leq |Gal(M : Fix(H))| = [M : Fix(H)] \leq |H|$. Where $|H| \leq |Gal(M : Fix(H))|$ (since $H \subseteq Gal(M : \text{Fix}(H))$ by (8.1.2, iii)), $|Gal(M : Fix(H))| = [M : Fix(H)]$ (by using (7.2.18), as $M : \text{Fix}(H)$ if finite, normal & separable) & $[M : Fix(H)] \leq |H|$ (by (7.3.3, since H finite). Thus, $H = Gal(M : \text{Fix}(H))$ & $[M : \text{Fix}(H)] = |H|$. Now, let $L \in \mathscr{F}$. Taking $H = Gal(M : L)$, the equality $|H| = [M : Fix(H)]$ above becomes $[M : Fix(Gal(M : L))] = |Gal(M : L)|$. By (7.2.18), $|Gal(M : L)| = [M : L]$. Overall, $[M : Fix(Gal(M : L))] = |Gal(M : L)| = [M : L]$. By (8.1.2, iii), $L \subseteq Fix(Gal(M : L))$ & by the Tower Law, $[M : Fix(Gal(M : L))] = [M : L] = [M : Fix(Gal(M : L))][Fix(Gal(M : L)) : L] \iff$ $[Fix(Gal(M : L)) : L] = 1 \iff L = Fix(Gal(M : L))$. We have proved most of 3) in (7.1.5, ii): remains to show that if L intermediate field with $Gal(M : L) \triangleleft Gal(M : K)$, then $L : K$ normal. Assume that $H = Gal(M : L) \triangleleft Gal(M : K)$. By (7.3.7), $Fix(Gal(M : L)) : K$ is a normal extension. But by 1), $Fix(Gal(M : L)) = L \therefore L : K$ normal.

Using the Fundamental Theorem

Useful Remarks
1.*The Galois Group permutes roots of polynomials: its action is completely determined by its effect on the roots, and it is faithful* (by (6.3.7) & (6.3.8)).
2.*The Galois Group is isomorphic to a subgroup of S_k, so its order divides k!* (by (6.3.10) & (6.3.14)).
3.*The Galois Group maps conjugates to conjugates* (by (7.1.9)). Recall, 2 elements are conjugate if they have the same MP (by (6.1.4)).
4.*If f irreducible, the action of the Galois Group on the roots of f is transitive* (by (7.1.11)).

Finding Fixed Fields for Subgroups
Let H be a subgroup of $Gal(M : K)$. Then:
1.Find elements $\alpha_1, \dots, \alpha_r$ fixed by H. Then $K(\alpha_1, \dots, \alpha_r) \subseteq \text{Fix}(H)$.
2.Ensure that $[M : K(\alpha_1, \dots, \alpha_r)] = |H|$.
3.Then, using the Fundamental Theorem $[M : \text{Fix}(H)] = |H|$ so by the Tower Law, $[M : \text{Fix}(H)] = [M : K(\alpha_1, \dots, \alpha_r)] = [M : \text{Fix}(H)][\text{Fix}(H) : K(\alpha_1, \dots, \alpha_r)] \iff$ $K(\alpha_1, \dots, \alpha_r) = Fix(H)$.

Corollary to the Fundamental Theorem (Corollary 8.2.7)
Let $M : K$ be a **finite**, **normal**, **separable** FE. Then: $\forall \alpha \in M \setminus K, \exists \varphi : \varphi(\alpha) \neq \alpha$ where φ is automorphism of M over K.

By (8.2.1, i), $\text{Fix}(Gal(M : K)) = K$. If $\alpha \in M \setminus K$, $\alpha \notin K \therefore \alpha \notin \text{Fix}(Gal(M : K)) \therefore$ no elements of Galois Group fix α.

Worked Examples of the Fundamental Theorem

Galois Group for Extensions of Prime Degree
If $[M : K] = p$, then $Gal(M : K) = p \therefore$ only trivial intermediate fields/subgroups.

Galois Group for Reducible Polynomial
Let $f = (t^2 + 1)(t^2 - 2) \in \mathbb{Q}[t]$, $M = SF_{\mathbb{Q}}(f) = \mathbb{Q}(\sqrt{2}, i)$ & $G = Gal(M : K) = Gal_{\mathbb{Q}}(f)$. M is SF $\therefore$ finite and normal. Over $\mathbb{Q} \therefore$ separable. By FTGT, $|G| = [M : K] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. MP of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2 \therefore$ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Similarly, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \therefore i$ has MP $t^2 + 1$ over $\mathbb{Q}(\sqrt{2}) \therefore$ $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. Hence, $|G| = 4$. Roots of f are $\pm\sqrt{2}, \pm i$, so the action of G on $SF_{\mathbb{Q}}(f)$ restricts to an action on these roots. Moreover, $\pm\sqrt{2}$ are conjugate, whereas $\pm i$ are conjugate. Thus, for any $\varphi \in G$, we must have that: $\varphi(i) = \pm i$ & $\varphi(\sqrt{2}) = \pm\sqrt{2}$. The choice of sign for where $i, \sqrt{2}$ get sent to determine φ entirely, and since $|G| = 4$, $\therefore$ all 4 possibilities occur. Let $G = \{\iota, \varphi_{+-}, \varphi_{-+}, \varphi_{--}\}$. Each element of G has order 2 $\therefore$ $G \cong C_2 \times C_2$. By construction, $\varphi_{+-}(\sqrt{2}) = \sqrt{2} \therefore \mathbb{Q}(\sqrt{2}) \subseteq Fix(\left\langle \varphi_{+-} \right\rangle)$. Moreover, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. By the FTGT, $[\mathbb{Q}(\sqrt{2}, i) : Fix(\left\langle \varphi_{+-} \right\rangle] = |\left\langle \varphi_{+-} \right\rangle| = 2$. By Tower Law, $\mathbb{Q}(\sqrt{2}) = Fix(\left\langle \varphi_{+-} \right\rangle)$. Similarly, $\varphi_{-+}(i) = i \implies Fix(\left\langle \varphi_{-+} \right\rangle) = \mathbb{Q}(i)$ & $\varphi_{--}(\sqrt{2}i) = \sqrt{2}i \implies Fix(\left\langle \varphi_{--} \right\rangle) = \mathbb{Q}(\sqrt{2}i)$. The Galois Correspondence then tells us that, for example, $Gal(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(i)) = \left\langle \varphi_{-+} \right\rangle$. Every subgroup of an abelian group is normal, so in particular all the intermediate fields lead to normal extensions.

