1 Introduction I

Theorem 1.1. For any symmetric function $\psi(x_1, \ldots, x_n)$, there exists a unique polynomial $P(t_1, \ldots, t_n)$ such that $\psi(x_1, \ldots, x_n) = P(\sigma_1, \ldots, \sigma_n)$.

Definition 1.2 (Vieta formulae)**.** Suppose $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ has roots $r_1, \ldots, r_n$. Then,

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -a_{n-1} \\ \sum_{1 \le i < j \le n} r_i r_j &= a_{n-2} \\ &\vdots \\ \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} r_{i_1} r_{i_2} \cdots r_{i_k} &= (-1)^k a_{n-k} \\ &\vdots \\ r_1 r_2 \cdots r_n &= (-1)^n a_0 \end{aligned}$$

Note: Any cubic equation can be converted to a depressed cubic by

$$x^3 + Ax^2 + Bx + c = \left(x + \frac{A}{3}\right)^3 + p\left(x + \frac{A}{3}\right) + q.$$

Theorem 1.3 (Vieta's method)**.** Using the trigonometric identity $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, we can solve certain cubic equations. For example, consider $4x^3 - 3x = -\frac{1}{2}$. Let $x = \cos\varphi$. Then

$$\begin{aligned} \cos 3\varphi = -\frac{1}{2} &\iff 3\varphi = \pm\frac{2\pi}{3} + 2\pi k \quad \text{for } k \in \mathbb{Z} \\ &\iff \varphi = \pm\frac{2\pi}{9} + 2\pi k \\ &\iff x \in \left\{\cos\frac{2\pi}{9}, \cos\frac{4\pi}{9}, \cos\frac{8\pi}{9}\right\}. \end{aligned}$$

In general, we can use this method to solve $4x^3 - 3x = a \implies x = \cos\varphi,\ \cos 3\varphi$ and $\cos : \mathbb{C} \to \mathbb{C}$ is now a complex function. For $x^3 + px + q = 0$, set $x = ky$ such that $\frac{k^3}{pk} = \frac{-4}{3} \implies k = \pm\frac{\sqrt{-4p}}{3}$.

Definition 1.4 (Ferrari's resolvent)**.** Let $f(x) = x^4 + ax^2 + bx + c$, and assume $b^2 - 4ac \neq 0$. Consider a parameter y. Then

$$\begin{aligned} f(x) &= \left(x^2 + \frac{y}{2}\right)^2 + (a - y)x^2 + bx + c - \frac{y^2}{4} \\ \implies D &= b^2 - 4(a - y)\left(c - \frac{y^2}{4} = 0\right) \end{aligned}$$

and hence we obtain *Ferrari' resolvent*:

$$y^3 - ay^2 - 4cy + 4ac - b^2 = 0$$

Solving the resolvent allows one to reduce solving f to solving a system of quadratics.

2 Introduction II

Theorem 2.1 (Lagrange)**.** Let $\varphi = \varphi(x_1, \ldots, x_n)$ and

$$\operatorname{orb}(\varphi) = \left\{\varphi^\omega = \varphi(x_{\omega(1)}, \ldots, x_{\omega(n)}) \mid \omega \in S_n\right\}.$$

Then $y_1, \ldots, y_k$ are roots of some polynomial with degree $\le k$ whose coefficients depend on elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ in a polynomial way.

Theorem 2.2 (Lagrange)**.** Let $\varphi, \psi \in K[x_1, \ldots, x_n]$ and $G_\varphi = \{\omega \in S_n \mid \varphi^\omega = \varphi\} \leqslant G_\psi$. Then $\psi = R(\varphi)$ where R is a rational function whose coefficients are symmetric functions on $x_1, \ldots, x_n$.

Theorem 2.3. Let G be a finite group that acts on X. Then for all $x \in X$, $|\text{orb}(x)| \cdot |\text{stab}(x)| = |G|$.

3 Field Extensions I

Lemma 3.1 (Gauss)**.** $\gcd(fg) = \gcd f \cdot \gcd g$

Corollary 3.2. $f \in \mathbb{Z}[t]$ is irreducible $\iff$ f is irreducible over $\mathbb{Q}[t]$

Corollary 3.3. If R is a UFD with field of fractions Q and $f \in R[X]$ with $\deg f > 0$, then f is irreducible in $R[X] \iff f$ is irreducible in Q.

Theorem 3.4 (Eisenstein's Criterion)**.** Let R be a UFD with field of fractions Q and let $f = a_0 + a_1X + \ldots + a_nX^n \in R[X]$ with $\gcd(f) = 1$. Suppose there exists an irreducible element $p \in R$ such that

$$\text{(i) } p \mid a_i \text{ for } 0 \leq i < n, \qquad \text{(ii) } p^2 \nmid a_0, \qquad \text{(iii) } p \nmid a_n$$

then f is irreducible in $R[X]$ (and hence also in $Q[X]$).

4 Field Extensions II

Theorem 4.1. Let $L : K$ with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K.

(i) $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$;

(ii) If $n = \deg \mu_\alpha^K$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K ($\implies [K(\alpha) : K] = \deg \mu_\alpha^K$).

