

# MA 45401-H01: Galois Theory Honors

## Definitions and Results

Prof. Ilya Shkredov  
Transcribed by Josh Park

Last updated May 7, 2025

### Contents

<b>1</b>	<b>Introduction I</b>	<b>2</b>
<b>2</b>	<b>Introduction II</b>	<b>3</b>
<b>3</b>	<b>Field Extensions I</b>	<b>4</b>
<b>4</b>	<b>Field Extensions II</b>	<b>5</b>
<b>5</b>	<b>Algebraic Conjugates</b>	<b>6</b>
<b>6</b>	<b>Ruler and Compass Constructions</b>	<b>6</b>
<b>7</b>	<b>Cyclotomic Polynomials</b>	<b>7</b>
<b>8</b>	<b>Splitting Fields, Abel-Ruffini</b>	<b>7</b>
<b>9</b>	<b>Algebraic Closure I</b>	<b>8</b>
<b>10</b>	<b>Algebraic Closure II</b>	<b>9</b>
<b>11</b>	<b>Galois Groups I</b>	<b>10</b>
<b>12</b>	<b>Galois Groups II</b>	<b>10</b>
<b>13</b>	<b>Galois Groups III</b>	<b>10</b>
<b>14</b>	<b>Separability</b>	<b>11</b>
<b>15</b>	<b>The Primitive Element Theorem</b>	<b>11</b>
<b>16</b>	<b>Galois Fields I</b>	<b>12</b>
<b>17</b>	<b>Galois Fields II</b>	<b>12</b>
<b>19</b>	<b>Fixed Fields</b>	<b>13</b>
<b>20</b>	<b>Fundamental Theorem of Galois Theory I</b>	<b>14</b>
<b>21</b>	<b>Fundamental Theorem of Galois Theory II</b>	<b>14</b>

22	Composita	14
23	Soluble Groups I	14
24	Soluble Groups II	15
25	Solvability by radicals and Galois theory I	15
26	Solvability by radicals and Galois theory II	16
27	Final remarks I	16
28	Final remarks II	17

## 1 Introduction I

**Definition 1** (Symmetric function). A function  $\varphi(x_1, \dots, x_n)$  is called *symmetric* if

$$\varphi(x_1, \dots, x_n) = \varphi(x_{\omega(1)}, \dots, x_{\omega(n)})$$

for all  $\omega \in S_n$ .

**Definition 2** (Elementary symmetric polynomial).

$$\begin{aligned} \sigma_1 &= \sigma_1(x_1, \dots, x_n) = x_1 + \dots + x_n \\ \sigma_2 &= \sigma_2(x_1, \dots, x_n) = x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_{n-1}x_n \\ &\vdots \\ \sigma_k &= \sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k} \\ &\vdots \\ \sigma_n &= \sigma_n(x_1, \dots, x_n) = \prod_{i=1}^n x_i \end{aligned}$$

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

**Definition 3** (Vieta formulae). Suppose  $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$  has roots  $r_1, \dots, r_n$ . Then,

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

**Corollary 1.** The discriminant  $D$  of  $f \in R[x]$ , where  $R$  is a ring and  $f = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ , is a polynomial in  $a_1, \dots, a_n$  and coefficients from  $R$  (i.e.  $D \in R[a_1, \dots, a_n]$ ).

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

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

**Vieta's method:** Using the trigonometric formula  $\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi$ , 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  $\cos : \mathbb{C} \rightarrow \mathbb{C}$  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 4** (Ferrari resolvent). Let  $f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$  be a quartic polynomial over a field  $K$  of characteristic not 2. We define the *Ferrari resolvent* of  $f$  to be the associated cubic resolvent polynomial  $R(z) \in K[z]$  given by

$$R(z) = z^3 - 2bz^2 + (b^2 - 4d + ac)z - c^2 - a^2d + 4bd.$$

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

**Lagrange's method:** Suppose  $f(x) = x^3 + px + q$  is a depressed cubic with roots  $x_1, x_2, x_3$ . *Lagrange's method* finds expressions involving the roots that take only a few values under permutation, then uses symmetry to connect them to the coefficients.