Galois Group for $t^3 - 2$
Let $f = t^3 - 2 \in \mathbb{Q}[t]$. Let α be real root of f & let $\omega = e^{2\pi i/2}$ be non-real root of $t^3 - 1 \in \mathbb{Q}[t]$. Roots of f are $\{\alpha, \alpha\omega, \alpha\overline{\omega} = \alpha\omega^2\}$. Let $M = SF_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha, \omega)$. Since f irreducible & annihilating, it is MP of roots $\therefore$ they are conjugate & G acts transitively on them $\therefore |G| \geq 3$. Since $G \leq S_3$, either $G \cong A_3$ or $G \cong S_3$. Conjugation (restricted to M) must be element of G, which has order 2 $\therefore$ by Lagrange's Theorem, $G \cong S_3$. The elements of G are ι, $\rho, \rho^{-1} = \rho^2$ (3-cycles, $\rho : \alpha \mapsto \alpha\omega \mapsto \alpha\omega^2 \mapsto \alpha$) & 3 transpositions σ_i (σ_i fixes $\alpha\omega^i$). Non-trivial proper subgroups are $\langle \rho \rangle \cong_A 3$ (only non-trivial normal subgroupo) & $\langle \sigma_i \rangle \cong C_2$. σ_i fixes $\alpha\omega^i \therefore \mathbb{Q}(\alpha\omega^i) \subseteq \text{Fix}\langle \sigma_i \rangle$. $[\mathbb{Q}(\alpha\omega^i) : \mathbb{Q}] = 3$ (MP is $t^3 - 2$), so $6 = [M : \mathbb{Q}] = [M : \text{Fix}\langle \sigma_i \rangle][\text{Fix}\langle \sigma_i \rangle : \mathbb{Q}]$ & $|\langle \sigma_i \rangle| = 2 \therefore$ by FTGT, $[M : \text{Fix}\langle \sigma_i \rangle] = 2 \therefore [\text{Fix}\langle \sigma_i \rangle : \mathbb{Q}] = 3 \therefore \text{Fix}(\alpha\omega^i) = \mathbb{Q}(\alpha\omega^i)$. ρ is homomorphism $\therefore$ $\alpha\omega^2 = \rho(\alpha\omega) = \rho(\alpha)\rho(\omega) = \alpha\omega\rho(\omega) \therefore \rho(\omega) = \omega$. Thus, $\mathbb{Q}(\omega) \subseteq \text{Fix}\langle \rho \rangle$. By FTGT, $[M : \text{Fix}\langle \rho \rangle] = |\langle \rho \rangle| = 3 \therefore [\text{Fix}\langle \rho \rangle : \mathbb{Q}] = 2 \therefore \text{Fix}\langle \rho \rangle = \mathbb{Q}(\omega)$.

Galois Group for $t^4 - 2$
Let $f = t^4 - 2 \in \mathbb{Q}$. Let α be unique real positive root. Roots are $\pm\alpha, \pm\alpha i$. Let $M = SF_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha, i)$, $G = Gal(M : \mathbb{Q})$. By Tower Law, $|G| = [M : \mathbb{Q}] = [M : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$. Claim: $G \cong D_4$. κ (complex conjugation restricted to M) in G. Using transitivity (f irreducible), $\exists \rho \in G : \rho(\alpha) = $ & $\rho(i)$ (argue by transitivity of elements in G, alongside the fact that i conjugate to $-i$). To show that $G =< \rho, \kappa$, construct table & apply (4.3.6), which shows that since elements are distinct on α, i, they are distinct on all of M. To confirm $G \cong D_4$, prove that $\kappa\rho(i) = \rho^{-1}\kappa(i)$ & $\kappa\rho(\alpha) = \rho^{-1}\kappa(\alpha)$. The subgroups of order 2 are $\left\langle \rho^2 \right\rangle, \langle \kappa \rangle, \langle \kappa\rho \rangle, \left\langle \kappa\rho^2 \right\rangle, \left\langle \kappa\rho^3 \right\rangle$. $\left\langle \rho^2 \right\rangle$ commutes with all elements of $G \therefore$ normal. The others aren't normal, since $\rho(\kappa\rho^r)\rho^{-1} \notin \langle \kappa\rho^r \rangle$. $\langle \rho \rangle$ subgroup of order 4. 2 other groups of order 4, which are isomorphic to $C_2 \times C_2$ and must contain ρ^2, which are $\left\langle \kappa, \rho^2 \right\rangle$ & $\left\langle \kappa\rho, \rho^2 \right\rangle$. All subgroups of order 4 are normal, since they have index 2. For intermediate fields, ρ^2 fixes i (but not enough); it also fixes α^2, and $\text{Fix}\left\langle \rho^2 \right\rangle = \mathbb{Q}(\alpha^2, i)$. κ fixes any real, and $\text{Fix}\,\kappa = \mathbb{Q}(\alpha)$. $\kappa\rho$ is diagonal reflection, which fixes $\alpha(1 - i)$. Since $\alpha(1 - i))^2 \notin \mathbb{Q}$ & the order of its MP divides 8 (Tower Law), $[\mathbb{Q}(\alpha(1 - i)) : \mathbb{Q}] \geq 4 \iff [M : \mathbb{Q}(\alpha(1 - i))] \leq 8/4 = 2$. But $[M : \mathbb{Q}(\alpha(1 - i))] > 1$ since $\alpha \notin \mathbb{Q}(\alpha(1 - i)) \therefore [M : \mathbb{Q}(\alpha(1 - i))] = 2 \therefore$ $\text{Fix}\langle \kappa\rho \rangle = \mathbb{Q}(\alpha(1 - i))$. Similarly, $\text{Fix}(\kappa\rho^2) = \mathbb{Q}(\alpha i)$ & $\text{Fix}(\kappa\rho^3) = \mathbb{Q}(\alpha(1 + i))$. Lastly, ρ fixes $i \therefore \text{Fix}\langle \rho \rangle = \mathbb{Q}(i)$; α^2 is fixed by κ & ρ^2, so $\text{Fix}\left\langle \kappa, \rho^2 \right\rangle = \mathbb{Q}(\alpha^2)$; $\alpha^2 i$ is fixed by $\kappa\rho$ & ρ^2, so $\text{Fix}\left\langle \kappa\rho, \rho^2 \right\rangle = \mathbb{Q}(\alpha^2 i)$. If $L = \mathbb{Q}(\alpha^2, i)$, the corresponding subgroup is $\left\langle \rho^2 \right\rangle$, and by FTGT, $G/\langle \rho \rangle^2 \cong Gal(\mathbb{Q}(\alpha^2, i) : \mathbb{Q})$. By Lagrange's Theorem, this group has order 4, but only contains elements of order at most 2, so $Gal(\mathbb{Q}(\alpha^2, i) : \mathbb{Q}) \cong C_2 \times C_2$. If L is a subfield of degree 4, then $|G/Gal(M : L)| = 2$ so the corresponding Galois Groups are isomorphic to C_2.