Theorem 4.2 (Rational Root Theorem)**.** Let $\frac{p}{q}$ be a root of $f = a_0t^n + \cdots + a_{n-1}t^{n-1} + a_n$, for $a_j \in \mathbb{Z}$, where p and q are coprime. Then $p \mid a_n$ and $q \mid a_0$.

5 Algebraic Conjugates

Corollary 5.1. If $L : K$ with $\alpha \in L$ algebraic over K, then $K[t]/(\mu_\alpha^K)$ is a field.

Theorem 5.2. Let K be a field, and suppose that $f \in K[t]$ is irreducible. Then there exists a field extension $L : K$, with associated embedding $\varphi : K[t] \to L[y]$, such that L contains a root of $\varphi(f)$.

Lemma 5.3. Let $(x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$ and $f(\overline{y}, x_1, \ldots, x_n) \in K[\overline{y}, x_1, \ldots, x_n]$ be symmetric polynomial in $x_1, \ldots, x_n$. Then $f(\overline{y}, x_1, \ldots, x_n) \in K[\overline{y}]$.

Theorem 5.4. Let α be algebraic over K with algebraic conjugates $\alpha = \alpha_1, \ldots, \alpha_n$. Then for all $f \in K[x]$, the conjugates of $f(\alpha)$ are exactly $f(\alpha_1), \ldots, f(\alpha_n)$.

6 Ruler and Compass Constructions

Lemma 6.1. If a, b, c constructible (or polyquadratic), then $a \pm b$, $\frac{ab}{c}$, and $\sqrt{ab}$ constructible.

Fact 6.2. If m-gon and n-gon are constructible for coprime m, n, then mn-gon is contructible.

Fact 6.3. If $p \geq$ prime, then p^k-gon constructible for $k \in \mathbb{N}$.

Corollary 6.4. The 17-gon is constructible.

Corollary 6.5. If $a \in \mathbb{R}$ is constructible, then $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$ for some $n \geq$

Theorem 6.6 (Gauss-Wantzel)**.** A regular n-gon is constructible $\iff n = 2^r p_1 p_2 \cdots p_s$ for $r \in \mathbb{Z}_{\geq 0}$ and Fermat primes $p_i = 2^{(2^k)} + 1$ for $k \in \mathbb{Z}_{\geq 0}$.

7 Cyclotomic Polynomials

Theorem 7.1. For prime p, we have $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$ and $\mu_{\varepsilon_p}^{\mathbb{Q}} = x^{p-1} + \cdots + 1$.

Definition 7.2 (n^{th} cyclotomic polynomial)**.**

$$\Phi_n(x) = \prod_{\substack{\varepsilon \in \sqrt[n]{1} \\ |\varepsilon| = n}} (x - \varepsilon) = \frac{x^n - 1}{\prod\limits_{d | n, d < n} \Phi_d(x)}$$

Theorem 7.3. Φ_n is irreducible over $\mathbb{Q}$.

Corollary 7.4. (a) $\left[\mathbb{Q}(\exp\left(\frac{2\pi i}{n}\right)) : \mathbb{Q}\right] = \varphi(n)$ (where φ is Euler's totient function);

(b) $\left[\mathbb{Q}(\cos\left(\frac{2\pi}{n}\right)) : \mathbb{Q}\right] = \frac{1}{2}\varphi(n)$. Furthermore, all algebraic conjugates of $\cos\frac{2\pi}{n}$ are $\cos\frac{2\pi k}{n}$ for $\gcd(k, n) = 1$.

(c) Let $c = \frac{a+bi}{a-bi} \in \sqrt[\infty]{1}$, where $a, b \in \mathbb{Z}$. Then $c \in \{\pm i, \pm 1\}$

8 Splitting Fields, Abel-Ruffini

Lemma 8.1. Let $L : K$ be a splitting field extension for $f \in K[t]$ relative to the embedding $\varphi : K \to L$, and let $\alpha_j \in L$ be roots of $\varphi(f)$. Then $L = \varphi(K)(\alpha_1, \ldots, \alpha_n)$.

Lemma 8.2. Let $L : K$ be a splitting field extension for $f \in K[t] \setminus K$. Then $[L : K] \leq (\deg f)!$.

Definition 8.3 (Radical)**.** Let $L : K$ and $\beta \in L$. We say that β is *radical* over K when $\beta^n \in K$ for some $n \in \mathbb{N}$ (so $\beta = \alpha^{1/n}$ for some $\alpha \in K$ and some $n \in \mathbb{N}$).

Definition 8.4 (Radical extension)**.** We say that $L : K$ is *an extension by radicals* when there is a tower of field extensions $L = L_r : L_{r-1} : \cdots : L_0 = K$ such that $L_i = L_{i-1}(\beta_i)$ with β_i radical over L_{i-1} (for $1 \leq i \leq r$).

Definition 8.5 (Solvable by radicals)**.** We say $f \in K[t]$ is *solvable by radicals* if there is a radical extension of K over which f splits.

Theorem 8.6 (Abel-Ruffini)**.** Let $K = \mathbb{C}(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ are formal variables. Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$ be the generic polynomial of degree $n \geq 5$ over K. Then $f(x)$ is not solvable by radicals.

9 Algebraic Closure I

Definition 9.1 (Algebraically closed field, algebraic closure)**.** Let M be a field.