For instance, define

$$y_1 = x_1 + \zeta x_2 + \zeta^2 x_3,$$

where  $\zeta = e^{2\pi i/3}$  is a primitive cube root of unity. Then define

$$y_2 = x_1 + \zeta^2 x_2 + \zeta x_3.$$

These expressions are not symmetric, but they only take a few values when the  $x_i$ 's are permuted. In particular,  $y_1^3$  and  $y_2^3$  are symmetric functions of the roots and thus can be written as polynomials in  $p$  and  $q$ .

Since the roots  $x_i$  are related to  $y_1$  and  $y_2$ , we can use symmetric combinations such as

$$x = \frac{1}{3}(y_1 + y_2)$$

to recover the original roots of  $f(x)$ .

## 2 Introduction II

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

$$\text{orb}(\varphi) = \{\varphi^\omega = \varphi(x_{\omega(1)}, \dots, x_{\omega(n)}) \mid \omega \in S_n\}.$$

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

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

**Definition 5** (Group action). Let  $G$  be a group and  $X$  be a set. The (left) group action of  $G$  on  $X$  is the map  $\cdot : G \times X \rightarrow X$  such that

1.  $e_G \cdot x = x, \quad \forall x \in X$
2.  $g \cdot (h \cdot x) = (g \cdot h) \cdot x, \quad \forall x \in X, \forall g, h \in G$

**Definition 6** (Orbit). Let  $G$  be a group,  $X$  be a set, and  $x \in X$ . Then we define *the orbit* of  $x$ ,  $G \cdot x = \text{orb}(x)$ , as  $\{g \cdot x \mid g \in G\}$ . Moreover,  $\text{orb}(x) \subseteq X$ .

**Definition 7** (Stabilizer). Let  $G$  be a group,  $X$  be a set, and  $x \in X$ . Then we define *the stabilizer* of  $x$ ,  $\text{stab}(x)$ , as  $\{g \in G \mid g \cdot x = x\}$ . Moreover,  $\text{stab}(x) \leq G$ .

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

**Definition 8** (Polynomial ring). Let  $R$  be a commutative ring. Then the ring of polynomials with coefficients in  $R$  is

$$R[t] = \left\{ \sum_{i=0}^n c_i t^i : n \in \mathbb{Z}_+, c_i \in R \right\}$$

### 3 Field Extensions I

**Definition 9** (Integral domain). Let  $R$  be a commutative ring. Then  $R$  is an *integral domain* if  $ab = 0$  implies that  $a = 0$  or  $b = 0$  for all  $a, b \in R$ .

**Definition 10** (Euclidean domain). Let  $R$  be an integral domain. Then  $R$  is a *Euclidean domain* if there exists some function  $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  such that for all  $a, b \neq 0 \in R$ , there exist elements  $q, r \in R$  such that  $a = qb + r$  where  $r = 0$  or  $f(r) < f(b)$ .

**Theorem 3.1** (Bézout's Identity). Let  $R$  be a Euclidean domain. For  $a, b \in R$ , there exists  $\alpha, \beta \in R$  such that  $\gcd(a, b) = \alpha a + \beta b$ .

**Definition 11** (Irreducible). Let  $F$  be a field, and  $f \in F[t] \setminus F$ . Then  $f$  is *irreducible* if  $\nexists g, h \in F[t] \setminus F$  of strictly smaller degree such that  $f = gh$ .

**Definition 12** (Unique factorization domain). Let  $R$  be an integral domain. Then  $R$  is a *unique factorization domain* (UFD) if for irreducible  $p_i \in R$ , any nonzero  $x \in R$  can be written uniquely (up to ordering) as  $x = p_1 p_2 \cdots p_k$ ,  $k \geq 1$ .

**Fact:** If  $R$  is an Euclidean domain, then  $R$  is a UFD (and PID)

**Corollary 2.** Let  $f \in \mathbb{F}[t]$  be a monic polynomial with  $\deg f \geq 1$ . Then we can write  $f = f_1 f_2 \cdots f_k$  uniquely (up to ordering) for irreducible monic polynomials  $f_j$ .

**Definition 13.** Let  $R$  be a UFD. When  $a_0, \dots, a_n \in R$  are not all 0, we can generalize the *greatest common divisor* of  $a_0, \dots, a_n$  (written  $\gcd(a_0, \dots, a_n)$ ) any element  $c \in R$  satisfying

- (i)  $c \mid a_i$  ( $0 \leq i \leq n$ ), and
- (ii) if  $d \mid a_i$  ( $0 \leq i \leq n$ ), then  $d \mid c$ .