Useful Theorems

DeMoivre's Theorem

Given $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, then $(e^{i\theta})^n = (\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta) = e^{in\theta}$. Can be used to derive trig identities, like $\cos(3\theta) = Re(\cos(3\theta) + i\sin(3\theta)) = Re\left((\cos(\theta) + i\sin(\theta))^3\right)$
$= Re\left(\cos^3(\theta) + 3\cos^2(\theta)(i\sin(\theta)) + 3\cos(\theta)(i\sin(\theta))^2 + (i\sin(\theta))^3\right)$
$= \cos^3(\theta) - 3\cos(\theta)\sin^2(\theta) = \cos^3(\theta) - 3\cos(\theta)(1 - \cos^2(\theta)) = 4\cos^3(\theta) - 3\cos(\theta)$. This shows that $\cos(\pi/9)$ has annihilating polynomial $4t^3 - 3t - \frac{1}{2}$.

Roots of Unity

From DeMoivre's Theorem, we can solve equations of the form $z^n = k$, by assuming $x = e^{i\theta}$. In particular, the nth **roots of unity** are the complex solutions to $z^n - 1 = 0$. The roots are ω^i, where $i \in [1, n]$, $\omega = e^{2\pi i/n}$. Recall, $e^{2\pi i} = 1, e^{i\pi} = -1, e^{i\pi/2} = i$. Then, to solve $z^n - k = 0$, the roots are $\alpha\omega^i$, where $\alpha = k^{1/n}$.

Trigonometric Identities

- $\sin(\pi/6) = \cos(\pi/3) = \frac{1}{2}$ • $\sin(\pi/3) = \cos(\pi/6) = \frac{\sqrt{3}}{2}$
- $\sin(\pi/4) = \cos(\pi/4) = \frac{1}{\sqrt{2}}$ • $\sin(\pi/2) = \cos(0) = 1$
- $\sin(n\pi) = 0$ for $n \in \mathbb{Z}$ • $\cos(n\pi) = (-1)^n$ for $n \in \mathbb{Z}$
- $\cos(2x) = \cos^2(x) - \sin^2(x) = 2\cos^2(x) - 1 = 1 - 2\sin^2(x)$
- $\sin(2x) = 2\sin(x)\cos(x)$ • $\sin^2(x) + \cos^2(x) = 1$

Vieta's Theorem

Let $p(t) = \sum_{i=0}^n a_i t^i$. Then if p has roots $r_1, \ldots, r_n$:

- $\sum_{i=1}^n r_i = -\frac{a_{n-1}}{a_n}$ • $\sum_{i=1}^n \sum_{j>i} r_i r_j = \frac{a_{n-2}}{a_n}$
- $\ldots$ • $\prod_{i=1}^n r_i = (-1)^n \frac{a_0}{a_n}$

For example, if $p = at^2 + bt + c$, then:

- $r_1 + r_2 = -\frac{b}{a}$ • $r_1 r_2 = \frac{c}{a}$

If $p = at^3 + bt^2 + ct + d$, then:

- $r_1 + r_2 + r_3 = -\frac{b}{a}$ • $r_1r_2 + r_1r_3 + r_2r_3 = \frac{c}{a}$ • $r_1r_2r_3 = -\frac{d}{a}$

Past Papers

Sample Paper

1.**Let $a, b \in \mathbb{Q}$. Prove that $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Hence or otherwise, prove that $\deg_{\mathbb{Q}}(\sqrt{a} + \sqrt{b})$ is 1,2, or 4.**

$\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$ is immediate. Sufficient to show that $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. 2 methods: $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}) \therefore \frac{1}{\sqrt{a}+\sqrt{b}} = \frac{\sqrt{a}-\sqrt{b}}{a-b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}) \therefore$ $\sqrt{a} - \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}) \therefore \sqrt{a} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ since $\sqrt{a} + \sqrt{b} + (\sqrt{a} - \sqrt{b}) = 2\sqrt{a}$. Alternatively, $(\sqrt{a} + \sqrt{b})^3 = (a + 3b)\sqrt{a} + (b + 3a)\sqrt{b}$. Since $(a + 3b)(\sqrt{a} + \sqrt{b}) \in \mathbb{Q}(\sqrt{a} + \sqrt{b}) \therefore$ subtracting yields $\sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Thus, $\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}]$. Then, can use Tower Law arguments to show that for different choices of $\sqrt{a}, \sqrt{b}$, the intermediate degrees are 1 or 2, which yields result.

2.**Call a FE special if it is finite, normal and Galois Group has order less than or equal to 10. Let $K, M \leq \mathbb{C}$ with $K \subseteq M$. Let $0_K \neq f \in K[t]$. Show that if $SF_K(f) : K$ special, then $SF_M(f) : M$ special.** By 6.3.12, $Gal_M(f)$ isomorphic to subgroup of $Gal_K(f) \therefore [SF_M(f) : M] \leq [SF_K(f) : K]$. Splitting fields are finite and normal by 7.1.5. Hence, $SF_M(f)$ special.