(i) We say that M is *algebraically closed* if every non-constant polynomial $f \in M[t]$ has a root in M.

(ii) We say that M is an algebraic closure of K if $M : K$ is an algebraic field extension such that M is algebraically closed.

Lemma 9.2. Let M be a field. The following are equivalent:

(i) The field M is algebraically closed;

(ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;

(iii) every irreducible polynomial in $M[t]$ has degree 1;

(iv) the only algebraic extension of M containing M is itself.

Definition 9.3 (Extension of field homomorphism, isomorphic field extensions)**.** For $i = 1$ and 2, let $L_i : K_i$ be a field extension relative to the embedding $\varphi_i : K_i \to L_i$. Suppose that $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are isomorphisms. We say that τ *extends* σ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$. In such circumstances, we say that $L_1 : K_1$ and $L_2 : K_2$ are *isomorphic field extensions.*

$$\begin{tikzcd}
L_1 \arrow[r, "\tau"] & L_2 \\
K_1 \arrow[u, "\varphi_1"] \arrow[r, "\sigma"] \arrow[ur, dashed] & K_2 \arrow[u, "\varphi_2"']
\end{tikzcd}$$

When $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are homomorphisms (instead of isomorphisms), then τ *extends σ as a homomorphism of fields* when the isomorphism $\tau : L_1 \to L_1' = \tau(L_1)$ extends the isomorphism $\sigma : K_1 \to K_1' = \sigma(K_1)$.

Lemma 9.4. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Suppose that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$.

(i) if $f(\alpha) = 0$, one has $f(\tau(\alpha)) = 0$;

(ii) if τ is a K-automorphism of L, then $f(\alpha) = 0 \iff f(\tau(\alpha)) = 0$.

Theorem 9.5. Let $\sigma : K_1 \to K_2$ be a field isomorphism. Suppose that L_i is a field with $K_i \subseteq L_i$ $(i = 1, 2)$. Suppose also that $\alpha \in L_1$ is algebraic over K_1, and that $\beta \in L_2$ is algebraic over K_2. Then we can extend σ to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ in such a manner that $\tau(\alpha) = \beta$ if and only if $\mu_\beta^{K_2} = \sigma(\mu_\alpha^{K_1})$.

$$\begin{tikzcd}
K_2 \arrow[r, "\varphi_2"] \arrow[d, "\sigma"] & K_2(\beta) \arrow[r, hook, "\iota_2"] \arrow[d, "\tau"] & L_2 \\
K_1 \arrow[r, "\varphi_1"] & K_1(\alpha) \arrow[r, hook, "\iota_1"] & L_1
\end{tikzcd}$$

Note: When $\tau : K_1(\alpha) \to K_2(\beta)$ is a homomorphism, and τ extends the homomorphism $\sigma : K_1 \to K_2$, then τ is completely determined by σ and the value of $\tau(\alpha)$.

Corollary 9.6. Let $L : M$ be a field extension with $M \subseteq L$. Suppose that $\sigma : M \to L$ is a homomorphism, and $\alpha \in L$ is algebraic over M. Then the number of ways we can extend σ to a homomorphism $\tau : M(\alpha) \to L$ is equal to the number of distinct roots of $\sigma(\mu_\alpha^M)$ that lie in L.

10 Algebraic Closure II

Theorem 10.1. Let $L : K$ be an algebraic extension with $K \subseteq L$ and $\varphi : K \to \overline{K}$ be a homomorphism. Then there exists an extension of φ to a homomorphism $\psi : L \to \overline{K}$.

Theorem 10.2. If L and M are both algebraic closures of K, then $L \cong M$.

Corollary 10.3. Let $L : K$ be an extension with $K \subseteq L$. Suppose that $g \in L[t]$ is irreducible over L, and that $g \mid f$ in $L[t]$, where $f \in K[t] \setminus \{0\}$. Then g divides a factor of f that is irreducible over K. Thus, there exists an irreducible $h \in K[t]$ such that $h \mid f$ in $K[t]$, and $g \mid h$ in $L[t]$.

Definition 10.4 (Normal extension)**.** The extension $L : K$ is *normal* if it is algebraic, and every irreducible polynomial $f \in K[t]$ either splits over L or has no root in L.

Theorem 10.5. A finite extension $L : K$ is normal $\iff$ L is a splitting field extension for some $f \in K[t] \setminus K$.

11 Galois Groups I

Definition 11.1 (Galois group of a field extension)**.** Let $L : K$ be a field extension. Then

$$\mathrm{Gal}_K(L) = \mathrm{Gal}(L : K) = \{\varphi \in \mathrm{Aut}(L) : \varphi \text{ is a K-homomorphism}\}.$$

Theorem 11.2. If $L : K$ is an algebraic extension and $\sigma : L \to L$ is a K-homomorphism, then $\sigma \in \mathrm{Aut}(L)$

Lemma 11.3. Suppose that $M : K$ is a normal extension. Then:

(a) for any $\sigma \in \mathrm{Gal}(M : K)$ and $\alpha \in M$, we have $\mu^K_{\sigma(\alpha)} = \mu^K_\alpha$;

(b) for any $\alpha, \beta \in M$ with $\mu^K_\alpha = \mu^K_\beta$, there exists $\tau \in \mathrm{Gal}(M : K)$ such that $\tau(\alpha) = \beta$.