When  $f = \sum_{j=0}^d a_j x^j \in R[x]$  is a non-zero polynomial, we define a *content* of  $f$  to be any  $\gcd(a_0, \dots, a_d)$  and  $\gcd(f) = \gcd(a_0, \dots, a_d)$ . We say that  $f \in R[X]$  is *primitive* if  $f \neq 0$  and the content of  $f$  is divisible only by units of  $R$ .

**Lemma 3.2** (Gauss).  $\gcd(fg) = \gcd f \cdot \gcd g$

**Corollary 3.**  $f \in \mathbb{Z}[t]$  is irreducible  $\iff f$  is irreducible over  $\mathbb{Q}[t]$

**Corollary 4.** 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 3.3** (Eisenstein's Criterion). Let  $R$  be a UFD with field of fractions  $Q$  and let  $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$  with  $\gcd(f) = 1$ . Suppose there exists an irreducible element  $p \in R$  such that

- (i)  $p \mid a_i$  for  $0 \leq i < n$ ,
- (ii)  $p^2 \nmid a_0$ , and
- (iii)  $p \nmid a_n$ ,

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

**Definition 14** (Field extension). Let  $L$  and  $K$  be fields. Then  $L$  is an *extension* of  $K$  if there exists a homomorphism  $\varphi : K \rightarrow L$ . Then we write  $L : K$  or  $L/K$ ,  $\varphi(K) \cong K$  and identify  $\varphi(K)$  with  $K$ .

**Fact:** Suppose that  $L$  is a field extension of  $K$  with associated embedding  $\varphi : K \rightarrow L$ . Then  $L$  forms a vector space over  $K$ , under the operations

$$\begin{aligned} & \text{(vector addition)} \quad \psi : L \times L \rightarrow L \quad \text{given by} \quad (v_1, v_2) \mapsto v_1 + v_2 \\ & \text{(scalar multiplication)} \quad \tau : K \times L \rightarrow L \quad \text{given by} \quad (k, v) \mapsto \varphi(k)v. \end{aligned}$$

**Definition 15** (Degree, finite extension). Let  $L : K$ . Then the *degree* of  $L : K$  is  $[L : K] = \dim L$  over  $K$  as a vector space. We say that  $L : K$  is a *finite extension* if  $[L : K] < \infty$ .

**Definition 16** (Tower, intermediate field). We say that  $M : L : K$  is a *tower* of field extensions if  $M : L$  and  $L : K$  are field extensions, and in this case we say that  $L$  is an *intermediate field* (relative to the extension  $M : K$ ).

**Theorem 3.4** (The Tower Law). Suppose that  $M : L : K$  is a tower of field extensions. Then  $M : K$  is a field extension, and  $[M : K] = [M : L][L : K]$ .

**Corollary 5.** Suppose that  $L : K$  is a field extension for which  $[L : K]$  is a prime number. Then whenever  $L : M : K$  is a tower of field extensions with  $K \subseteq M \subseteq L$ , one has either  $M = L$  or  $M = K$ .

## 4 Field Extensions II

**Definition 17** (Smallest subring/subfield). Let  $L : K$  with  $K \subseteq L$ .

- (i) When  $\alpha \in L$ , we denote by  $K[\alpha]$  the *smallest subring of  $L$  containing  $K$  and  $\alpha$* , and by  $K(\alpha)$  the *smallest subfield of  $L$  containing  $K$  and  $\alpha$* ;
- (ii) More generally, when  $A \subseteq L$ , we denote by  $K[A]$  the *smallest subring of  $L$  containing  $K$  and  $A$* , and by  $K(A)$  the *smallest subfield of  $L$  containing  $K$  and  $A$* .

Then

$$\begin{aligned} K[\alpha] &= \left\{ \sum_{i=0}^d c_i \alpha^i : d \in \mathbb{Z}_{\geq 0}, c_0, \dots, c_d \in K \right\} \\ K(\alpha) &= \{f/g : f, g \in K[\alpha], g \neq 0\}. \end{aligned}$$

**Definition 18** (Algebraic/transcendental element). Suppose that  $L : K$  is a field extension with  $K \subseteq L$  and  $\alpha \in L$ .