3.**Prove that $Gal_{\mathbb{Q}}(t^7 - 12)$ is nor abelian.** Use irreducibility of $t^7 - 12$, then G acts transitively, which yields κ (complex conjugation) and φ as an element of order 7 mapping $\varphi(\alpha) = \alpha\omega$, where α real root ot $t^7 - 12$ and $\omega = e^{2\pi i/7}$. But $\varphi \circ \kappa \neq \kappa \circ \varphi$ (for example, evaluate on $a\omega$) $\therefore G$ not abelian. Alternatively, Since $t^7 - 12$ irreducible of degree 7, $|G|$ divisible by 7 $\therefore$ by Cauchy's Theorem, contains element of order 7. Moreover, contains complex conjugation (order 2). If G abelian, then if orders of elements are coprime m, n, their product yields element of order mn. Hence, if G abelian, it contains element of order 14. But G subgroup of S_7, and no element in S_7 has order 14 (look at cycle decompositions).

4.**Let $M : K$ FE of degree n. Let $\theta \in Gal(M : K)$. Prove that at most n elements of $X = \{\theta(\alpha)/\alpha | 0_K \neq \alpha \in M\}$ belong to K.** Let $a \in K \cap X$. Then, $\exists\alpha \in M$ such that $a = \theta(\alpha)/\alpha \therefore \theta(\alpha) = a\alpha$. Hence, $a \in K$ is an eigenvalue, and there are at most n eigenvalues for a K-linear map like θ.

May 2020/2021

1.**Justify whether the following are irreducible or not.**

- $t^5 - 2t^4 + 3t^3 - t - 1$ is reducible, $t = -1$ is a root
- $t^6 - t^5 + t^4 - t^3 + t^2 - t + 1$ is irreducible. The mapping $t \mapsto -t$ is a bijection $\therefore$preserves irreducibility. The result under the map is the 7th cyclotomic polynomial, which is irreducible.
- $t^3 - 2t^2 - t - 1$ is irreducible: reduce modulo 2, results in $t^3 + t + 1$ which has no roots in $\mathbb{Z}_2$.
- $t^4 - 14t^2 + 49$ is reducible. Let $y = t^2$, then this becomes $y^2 - 14y + 49 = (y - 7)^2 \therefore$ polynomial factorises into $(t^2 - 7)^2$

2.**Let $K(\alpha)$ be a simple extension of a field K by element α with MP $m \in K[t]$. Let L be an extension of K. Show by example that there need not exist a homomorphism $K(\alpha) \to L$ over K.**

- no homomorphism over $\mathbb{Q}$ can exist between $\mathbb{Q}(\alpha) : \mathbb{Q}$, since there is no element of $\mathbb{Q}$ to which $\sqrt{2}$ can be sent to if the mapping fixes $\mathbb{Q}$
- no homomorphism over $\mathbb{Q}$ can exist $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(i)$, as we'd require that $\sqrt{2} \mapsto a + ib$. Expanding $(a + ib)^2$ shows that this can never be mapped to from 2 $\therefore$ no homomorphism can exist

3.**Let $a, b \in \mathbb{Q}$ with $\sqrt{a}, \sqrt{b} \notin \mathbb{Q}$. Prove that if $\sqrt{ab} \in \mathbb{Q}$, then $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 2$. If $\sqrt{ab} \notin \mathbb{Q}$, then $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 4$.**

Workshops

Workshop 1

1.**Let f be quadratic over $\mathbb{Q}$ with roots $\alpha_1, \alpha_2 \in \mathbb{C}$. Show that it is impossible that $\alpha_1 \in \mathbb{Q}$ but $\alpha_2 \in \mathbb{Q}$.** Let $f = at^2 + bt + c$. By quadratic formula, the rationality of the roots is dependnent on whether $\sqrt{b^2 - 4ac}$ is rational or not. If rational, both roots rational. Otherwise, neither root can be rational.

2.**Let $f \in \mathbb{Q}[t]$ quadratic. Prove $Gal(f)$ is S_2 if f has 2 distinct irrational roots, and trivial otherwise (using original definition of Gal).** By 1), either both roots are rational or irrational. If both rational, trivial galois group. Other wise, let $\Delta = b^2 - 4ac$. Define $\mathbb{Q}(\sqrt{\Delta})$. Adapting conjugation, $\overline{p(\alpha, \beta)} = p(\overline{\alpha}, \overline{\beta})$. By quadratic formula, $\alpha_1, \alpha - 2 \in \mathbb{Q}(\Delta)$, and by above, $\overline{\alpha}_1 = \alpha_2, \overline{\alpha}_2 = \alpha_2$, so $p(\alpha_1, \alpha_2) = 0 \iff p(\alpha_2, \alpha_2) = 0$ so conjugate.

3.(a)**Let $f = \sum_{i=0}^n a_i t^i \in \mathbb{Z}$. Let c/d be a rational root of f, with c, d coprime. Prove that $c|a_0$ and $d|a_n$.** $\sum_i a_i c^i/d^i = 0 \therefore d^n \sum_i a_i c^i/d^i = 0 \therefore \sum_i a_i c^i/d^{n-i} = 0$ where we have a sum of integers. Notice, $c|0$, so c divides the LHS. In particular, it must thus divide $a_0 d^n$. Since c, d coprime, $c|a_0$. Similarly, $d|0$ so d divides the LHS $\therefore d|a_n c^n$. c, d coprime $\therefore d|a_n$.

(b)**Deduce that every rational root of a monic polynomial over $\mathbb{Z}$ is an integer.** If c/d is a rational root, we must have $d|1$, so $d = \pm 1$ and $c/d \in \mathbb{Z}$.

(c)**Show that $2t^5 + 4t + 3$ has no rational roots.** By rational roots theorem above, the roots are c/d such that $c \in \{\pm 1, \pm 3\}$ and $d \in \{\pm 1, \pm 2\}$. The polynomial has no positive roots, and we can check that none of the negative combinations work.