12 Galois Groups II

Lemma 12.1. Suppose that $L : K$ is a normal extension with $K \subseteq L \subseteq \overline{K}$. Then for any K-homomorphism $\tau : L \to \overline{K}$, we have $\tau(L) = L$.

Lemma 12.2. For $n \geq 2$, S_n is generated by

1. transpositions (ij);
2. transpositions $(1i)$;
3. adjacent transpositions $(12), (23), \ldots, (n-1, n)$;
4. (12) and $(12 \ldots n)$;
5. (12) and $(23 \ldots n)$;
6. (ij) and $(i \ldots i_p)$ where p is prime.

Lemma 12.3. Let $(i_1 \ldots i_k) \in S_n$. Then for all $\sigma \in S_n$, one has $\sigma(i_1 \ldots i_k)\sigma^{-1} = (\sigma(i_1) \ldots \sigma(i_k))$.

Note: $|Gal_K(f)| = [L : K]$ where $L : K$ is a splitting field extension for f.

13 Galois Groups III

Theorem 13.1 (Kronecker)**.** Let $p \geq 3$ be a prime and $f \in \mathbb{Q}[x]$ be irreducible over $\mathbb{Q}$ with $\deg f = p$. If the equation $f(x) = 0$ is solvable by radicals, then the number of real roots of f is 1 or p.

Lemma 13.2. Let p be prime and $G \leqslant S_p$ such that G acts transitively on $\{1, \ldots, p\}$. Then G contains a cycle of order p.

Theorem 13.3. If $L : K$ is a finite extension, then $|\mathrm{Gal}_K(L)| \leq [L : K]$.

14 Separability

Lemma 14.1. Suppose that $L : M : K$ is a tower of algebraic field extensions. Assume that $K \subseteq M \subseteq L \subseteq \overline{K}$, and suppose that $f \in K[t] \setminus K$ satisfies the property that f is separable over K. If $g \in M[t] \setminus M$ has the property that $g \mid f$, then g is separable over M. Thus, if $\alpha \in L$ is separable over K then α is separable over M, and if $L : K$ is separable then so is $L : M$.

Lemma 14.2.

1. If $L : M$ is an algebraic field extension, $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism, then $\sigma(\mu^M_\alpha)$ is separable over $\sigma(M) \iff \mu^M_\alpha$ is separable over M.
2. If $L : K$ is a splitting field extension for $f \in K[t]$ and f is separable over K, then $L : K$ is separable.

Theorem 14.3. Let $L : K$ be a finite extension with $K \subseteq L \subseteq \overline{K}$, whence $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$. Put $K_0 = K$, and for $1 \leq i \leq n$, set $K_i = K_{i-1}(\alpha_i)$. Finally, let $\sigma_0 : K \to \overline{K}$ be the inclusion map.

(i) If α_i is separable over K_{i-1} for $1 \leq i \leq n$, then there are $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.

(ii) If α_i is not separable over K_{i-1} for some i with $1 \leq i \leq n$, then there are fewer than $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.

Theorem 14.4. Let $L : K$ be a finite extension with $L = K(\alpha_1, \ldots, \alpha_n)$. Set $K_0 = K$, and for $1 \leq i \leq n$, inductively define K_i by putting $K_i = K_{i-1}(\alpha_i)$. Then the following are equivalent:

(i) the element α_i is separable over K_{i-1} for $1 \leq i \leq n$;

(ii) the element α_i is separable over K for $1 \leq i \leq n$;

(iii) the extension $L : K$ is separable.

Corollary 14.5. Suppose that $L : K$ is a finite extension. If $L : K$ is a separable extension, then the number of K-homomorphism $\sigma : L \to \overline{K}$ is $[L : K]$, and otherwise the number is smaller than $[L : K]$.

Corollary 14.6. Suppose that $f \in K[t] \setminus K$ and that $L : K$ is a splitting field extension for f. Then $L : K$ is a separable extension $\iff$ f is separable over K.

15 The Primitive Element Theorem

Theorem 15.1 (The Primitive Element Theorem)**.** If $L : K$ is a finite, separable extension with $K \subseteq L$, then $L : K$ is a simple extension.

Corollary 15.2. Suppose that $L : K$ is an algebraic, separable extension, and suppose that for every $\alpha \in L$, the polynomial μ_α^K has degree at most n over K. Then $[L : K] \leq n$.

Fact: Let $L : K$ be a normal extension and let $\deg(\mu_\alpha^K) \leq n$ for all $\alpha \in L$. Then $[L : K] \leq n$.

16 Galois Fields I

Definition 16.1 (Formal derivative)**.** We define the *derivative operator* $\mathcal{D} : K[t] \to K[t]$ by

$$\mathcal{D}\left(\sum_{k=0}^{n} a_k t^k\right) = \sum_{k=1}^{n} k a_k t^{k-1}.$$

Theorem 16.2. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f with $K \subseteq L$. Then the following are equivalent:

(i) f has a repeated root over L;

(ii) There exists $\alpha \in L$ such that $f(\alpha) = 0 = (\mathcal{D}f)(\alpha)$;

(iii) There exists $g \in K[t]$ with $\deg g \geq 1$ such that $g \mid f$ and $g \mid \mathcal{D}f$.