- (i) We say  $\alpha$  is *algebraic over  $K$*  if  $\exists f_{\neq 0} \in K[t]$  such that  $f(\alpha) = 0$ .
- (ii) If  $\alpha$  is not algebraic over  $K$ , then we say  $\alpha$  is *transcendental over  $K$* .
- (iii) When every element of  $L$  is algebraic over  $K$ , we say that  $L$  is *algebraic over  $K$* .

**Definition 19** (Evaluation map). Suppose that  $L : K$  is a field extension with  $K \subseteq L$ , and that  $\alpha \in L$ . We define the *evaluation map*  $E_\alpha : K[t] \rightarrow L$  by putting  $E_\alpha(f) = f(\alpha)$  for each  $f \in K[t]$ .

**Definition 20** (Minimal polynomial). Suppose that  $L : K$  is a field extension with  $K \subseteq L$ , and suppose that  $\alpha \in L$  is algebraic over  $K$ . Then the minimal polynomial of  $\alpha$  over  $K$  is the unique monic polynomial  $\mu_\alpha^K$  such that  $\ker(E_\alpha) = (\mu_\alpha^K)$ .

- Lemma 4.1.**
1.  $\mu_\alpha^K$  is irreducible over  $K$ ;
  2. If  $f \in K[t]$  such that  $f(\alpha) = 0$ , then  $\mu_\alpha^K \mid f$ ;
  3. If  $f \in K[t]$  such that  $f(\alpha) = 0$  and  $f$  is irreducible over  $K$ , then  $\exists k \in K$  such that  $f = k\mu_\alpha^K$ .

**Theorem 4.2.** 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  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a basis for  $K(\alpha)$  over  $K$  ( $\implies [K(\alpha) : K] = \deg \mu_\alpha^K$ ).

**Theorem 4.3** (Rational Root Theorem). Let  $\frac{p}{q}$  be a root of  $f = a_0t^n + \dots + a_{n-1}t^{n-1} + a_n$ , for  $a_j \in \mathbb{Z}$ , where  $p$  and  $q$  are coprime. Then  $p \mid a_n$  and  $q \mid a_0$ .

**Note:** If  $\alpha$  is transcendental over  $K$ , then  $K(\alpha) \cong K(x)$  (where  $x$  is a formal variable).

**Corollary 6.** Let  $L : K$  with  $K \subseteq L$ , and suppose that  $\alpha \in L$  is algebraic over  $K$ . Then every element of  $K(\alpha)$  is algebraic over  $K$ .

**Corollary 7.** Let  $L : K$  with  $K \subseteq L$ . Then  $[L : K] < \infty \iff L = K(\alpha_1, \dots, \alpha_n)$  for  $\alpha_j \in L$ .

**Theorem 4.4.** Let  $L : K$  be a field extension, and define

$$L^{\text{alg}} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then  $L^{\text{alg}}$  is a subfield of  $L$ .

## 5 Algebraic Conjugates

**Lemma 5.1.** Let  $\mathbb{F}$  be a field with  $f \in \mathbb{F}[t]$  irreducible. Then  $\mathbb{F}[t] / (f)$  is a field.

**Corollary 8.** 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  $\varphi : K[t] \rightarrow L[y]$ , such that  $L$  contains a root of  $\varphi(f)$ .

**Definition 21** (Algebraic conjugate). Suppose  $\alpha$  is algebraic over  $K$  and  $\mu_\alpha^K$  factors as a product of linear polynomials over a field  $L \supseteq K$ :

$$\mu_\alpha^K(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_1, \dots, \alpha_n \in L.$$

Then  $\alpha_1, \dots, \alpha_n$  are *algebraic conjugates* of  $\alpha$ .

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

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

## 6 Ruler and Compass Constructions

**Definition 22** (Constructible points/angles). Let  $P_0 = (0, 0)$  and  $P_1 = (1, 0)$ , and let  $\mathcal{S}_n = (P_0, \dots, P_n)$ . Then  $P_{n+1}$  is a constructible point if it is the intersection of either

1. two lines containing points in  $\mathcal{S}_n$ ;
2. two circles with centers in  $\mathcal{S}_n$ ;

3. a circle and line with center and endpoints in  $\mathcal{S}_n$ .