(d)**Let K be a field such that for $\alpha, \beta \in K$, α square root of $\beta \iff \beta$ square root of α.** If α square root of β, then $\alpha^2 = \beta$. Similarly, $\beta = \alpha^2$. Equivalently, $\forall\alpha \in K, \alpha^4 =$. Every element of K is root of $t^4 - t$, which has at most 4 roots in K, so $|K| \leq 4$. A field has at most 2 elements ($0_K \neq 1_K$). Suppose $|K| = 3$. Then, $\exists\alpha \in K$, $\alpha \neq 0_K, 1_K$ such that $\alpha^2 = 1$. Then, $\alpha^4 = 1_K \neq \alpha$. Hence, $|K| \in \{2, 4\}$. Now, if $|K| = 2$, this forces $K = \{0_K, 1_K\}$, so certainly $0_K^4 = 0_K, 1_K^4 = 1_K$. If $|K| = 4$, $K^\times$ forms a group of order 3, so if $0_K \neq \alpha \in K^\times$, $\alpha^3 = 1_K$ so $\alpha^4 = \alpha$. Hence, the condition is satisfied $\iff$ $|K| = 2$ or $|K| = 4$.

Workshop 2

1.(a)**Can C_6 act faithfully on a 4-element set?** No. Assume C_6 acts faithfully. Then, by (2.1.11), C_6 is isomorphic to a subgroup of S_4. C_6 contains element of order 6, but S_4 doesn't (consider cycle decompositions).

(b)**Let G be a finite group acting transitively on non-empty set X. Prove that $|X|$ divides $|G|$.** G acts transitively, so it has a single orbit. Then, by Orbit-Stabilizer Theorem, $|G| = |X||Stab_G(x)|$ for some $x \in X$.

2.(a)**Let F ring and $I_0 \subseteq I_1 \subseteq \ldots$ ideals of R. Prove that $\bigcup_{n=0}^\infty I_n$ is an ideal of R.** Let $I = \bigcup_n I_n$. Then, $0_R \in I_0 \subseteq I$, so $0_R \in I$. Let $r, s \in I$. Then $\exists n, m \geq 0$ such that $r \in I_n, s \in I_m$. Let $p = \max\{m, n\}$. Then $r, s \in I_p \therefore r - s \in I_p \subseteq I \therefore r - s \in I$. Lastly, let $r \in I$, $a \in R$. Then $r \in I_n$ for some $n \therefore ar \in I_n \subseteq I \therefore ar \in I$.

(b)**Let R be a PID, and let $I_0 \subseteq I_1 \subseteq \ldots$ be ideals of R. Prove that $\exists n \geq 0$: $I_n = I_{n+1} = I_{n+2} = \ldots$.** By part above, $I = \bigcup_n I_n$ is ideal. R is PID, so $\exists r \in R$: $I = \langle r\rangle$. Since $r \in I$, choose $n \geq 0 : r \in I_n$. $\forall m \geq n$, $r \in I_m \therefore \langle r\rangle \subseteq I_m \therefore II_m$. By definition, $I_m \subseteq I \therefore I = I_m$.

(c)**Let R ID. Let $r, s \in R$, $r \neq 0$ s not unit. Prove that $\langle rs\rangle$ is a proper subset of $\langle r\rangle$.** Certainly, $\langle rs\rangle \subseteq \langle r\rangle$, since $rs \in \langle r\rangle$ and $\langle rs\rangle$ is smallest ideal containing rs. Assume $\langle rs\rangle = \langle r\rangle$. Then, $r \in \langle rs\rangle \therefore \exists a \in R : r = rsa$. $r \neq 0$ & R is ID, so by cancellation, $1_R = sa \therefore s$ is unit, a contradiction.

(d)**Let R be PID. Let $r \in R$ be neither 0_R nor unit. Prove that some irreducible divides r.** Suppose by contradiction that no irreducible divides r. Let $r_0 = r$. Then, r_0 not irreducible, 0_R or a unit, so r_0 is reducible & $r_0 = r_1 s_1$, where neither r_1 nor s_1 are units. r_1 is non-zero (r is not), can't be irreducible (it divides r) and isn't a unit by assumption, so r_1 reducible. Continuing logic, we obtain an infinite sequence $(r_n)_{n \geq 0}$ and $(s_n)_{n \geq 1}$ where non of the elements are 0_r or units, and $r_n = r_{n+1}s_{n+1}$ for each $n \geq 0$. By work above , $\langle r_n\rangle$ is proper subset of r_{n+1}, so $\langle r_0\rangle \subset \langle r_1\rangle \subset \ldots$. But R is PID, so we should have that $\langle r_n\rangle = \left\langle r_{n+1}\right\rangle = \ldots$, but since we have proper subsets, this can never be the case.

3.**Let K field.**

(a)**For $f \in K[t]$, (3.1.6) guarantees that there is a unique homomorphism $\theta_f : K[t] \to K[t]$ such that $\theta_f(t) = f, \theta_f(a) = a$ for K. Let $f, g \in K[t]$. What is $\theta_f(g)$ in explicit terms? What is its degree?** Let $g = \sum_i b_i t^i$. Then, $\theta_f(g) = \sum_i b_i \theta(_f(t)^i$ $= \sum_i b_i f(t)^i = g(f(t)) = (g \circ f)(t)$. Then, $\deg(\theta_f(g)) = \deg(g) \cdot \deg(f)$.

(b)**For $f_1, f_2 \in K[t]$, what can you say about the composite homomorphism $\theta_{f_2} \circ \theta_{f_1}$?** By previous part, $(\theta_{f_2} \circ \theta_{f_1})(t) = (f_1 \circ f_2)(t)$ and $(\theta_{f_2} \circ \theta_{f_1})(a) = a$. By Universal Property, there is only one homomorphism mapping $t \mapsto f_1 \circ f_2$ and $a \mapsto a$, namely $\theta_{f_1 \circ f_2}$, so $\theta_{f_2} \circ \theta_{f_1} = \theta_{f_1 \circ f_2}$.