Definition 16.3 (Inseparable)**.** A polynomial $f \in K[t]$ is *inseparable over* K if f is not separable over K, i.e. f has an irreducible factor $g \in K[t]$ such that g has fewer than $\deg g$ distinct roots in K.

Theorem 16.4. Suppose $f \in K[t]$ is irreducible over K. Then f is inseparable over $K \iff \operatorname{char} K = p > 0$ and $f \in K[t^p]$.

Definition 16.5 (Frobenius map)**.** Suppose that $\operatorname{char} K = p > 0$. The *Frobenius map* $\varphi : K \to K$ is defined by $\varphi(\alpha) = \alpha^p$.

Theorem 16.6. Suppose that $\operatorname{char} K = p > 0$, and put $F = \{c \cdot 1_K : c \in \mathbb{Z}\}$. Then F is a subfield (called the prime subfield) of K, and $F \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 16.7 (Fixed field)**.** Let $L : K$ be a field extension and $G \leqslant \operatorname{Aut}(L)$. We define the *fixed field of* G as

$$\operatorname{Fix}_L(G) = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Theorem 16.8. Suppose that $\operatorname{char} K = p > 0$, and let F be the prime subfield of K. Let $\varphi : K \to K$ denote the Frobenius map. Then φ is an injective homomorphism, and $\operatorname{Fix}_\varphi(K) = F$.

Corollary 16.9. Suppose that $\operatorname{char} K = p > 0$ and K is algebraic over its prime subfield. Then the Frobenius map is an automorphism of K.

Corollary 16.10. Suppose that $\operatorname{char} K = p > 0$ and K is algebraic over its prime subfield. Then all polynomials in $K[t]$ are separable over K.

Corollary 16.11 (**)**.** Suppose that $\operatorname{char} K = 0$. Then all polynomials in $K[t]$ are separable over K.

Theorem 16.12. Suppose that $\operatorname{char} K = p > 0$. Let

$$f(t) = g(t^p) = a_0 + a_1 t^p + \cdots + a_{n-1} t^{(n-1)p} + t^{np}$$

be a non-constant monic polynomial over K. Then $f(t)$ is irreducible in $K[t]$ if and only if $g(t)$ is irreducible in $K[t]$ and not all the coefficients a_i are p-th powers in K.

17 Galois Fields II

Theorem 17.1. Let p be a prime, and let $q = p^n$ for some $n \in \mathbb{N}$. Then:

(a) There exists a field $\mathbb{F}_q$ of order q, and this field is unique up to isomorphism.

(b) All elements of $\mathbb{F}_q$ satisfy the equation $t^q = t$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $t^q - t$.

(c) There is a unique copy of $\mathbb{F}_q$ inside any algebraically closed field containing $\mathbb{F}_p$.

Theorem 17.2. Let p be a prime, and suppose that $q = p^n$ for some $n \in \mathbb{N}$. Then:

(a) $\operatorname{Gal}(\mathbb{F}_q : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$;

(b) The field $\mathbb{F}_q$ contains a subfield of order p^d if and only if $d \mid n$. When $d \mid n$, moreover, there is a unique subfield of $\mathbb{F}_q$ of order p^d.

Definition 17.3 (Norm, Trace)**.** Let p be a prime and let $\alpha \in F_q$ where $q = p^n$ for some $n \in \mathbb{N}$. Then we define

$$\begin{aligned} \operatorname{Tr}(\alpha) &= \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} \\ &= \alpha + \varphi(\alpha) + \cdots + \varphi^{n-1}(\alpha) \end{aligned}$$

and

$$\begin{aligned} \operatorname{Norm}(\alpha) &= \alpha \cdot \alpha^p \cdots \alpha^{p^{n-1}} = \alpha^{\frac{p^n-1}{p-1}} \\ &= \alpha \cdot \varphi(\alpha) \cdots \varphi^{n-1}(\alpha) \end{aligned}$$

Lemma 17.4. Let p be a prime and let $\alpha \in F_q$ where $q = p^n$ for some $n \in \mathbb{N}$.

1. For all $\alpha \in \mathbb{F}_q$, one has $\operatorname{Tr}(\alpha), \operatorname{Norm}(\alpha) \in \mathbb{F}_p$;
2. If $p \neq 2$, then $\exists \alpha_1$ such that $\operatorname{Tr}(\alpha_1) \neq 0$ and $\exists \alpha_2 (\neq 0)$ such that $\operatorname{Norm}(\alpha_2) \neq 1$.