Similarly, an angle  $\theta$  is constructible if for some  $a \in \mathbb{R}$ , there exists some constructible point  $x$  such that  $x^2 = a^2$ .

**Lemma 6.1.** If  $n$ -gon constructible, then  $2n$ -gon is constructible.

**Lemma 6.2.** If  $a, b, c$  constructible (or polyquadratic), then  $a \pm b$ ,  $\frac{ab}{c}$ , and  $\sqrt{ab}$  constructible.

**Fact 1.** If  $m$ -gon and  $n$ -gon are constructible for coprime  $m, n$ , then  $mn$ -gon is constructible.

**Fact 2.** If  $p \geq$  prime, then  $p^k$ -gon constructible for  $k \in \mathbb{N}$ .

**Theorem 6.3** (Gauss).

$$\cos \frac{2\pi}{17} = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}}}}{16}$$

**Corollary 9.** The 17-gon is constructible.

**Corollary 10.** If  $a \in \mathbb{R}$  is constructible, then  $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$  for some  $n \geq$

**Corollary 11.** Given a cube  $C_1$  with volume  $V_1$ , it is impossible to construct a cube  $C_2$  with volume  $2V_1$  by ruler and compass. That is, the volume of a cube can not be duplicated by ruler and compass.

**Corollary 12.** An arbitrary angle cannot be trisected by ruler and compass.

**Theorem 6.4** (Gauss-Wantzel). A regular  $n$ -gon is constructible  $\iff n = 2^r \prod_{i=1}^s p_i$  for  $r \in \mathbb{Z}_{\geq 0}$  and Fermat primes  $p_i = 2^{(2^k)} + 1$  for  $k \in \mathbb{Z}_{\geq 0}$ .

**TODO:** define  $V_n$

**Lemma 6.5.** For all integers  $d$  and all  $d$ -periods  $\theta$ ,  $V_d = \mathbb{Q}(\theta)$ .

## 7 Cyclotomic Polynomials

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

**Definition 23** ( $n^{\text{th}}$  cyclotomic polynomial).

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

**Theorem 7.2.**  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .

**Corollary 13.** (a)  $[\mathbb{Q}(\exp(\frac{2\pi i}{n})) : \mathbb{Q}] = \varphi(n)$  (where  $\varphi$  is Euler's totient function);

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

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

**Lemma 7.3.** Let  $\mathbb{F}$  be a finite field. Then  $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$  is a cyclic group.

## 8 Splitting Fields, Abel-Ruffini

**Definition 24** (Splitting field). Let  $L : K$  with embedding  $\varphi : K \rightarrow L$  and  $f \in K[t] \setminus K$ . We say  $f$  splits over  $L$  if  $\varphi(f) = c \prod_{j=1}^n (x - \alpha_j)$  for  $\alpha_j \in L$  and  $c \in \varphi(K)$ . We say that  $M : K$  is a splitting field extension for  $f$  if  $f$  splits over  $L$ ,  $\varphi(K) \subseteq M \subseteq L$ , and  $M$  is the smallest subfield of  $L$  containing  $\varphi(K)$  over which  $f$  splits.

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

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

**Lemma 8.3.** Let  $L : K$  and  $M : K$  be splitting field extensions for  $f \in K[t] \setminus K$ . Then  $L \cong M$  (in particular,  $[L : K] = [M : K]$ ).

**Definition 25** (Radical, radical extension, solvability by radicals). Let  $L : K$  and  $\beta \in L$ . We say that  $\beta$  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  $n \in \mathbb{N}$ ). We say that  $L : K$  is *an extension by radicals* when there is a tower of field extensions  $L = L_r : L_{r-1} : \dots : L_0 = K$  such that  $L_i = L_{i-1}(\beta_i)$  with  $\beta_i$  radical over  $L_{i-1}$  (for  $1 \leq i \leq r$ ). We say  $f \in K[t]$  is *solvable by radicals* if there is a radical extension of  $K$  over which  $f$  splits.