(c)**Find all isomorphisms $K[t] \to K[t]$ over K.** Let $\theta : K[t] \to K[t]$ be isomorphism over K. Let $f = \theta(t)$. By uniqueness, $\theta = \theta_f$. Similarly, $\theta^{-1}(t) = \tilde{f}$ implies $\theta^{-1} = \theta_{\tilde{f}}$. Hence, $\theta_f \circ \theta_{\tilde{f}} = \mathrm{id}$. But then, $\tilde{f} \circ f = t$ and taking degrees of both sides implies that $\deg(f) = \deg(\tilde{f}) = 1$. Write $f = at + b$. By direct calculation, $\tilde{f} = (t - b)/a$, such that $\tilde{f} \circ f = \mathrm{id} = f \circ \tilde{f}$. Thus, θ_f is isomorphism with inverse $\theta_{\tilde{f}}$ with $\theta_f(g) = g(at + b)$.

4.**Let $f = t^4 + t^3 + t^2 + t + 1$ have roots $\omega, \omega^2, omega^3, \omega^4$, where $\omega = e^{2\pi i/5}$. One of the elements of $Gal(f)$ is $\sigma = (1243)$. Prove that $Gal(f)$ is generated by σ and deduce that $Gal(f) \cong C_4$.** Let $\tau \in Gal(f)$. Every non-zero integer mod 5 is a power of 2: $2^0 \cong 1, 2^1 \cong 2, 2^2 \cong 4, 2^3 \cong 3$. Then, $\exists r \geq 0 : \tau(1) = 2^r$ $(mod\ 5)$. Claim: $\tau = \sigma^r$. Let $i \in [1, 4]$ and define $p(t_1, t_2, t_3, t_4) = t_i - t_1^i$. Then, $p(\omega, \omega^2, \omega^3, \omega^4) = \omega^i - \omega^i = 0$, so by definition of Galois Group, $p(\omega^{\tau(1)}, \omega^{\tau(2)}, \omega^{\tau(3)}, \omega^{\tau(4)}) = 0 \therefore \omega^{\tau(i)} = \omega^{\tau(1)i} \therefore$ $\tau(i) \cong \tau(1)i$ $(mod\ 5) \therefore \tau(i) \cong 2^r i$ $(mod\ 5)$. Now, $\sigma(i) \cong 2i$ $(mod\ 5) \therefore$ $\sigma^r(i) \cong 2^r i$ $(mod\ 5) \therefore \tau = \sigma^r \therefore Gal(f) \langle\sigma\rangle$. Since $o(\sigma) = 4$ (as $\sigma^2 \neq \iota$), $\langle\sigma\rangle \cong C_4$.

Workshop 3

1.**Which of the following are irreducible over $\mathbb{Q}$?**

(a)$1 + 2t - 5t^3 + 2t^6$ is reducible, as $t = 1$ is a root.
(b)$4 - 3t - 2t^2$ is irreducible, as it is quadratic without rational (discriminant is 41)
(c)$4 - 13t - 2t^3$ is irreducible: reduce mod 3, becomes $1 - t + t^3$ which has no roots in $\mathbb{Z}_3$.
(d)$1 + t + t^2 + t^3 + t^4 + t^5$ is reducible, as -1 is a root (it factorises as $(1 + t + t^2)(1 + t^3)$
(e)$2.2 + 3.3t - 1.1t^3 + t^7$ is irreducible, by multiplying by 10 and using Eisenstein with $p = 11$.
(f)$1 + t^4$ is irreducible. Either substitute $t = u + 1$ & use Eisenstein with $p = 2$. alternatively, assume reducible, so by Gauss, can be factorised as $(t^2 + a_1 + a_0)(t^2 + b_1 t + b_0)$ with a_0, a_1, b_0, b_1 integers, which leads to contradiction.

2.**Find irreducible $f \in \mathbb{R}[t]$ such that $\mathbb{R}[t]/\langle f\rangle \cong \mathbb{C}$.** Let $f = t^2 + 1$. Since $\mathbb{C} = \mathbb{R}(i)$ and i has MP f over $\mathbb{R}$, so (4.3.11, i) implies $\mathbb{R}[t]/\langle f\rangle \cong \mathbb{C}$.

3.**Let $M : K$ finite, $\alpha \in M$ with MP $m \in K[t]$. Show that $\deg(m)$ divides $[M : K]$.** $[K(\alpha) : K] = \deg(m)$ by (5.1.5) & by Tower Law, $[M : K] = [M : K(\alpha)][K(\alpha) : K]$.

4.**Let $M : K$ be FE with $\alpha, \beta \in M$.**

(a)**Prove that α, β conjugate over $K \iff$ either both are transcendental or both are algebraic and have the same MP.** By (4.2.6), APs of α over K are $\langle m_\alpha\rangle$. Similarly, APs of β over K are $\left\langle m_\beta\right\rangle$. Then, α, β conjugate over $K \iff \langle m_\alpha\rangle = \left\langle m_\beta\right\rangle$. Since m_α, m_β are either zero or monic, this is true if and only if $m_\alpha = m_\beta$. $m_\alpha = m_\beta \iff$ either $m_\alpha = 0 = m_\beta$ (so α, β transcendental) or $0 \neq m_\alpha = m_\beta \neq 0$ (α, β algebraic with same MP).

(b)**Show that if there exists irreducible $p \in K[t]$ with $p(\alpha) = 0 = p(\beta)$, then α, β conjugate over K.** Can assume p monic (divide by constant). By 4.2.10, p is MP of α, β, so by result above, α, β conjugate

5.**Let $M : L : K$ be FE, which you may not assume to be finite. Let $\alpha \in M$. Prove that if α algebraic over L, and L algebraic over K, then α algebraic over K. Thus, deduce that if $M : L$, $L : K$ are algebraic, then so is $M : K$.** α algebraic over L, so $\exists b_i \in L$ such that $\sum_{i=0}^n b_i\alpha^i$, not all of which are 0. By the Tower Law, $[K(b_0, \ldots, b_n, \alpha) : K] = [K(b_0, \ldots, b_n, \alpha) : K(b_0, \ldots, b_n)][K(b_0, \ldots, b_n) : K]$. Since α algebraic over $K(b_0, \ldots, b_n)$ (since not all b_i are 0), then $[K(b_0, \ldots, b_n, \alpha) : K(b_0, \ldots, b_n)] < \infty$. Since the b_i are algebraic over K, by (5.2.4) then $[K(b_0, \ldots, b_n) : K] < \infty$. Thus, $K(b_0, \ldots, b_n, \alpha) : K$ is an algebraic extension, so α algebraic over K. For any $\alpha \in M$, since $M : L$ algebraic, α algebraic over L, so by the previous part, and since $L : K$ algebraic, it follows that α algebraic over K, so $M : K$ algebraic.