18 Fixed Fields

Definition 18.1 (Fixed field)**.** Let $L : K$ be a field extension and $G \leqslant \mathrm{Aut}(L)$. Then the *fixed field* of G is

$$\mathrm{Fix}_L(G) = L^G = \{\alpha \in L : g\alpha = \alpha \ \forall g \in G\}$$

Theorem 18.2. Let $K, M \subseteq L$ be fields and $G, H \leqslant \mathrm{Aut}(L)$. Then

1) if $K \subseteq M$, then $\mathrm{Gal}(L : K) \geqslant \mathrm{Gal}(L : M)$;
2) if $G \leqslant H$, then $\mathrm{Fix}_L(G) \supseteq \mathrm{Fix}_L(H)$;
3) $K \subseteq \mathrm{Fix}_L(\mathrm{Gal}(L : K))$;
4) $G \leqslant \mathrm{Gal}(L : \mathrm{Fix}_L(G))$;
5) $\mathrm{Gal}(L : K) = \mathrm{Gal}(L : \mathrm{Fix}_L(\mathrm{Gal}(L : K)))$;
6) $\mathrm{Fix}_L(G) = \mathrm{Fix}_L(\mathrm{Gal}(L : \mathrm{Fix}_L(G)))$.

Definition 18.3 (Galois Extension)**.** Let $L : K$ be a field extension. Then $L : K$ is a *Galois extension* if it is normal and separable.

Theorem 18.4. Let $L : K$ be algebraic. Then $L : K$ is Galois $\iff K = \mathrm{Fix}_L(\mathrm{Gal}_K(L))$

Theorem 18.5. Suppose that L is a field, $G \leqslant \mathrm{Aut}(L)$ such that $|G| < \infty$, and put $K = \mathrm{Fix}_L(G)$. Then $L : K$ is a finite Galois extension with $[L : K] = |\mathrm{Gal}(L : K)|$, and furthermore $G = \mathrm{Gal}_K(L)$.

Theorem 18.6. Let $L : K$ be finite.

1. If $L : K$ is a Galois extension, then $|\mathrm{Gal}(L : K)| = [L : K]$ and $K = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$.
2. If $L : K$ is not Galois, then $|\mathrm{Gal}(L : K)| < [L : K]$ and K is a proper subfield of $\mathrm{Fix}_L(\mathrm{Gal}(L : K))$.

Corollary 18.7. Let $L : M : K$ be a tower such that $L : K$ is Galois. Then $L : M$ is Galois.

19 Fundamental Theorem of Galois Theory I

Theorem 19.1 (Fundamental Theorem of Galois Theory, Part 1)**.** Let $L : K$ be a Galois extension with $G = \mathrm{Gal}(L : K)$. Define $\mathcal{I}(K, L)$ and $\mathcal{S}(G)$ as the set of all intermediate fields of $L : K$ and the set of all subgroups of G, respectively. For all $P \in \mathcal{I}(K, L)$, we have $P = L^{G_P}$ where $G_P = \mathrm{Aut}_P(L)$ Then

$$\begin{aligned} \forall P \in \mathcal{I}(K, L), &\quad L^{G_P} = P, \\ \forall H \in \mathcal{S}(G), &\quad G_{L^H} = H, \end{aligned}$$

Also, $P_1 \subseteq P_2 \iff G_{P_1} \geqslant G_{P_2}$ and $H_1 \leqslant H_2 \iff L^{H_1} \supseteq L^{H_2}$.

20 Fundamental Theorem of Galois Theory II

Theorem 20.1 (Fundamental Theorem of Galois Theory, Part 2)**.** For all $P \in \mathcal{I}(K, L)$, we have $P : K$ is a normal extension $\iff G_P \lhd G$. Then, $\mathrm{Gal}_K P \cong G/G_P$.

Lemma 20.2. Let $K - P - L$ be a tower of fields and $g \in \mathrm{Aut}\, L$. Then $G_{gP} = gG_Pg^{-1}$.

Remark 20.3. Let $L : P : K$ be a tower of fields, where $[L : K] = [L : P]\,[P : K]$. Then Id. $: G_P : G$ is a tower of groups, where $[G : G_P] \cdot |G_P|$. That is, for all $P \leqslant L$ we have $[P : K] = [G : G_P]$ and $[L : P] = |G_P|$.

21 Composita

Remark 21.1. Let A, B be sets. Then $A \cap B$ can be expressed using only the operation $\subseteq$. Notice $A \cap B \subseteq A, B$ and $A \cap B$ is the maximal set with this property:

$$\forall C \text{ such that } C \subseteq A, B \quad \Longrightarrow \quad C \subseteq A \cap B.$$

Let $H_1, H_2 \leqslant G$. Then $H_1 \cap H_2 \leqslant G$ is the *maximal* subgroup contained in both H_1 and H_2. Hence by the Galois correspondence we have $L^{H_1 \cap H_2}$ is the *minimal* subfield of L containing both L^{H_1} and L^{H_2}.

Definition 21.2 (Compositum)**.** Let K_1 and K_2 be fields contained in some field L. The *compositum* of K_1 and K_2 in L (or the *composite field*), denoted by K_1K_2, is the smallest subfield of L containing both K_1 and K_2.

Lemma 21.3. Let $K, E, F \subseteq L$. Then

1. $E : K,\ F : K$ finite $\Longrightarrow$ $EF : K$ finite;
2. $E : K,\ F : K$ normal $\Longrightarrow$ $E \cap F : K$ normal;
3. $E : K,\ F : K$ finite and $E : K$ normal $\Longrightarrow$ $EF : F$ normal;
4. $E : K,\ F : K$ finite and normal $\Longrightarrow$ $EF : K,\ E \cap F : K$ normal;
5. $E : K,\ F : K$ normal $\Longrightarrow$ $EF : E \cap F$ normal.