6.**Prove that $\overline{\mathbb{Q}}$ is algebraically closed.** Let $f \in \overline{\mathbb{Q}}[t]$ be non-constant. $\mathbb{C}$ is algebraically closed, so $\exists\alpha \in \mathbb{C}$ with $f(\alpha) = 0$. Then, α algebraic over $\overline{\mathbb{Q}}$. But also, $\overline{\mathbb{Q}} : \mathbb{Q}$ is algebraic, so by the question above, α algebraic over $\mathbb{Q}$, so $\alpha \in \overline{\mathbb{Q}}$ & f has root in $\mathbb{Q}$.

7.**Show that $\forall X \subseteq K$ and filed homomorphism $\varphi : K \to L$, $\varphi\langle X\rangle = \langle\rangle$. Thus, if $M : K$ and $M' : K$ are FE, and $\varphi : M \to M'$ is homomorphism over K, show that $\varphi(K(/)) = K(\varphi(Y)$ for all subsets $Y \subseteq M$.** The first part follows by using the fact that $\langle X\rangle$ is the smallest subfield containing X, and employing (2.3.6, ii) (to show that $\varphi\langle X\rangle \subseteq \langle\varphi X\rangle$) and (2.3.6, ii) (to show that $\langle\varphi X\rangle \subseteq \varphi\langle X\rangle$). Then, taking $X = K \cup Y$, it follows that $\varphi(K(Y)) = \langle\varphi(K \cup Y)\rangle$. Using $\varphi(K \cup Y) = \varphi(K) \cup \varphi(Y)$, the result follows.

8.**Let f be a non-constant polynomial over $\mathbb{Z}$. Prove that f is primitive and irreducible over $\mathbb{Q} \iff f$ is irreducible over $\mathbb{Z}$.** ($\implies$): let f primitive, irreducible over $\mathbb{Q}$. Then, $\deg(f) \geq 1$, so f not unit or 0. Suppose $f = gh$ $g, h \in \mathbb{Z}[t]$. f irreducible over $\mathbb{Q} \therefore$ WLOG, let g unit in $\mathbb{Q}[t]$, so that $g = a \in \mathbb{Z}$. Then, a divides every coefficient of f, which is primitive, so $a = 1 \therefore g$ is unit in $\mathbb{Z}[t] \therefore g$ irreducible. ($\impliedby$): by Gauss's Lemma, f irreducible over r$\mathbb{Q}$. Let $a \in \mathbb{Z}$ divide every coefficient of f, such that $f/a \in \mathbb{Z}[t]$. Then, $f = a \cdot f/a$. But f irreducible over $\mathbb{Z}$, so a is unit in $\mathbb{Z}[t] \therefore a = \pm 1 \therefore f$ primitive.

9.**This question is about extensions of degree 2.**

(a)**Let K field, $a \in K$. Show that $[K(\sqrt{a}) : K] = 1$ if a has square root in K, and 2 otherwise.** If $\sqrt{a} \in K$, then $[K(\sqrt{a}) : K] = 1$. Else, $t^2 - a$ irreducible and MP of $\sqrt{a}$, so $[K(\sqrt{a}) : K] = 2$.

(b)**Let L field, $\mathrm{char}(L) \neq 2$, $a, b, c, \alpha \in L$, $a \neq 0$. Suppose that $a\alpha^2 + b\alpha + c = 0$. Prove that $b^2 - 4ac$ has a square root $\sigma \in L$, and that $\alpha \in \{(-b \pm \sigma)/(2a)\}$.** Complete square of quadratic, and since $\mathrm{char}(L) \neq 2$, we can divide by 2 to get that $b^2 - 4ac = (2a\alpha + b)^2$. Rearranging gives result.

(c)**Let $L : K$ be FE of degree 2 and $\mathrm{char}(K) \neq 2$. Prove that $L \cong K(\sqrt{d})$ for some $d \in K$.** Pick $\alpha \in L \setminus K$ with MP $m \in K[t]$. Then, $\deg(m) = 2$, so write $m = t^2 + bt + c$ and $d = b^2 - 4c \in K$. By part above, $\sqrt{d} = \sigma\ inL$ and $\alpha \in K(\sigma)$, so $L = K(\alpha) \subseteq K(\sigma) \therefore$ $L = K(\sigma) = K(\sqrt{d})$.

10.**Prove that $\overline{\mathbb{Q}} : \mathbb{Q}$ is not finite.** $t^n - 2$ is an irreducible polynomial over $\mathbb{Q}$, call it m_n, and let it have root α_n. Then, since $\alpha_n \in \overline{\mathbb{Q}}$, by Tower law, $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$. Since not finite, it cna't be finitely generated, by (5.2.4).

11.**Let $M : K$ simple algebraic if $\exists\alpha \in M$ such that $m = K(\alpha)$ and α algebraic over K. Prove that $M : K$ simple algebraic $\iff$ it is simple and algebraic.** If $M.K$ simple, $\exists\alpha \in M$ with $M = K(\alpha)$. If $M : K$ algebraic, every element of M algebraic over $K \therefore \alpha$ algebraic. Conversely, if $M : K$ simple algebraic, $M : K$ certainly simple; algebraicity follows from (5.2.4), using $iii \Rightarrow ii$.

12.**Prove that $\mathbb{Q}(t_1, t_2, \ldots)$ and $\mathbb{Q}(t_2, t_3, \ldots)$ are isomorphic, but not isomorphic over $\mathbb{Q}(t_2, t_3, \ldots)$.** Let fileds be K_1, K_2 respecitvely. Define isomorphism $t_i \mapsto t_{i+1}$. However, this can't be isomorphism over K_2, as t_1 is not in the image of φ^{-1}.

13.**Let $M.K$ FE. Prove that every homomorphism $M \to M$ over K is automorphism of M over K.** From linear algebra, if V is isfinite dimensional vector space, ay injective linear map $\varphi : V \to V$ is surjective. Then φ injective $\iff nullity(\varphi) = 0 \iff$ $\dim(V) - rank(\varphi) = 0 \iff \varphi$ surjective. Every $\varphi : M \to M$ over K is injective K-linear map, and $[M : K] < \infty$, so φ sujrective & automorphism of M over K.