22 Soluble Groups I

Definition 22.1 (Soluble group)**.** A group G is *soluble* if there exists a finite series of subgroups

$$\{Id.\} = G_n \leqslant G_{n-1} \leqslant \cdots \leqslant G_0 = G$$

such that

1. $G_j \lhd G_{j-1}$ $\forall 1 \leq j \leq n$ and
2. G_{j-1}/G_j is cyclic $\forall 1 \leq j \leq n$.

Definition 22.2 (Simple group)**.** A group G is *simple* if G has no non-trival normal subgroups.

Lemma 22.3. For $n \geq 5$ the group A_n is simple (and hence not soluble).

Lemma 22.4. Let G be a group with $H \trianglelefteq G$ and $A \leqslant G$. Then

1. $(A \cap H) \trianglelefteq A$ and $A/(A \cap H) \cong (HA)/H$
2. if $H \subseteq A$ and $A \trianglelefteq G$, then $H \trianglelefteq A$, $(A/H) \trianglelefteq (G/H)$ and $(G/H)/(A/H) \cong G/A$.

Theorem 22.5.
1. If G is a soluble group with $A \leqslant G$, then A is soluble.
2. Let $H \trianglelefteq G$. Then G is soluble $\Longleftrightarrow$ H and G/H are soluble.

Corollary 22.6. S_n is not soluble for $n \geq 5$.

Corollary 22.7. All p-groups are soluble (i.e. groups G such that $|G| = p^n$ for some prime p)

23 Soluble Groups II

Theorem 23.1 (Theorem - Definition)**.** Let G be a group. Then the following are equivalent:

0. G is a (finite) soluble group;
1. There exists some $n \in \mathbb{Z}^+$ such that $G^{(n)} = \{e\}$;

2. There exists a normal series

$$\{Id.\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

   such that all quotients G_{j-1}/G_j are abelian;

3. There exists a subnormal series such that quotients G_{j-1}/G_j are abelian.

Definition 23.2 (Derived group)**.** Let G be a group. Then the *derivative of* G is $G' = \langle [x, y] : x, y \in G \rangle = [G, G]$ where $[x, y] = xyx^{-1}y^{-1}$ is the *commutator* of x and y, and $(G')' = G''$.

Definition 23.3 (Derived series)**.** The *derived series* of G is $G^{(n)} = \left(G^{(n-1)}\right)'$ and $\{\text{Id.}\} = G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G' \lhd G$ (not to be confused with $G_{n+1} = [G_n, G]$, the *lower central series*).

Lemma 23.4. Let $\varphi : G \mapsto H$ be an epimorphism. Then $\varphi(G') = H'$.

Definition 23.5 (Composition series)**.** Let G be a group. Then a *composition series* of G is a subnormal series of finite length

$$\{Id.\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{\ell-1} \lhd G_\ell = G$$

such that G_j/G_{j-1} is a simple group for all j.

Theorem 23.6 (Jordan-Hölder)**.** Any 2 composition series of some group G are equivalent up to permutation and isomorphism.

Theorem 23.7. Let K be a field with $\operatorname{char} K \neq 2$ and let $f \in K[t]$ be a separable polynomial with splitting field L. Then $f = 0$ is solvable by *quadratic* radicals $\iff [L : K] = 2^t$.

24 Solvability by radicals and Galois theory I

Theorem 24.1. Let K be a field with $\operatorname{char} K = 0$. Then $f \in K[t]$ is solvable by radicals $\iff \operatorname{Gal}_K(f)$ is soluble.

Lemma 24.2. Let $\operatorname{char} K = 0$ and $R : K$ be a radical extension. Then there exists a tower $K - R - N$ such that $N : K$ is normal and radical.

Definition 24.3 (Cyclic extension)**.** Let L be the splitting field of some polynomial f over K. If $\operatorname{Gal}(L : K)$ is a cyclic group, then $L : K$ is a *cyclic* extension.

Lemma 24.4. Let $\operatorname{char} K = 0$ and let n be a positive integer such that $t^n - 1$ splits over K, and let $L : K$ be the splitting field extension for $t^n - a$ for some $a \in K$. Then $\operatorname{Gal}(L : K)$ is abelian.

Theorem 24.5. Let $\operatorname{char} K = 0$ and $L : K$ be Galois. Suppose there exists some extension $M : L$ such that $M : K$ is normal. Then $\operatorname{Gal}(L : K)$ is soluble.

Corollary 24.6. Let $\operatorname{char} K = 0$. Then $f \in K[t]$ is SBR $\implies \operatorname{Gal}_K(f)$ is soluble.

25 Solvability by radicals and Galois theory II

Lemma 25.1. Let p be prime and $G \leqslant S_p$ such that G acts transitivley on $\{1, \ldots, p\}$. Then G contains a cycle of order p.

Theorem 25.2. Let $\operatorname{char} K = 0$ and $f \in K[t] \setminus K$. Then $\operatorname{Gal}_K(f)$ is soluble $\implies f$ is SBR.