Workshop 5

1.**Let $M : K$ FE. Let $0_K \neq f \in K[t]$, $\alpha \in M$ be root of f. Then, $f = (t - \alpha)g$, $g \in K(\alpha)[t]$. Prove that $M = SF_{K(\alpha)}(g) \iff M = SF_K(f)$.** Let $\alpha_1 = \alpha, \ldots, \alpha_n$ roots of f in M. If $M = SF_K(g)$, g splits in $M \therefore f$ splits in M. Moreover, $M = K(\alpha)(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n) \therefore$ roots of f in M generate M over $K \therefore$ $M = SF_K(f)$. Conversely, let $M = SF_K(f)$. f, g split in M, and $M = K(\alpha_1, \ldots, \alpha_n) = K(\alpha)(\alpha_2, \ldots, \alpha_n) \therefore M$ generated by roots of g in M over $K(\alpha)$.

2.**Let K field and $f \in K[t]$ irreducible. Prove that $|Gal_K(f)|$ divisible by number of distinct roots of f in SF, and thus deduce that if $(K) = 0$, $\deg(f)$ divides $|Gal_K(f)|$.** Let K be number of distinct roots. Galois acts transitively $\therefore$ generates single orbit over set of roots $\therefore$ by OST, number of roots divides $|Gal_K(f)|$. If $\mathrm{char}(K)$, K separable, so has $\deg(f)$ distinct roots.

3.**Show that any automorphism of a field M is an automorphism over th eprime subfield of M.** Let M field with prime subfield K. Let φ automorphism of M. Then, $\mathrm{Fix}(\{\varphi\})$ is subfield of M by (7.3.1). But K smallest subfield, so $K \subseteq \mathrm{Fix}(\{\varphi\}) \therefore \varphi$ automorphism over K.

4.**Show by example that if $M : L$, $L : K$ normal, then $M : K$ needn't be normal.** Let $M = \mathbb{Q}(2^{1/4}$, $L = \mathbb{Q}(2^{1/2}$ and $K = \mathbb{Q}$.

5.**Let K field, $f, g \in K[t]$ non-zero. Let $L = SF_K(g)$. Show that $SF_L(f) \cong SF_K(fg)$ over K.** Sufficient to show that $SF_L(f)$ is SF of fg over K. Both f, g split in $SF_L(f)$. Let $\alpha_1, \ldots, \alpha_n$ be roots of f in $SF_L(f)$ and $\beta_1, \ldots, \beta_m$ roots of g in L. Then, $SF_L(f) = L(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \therefore SF_L(f)$ generated over K by roots of fg. For second part, $SF_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ $SF_{\mathbb{Q}}(g) = \mathbb{Q}(\beta_1, \ldots, \beta_m)$ so compositum contains generated by all roots of fg.

6.**Let $0 \neq f \in \mathbb{Q}[t]$ with distinc complex roots $\alpha_1, \ldots, \alpha_k$. Prove that $\sum_{i=1}^{n} \alpha_i^{10}$ is rational.** Let $\alpha = \sum_{i=1}^{n} \alpha_i^{10}$. Each element of Galois group permutes distinct roots of f so it fixes α (since α is symmetric function of these roots). By (8.2.7) applied on $SF_{\mathbb{Q}}(f) : \mathbb{Q}$, $\alpha \in \mathbb{Q}$.

7.**State whether True or False**

(a)**Let $f \in K[t]$ irreducible of degree n. Then $[SF_K(f) : K] \leq n$.** False, let $f = t^3 - 2$, then SF has degree 6

(b)**Let $M : K$ FE and $\alpha, \beta \in M$. Then $[K(\alpha\beta) : K] \leq [K(\alpha, \beta) : K]$.** True, use Tower Law and the fact that $K(\alpha\beta)$ subfield of $K(\alpha, \beta)$.

(c)**Let $(x, y) \in \mathbb{R}^2$. Suppose that x, y have AP of degree 4 over $\mathbb{Q}$. Then, (x, y) are construcible by ruler and compass from $(0, 0), (1, 0)$.** False, $(2^{1/3}, 0)$ not constructible, but have AP $x^4 - 2x = 0, y^4 = 0$.

(d)**For all non-trivial finite FE, Galois group is non trivial.** False, if $\alpha = 2^{1/3}$, Galois Group of $\mathbb{Q}(\alpha) : \mathbb{Q}$ is trivial (Example 6.3.3, ii) of the notes).

(e)**For all finite FE $M : K$, $M' : K'$, every isomorphism $\psi : K \to K'$ can be extended to a homomorphism $\varphi : M \to M'$.** False, let $M = \mathbb{Q}(\sqrt{2})$ and $K = M' = K' = \mathbb{Q}$, with ψ as the identity. Then, $\varphi(\sqrt{2})$ would be a square root of 2 in $\mathbb{Q}$.

(f)**The Galois Group of $(t^4 - 2t^3 + t^2 - 4t + 1)^3$ over $\mathbb{Q}$ is solvable.** True, it hass at most 4 distinct roots, so Galois Group embeds in S_4, which is solvable, and all subgroups of solvable groups are solvable.

8.**Let $L : K$ algebraic. Prove that $L : K$ normal $\iff$ for every extension $M : L$ the field L is a union of conjugacy classes in M voer K.** Suppose $L.K$ is normal & consider $M : L$. Let $\alpha, \beta \in M$ conjugate over K, and suppose $\alpha \in L$. Claim: $\beta \in L$. Since $\alpha \in L$ and $L : K$ normal, MP m of α splits in L. Hence, the roots of m in M are all in L. α conjugate to β over K, and $m(\alpha) = 0$ so $m(\beta)00$ so $\beta \in L$. Conversely, let L be uion of conjugacy classes in M over K for every extension M of L. Let $\alpha \in L$ have MP $m \in K[t]$. Take M as SF of m over L. Then, m splits in M, and all its roots in M are conjugate over K. But $\alpha \in L$, so by assumption all roots of M in M are in L, so m splits in L, Hence, $L : K$ is normal.