Lemma 25.3 (Wooley 14.8)**.** Let $\operatorname{char} K = 0$, and suppose that $L : K$ is a cyclic extension of degree n. Suppose also that K contains a primitive n-th root of 1. Then there exists $\theta \in K$ having the property that $t^n - \theta$ is irreducible over K, and $L : K$ is a splitting field for $t^n - \theta$. Further, if β is a root of $t^n - \theta$ over L, then $L = K(\beta)$.

Theorem 25.4 (Abel-Galois)**.** Let $\operatorname{char} K = 0$ and $f \in K[t]$ be irreducible over K with $\deg f = p$. Then following are equivalent

1. f is SBR over K;
2. $\mathrm{Gal}_K(f)$ is conjugated to a subgroup of $\mathrm{Aff}(\mathbb{F}_p)$;
3. for the splitting field L of f, one has $L = K(\alpha_i, \alpha_j)$ where α_i, α_j are any two destinct roots of f.

Lemma 25.5. Let $\{\mathrm{Id.}\} \neq N \trianglelefteq G \leqslant S_p$ for p prime. If G is a transitive group, then N is a transitive group.

26 Final remarks I

Definition 26.1 (Sylvester matrix)**.** Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ be two polynomials in $\mathbb{K}[x]$. The *Sylvester matrix* $S(f, g)$ is the $(m+n) \times (m+n)$ matrix whose first n rows are the coefficients of f shifted right, and whose last m rows are the coefficients of g shifted right. Concretely,

$$S(f,g) = \begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix}.$$

Definition 26.2 (Resultant)**.** With notation as above, the *resultant* of f and g is

$$R(f,g) = \det\left(S(f,g)\right).$$

Equivalently, if $\alpha_1, \ldots, \alpha_m$ are the roots of f in an algebraic closure of $\mathbb{K}$, then

$$R(f,g) = a_m^n \prod_{i=1}^{m} g(\alpha_i).$$

Theorem 26.3. Let α_i be roots of f and β_j be roots of g. Then

$$\begin{aligned} R(f,g) &= a_0^m b_0^n \prod_i (\alpha_i - \beta_j) \\ &= a_0^m \prod_i g(\alpha_i) = b_0^n \prod_i f(\beta_i) \end{aligned}$$

Corollary 26.4.
1. $R(f,g) = (-1)^{\deg f \cdot \deg g} R(g,f)$
2. If $f = gq + r \implies R(f,g) = b_0^{\deg f - \deg R} R(r,g)$
3. $R(f,gh) = R(f,g)R(f,h)$

Corollary 26.5. Let $f(t) = a_0 t^n + \cdots + a_n,\ a_0 \neq 0$. Then $R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2$

27 Final remarks II

Definition 27.1 (Resolvent invariant)**.** Let $G \leqslant S_n$ and $P \in K[x_1, \ldots, x_n]$. Then P is *resolvent invariant* for G if $P^g = P \iff g \in G$.

Lemma 27.2. Let P be resolvent invariant for G. Then

1. $P^a = P^b \iff ab^{-1} \in G$ (obvious: $P^a = P^b \iff P^{ab^{-1}} = P$)
2. P^a is resolvent invariant for $a^{-1}Ga$

Corollary 27.3. Let $S_n = \sqcup_j a_j G$. Then P is resolvent invariant for $G \iff P^{a_j}$ are distinct.

Definition 27.4 (Resolvent)**.** Let P be a resolvent polynomial for $G \leqslant S_n$ and $S_n = \sqcup_{j=1}^s a_j G$. Then

$$R_G(z) = R_G(z, x_1, \ldots, x_n) = (z - P^{a_1}) \cdots (z - P^{a_s})$$

is a *resolvent* for G (depends on P).

Lemma 27.5. Let $G \leqslant S_n$, $f \in K[t]$ be a separable polynomial. If $\mathrm{Gal}_K(f) \leqslant G$ (and its conjugation), then $\exists \jmath \in K$ such that $R_{G,f}(\jmath) = 0$

Lemma 27.6. Let $|K| = \infty$ and $f \in K[t]$ be a separable polynomial. Then $\exists c_1, \ldots, c_n \in K$ such that for all k,

$$h_k(x_1, \ldots, x_k) = c_1 x_1 + \cdots + c_k x_k$$

has the property

$$h_k^a(\alpha_1, \ldots, \alpha_k) = h_k^b(\alpha_1, \ldots, \alpha_k) \iff x_i^a = x_i^b \text{for} i = 1, \ldots, k,$$

where $a, b \in S_n$ are any permutations.

Theorem 27.7. Let $|K| = \infty$, $f \in K[t]$ be a separable polynomial, and $G \leqslant S_n$. Then there exists a resultant $R_{G,f}(z)$ with no multiple roots.

Theorem 27.8. Let $|K| = \infty$ and $f \in K[t]$ be irreducible and separable with $\deg f = 4$. Then

1. $\sqrt{D} \notin K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong S_4$ or $G \cong Z_4$
2. $\sqrt{D} \in K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong A_4$
3. $\sqrt{D} \in K$ and $R_{V_4}^{(f)}$ has a roots in $K \implies G \cong V_4$
4. $\sqrt{D} \notin K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong S_4$ or $G \cong D_4$

Exercise, the point is to show that computing each $R_{V_4, D_4, Z_4, A_4}^{(f)}$ is not necessary