**Theorem 8.4** (Abel-Ruffini). Let  $K = \mathbb{C}(a_1, \dots, a_n)$  where  $a_1, \dots, a_n$  are formal variables. Let  $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in K[x]$  be the generic polynomial of degree  $n \geq 5$  over  $K$ . Then  $f(x)$  is not solvable by radicals.

## 9 Algebraic Closure I

**Definition 26** (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 9.1.** 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 27** (Chain). Suppose that  $X$  is a nonempty, partially ordered set with  $\leq$  denoting the partial ordering. A *chain*  $C$  in  $X$  is a collection of elements  $\{a_i\}_{i \in I}$  of  $X$  such that for every  $i, j \in I$ , either  $a_i \leq a_j$  or  $a_j \leq a_i$ .

**Zorn's Lemma:** Suppose that  $X$  is a nonempty, partially ordered set with  $\leq$  the partial ordering. If every non-empty chain  $C$  in  $X$  has an upper bound in  $X$ , then  $X$  has at least one maximal element  $m$  (i.e.  $b \in X$  with  $m \leq b \implies b = m$ ).

**Corollary 14.** Any proper ideal  $A$  of a commutative ring  $R$  is contained in a maximal ideal.

**Lemma 9.2.** Let  $K$  be a field. Then there exists an algebraic extension  $E : K$ , with  $K \subseteq E$ , such that  $E$  contains a root of every irreducible  $f \in K[t]$ , and hence also every  $g \in K[t] \setminus K$ .

**Theorem 9.3** (Existence of Algebraic Closures). Suppose that  $K$  is a field. Then there exists an algebraic extension  $\overline{K}$  of  $K$  such that  $\overline{K}$  is algebraically closed.

**Definition 28** (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  $\varphi_i : K_i \rightarrow L_i$ . Suppose that  $\sigma : K_1 \rightarrow K_2$  and  $\tau : L_1 \rightarrow L_2$  are isomorphisms. We say that  $\tau$  *extends*  $\sigma$  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*.



$$\begin{array}{ccc} L_1 & \xrightarrow{\tau} & L_2 \\ \uparrow \varphi_1 & \nearrow \tau & \uparrow \varphi_2 \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

When  $\sigma : K_1 \rightarrow K_2$  and  $\tau : L_1 \rightarrow L_2$  are homomorphisms (instead of isomorphisms), then  $\tau$  *extends*  $\sigma$  as a homomorphism of fields when the isomorphism  $\tau : L_1 \rightarrow L'_1 = \tau(L_1)$  extends the isomorphism  $\sigma : K_1 \rightarrow K'_1 = \sigma(K_1)$ .

**Definition 29** ( $K$ -homomorphism). Let  $L : K$  be a field extension relative to the embedding  $\varphi : K \rightarrow L$ , and let  $M$  be a subfield of  $L$  containing  $\varphi(K)$ . Then, when  $\sigma : M \rightarrow L$  is a homomorphism, we say that  $\sigma$  is a  $K$ -homomorphism if  $\sigma$  leaves  $\varphi(K)$  pointwise fixed, which is to say that for all  $\alpha \in \varphi(K)$ , one has  $\sigma(\alpha) = \alpha$ .

**Lemma 9.4.** Suppose that  $L : K$  is a field extension with  $K \subseteq L$ , and that  $\tau : L \rightarrow L$  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  $\tau$  is a  $K$ -automorphism of  $L$ , then  $f(\alpha) = 0 \iff f(\tau(\alpha)) = 0$ .

**Theorem 9.5.** Let  $\sigma : K_1 \rightarrow K_2$  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  $\sigma$  to an isomorphism  $\tau : K_1(\alpha) \rightarrow K_2(\beta)$  in such a manner that  $\tau(\alpha) = \beta$  if and only if  $m_\beta(K_2) = \sigma(m_\alpha(K_1))$ .

$$\begin{array}{ccccc} K_2 & \xrightarrow{\varphi_2} & K_2(\beta) & \xhookrightarrow{\iota_2} & L_2 \\ \downarrow \sigma & & \downarrow \tau & & \\ K_1 & \xrightarrow{\varphi_1} & K_1(\alpha) & \xhookrightarrow{\iota_1} & L_1 \end{array}$$

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

**Corollary 15.** Let  $L : M$  be a field extension with  $M \subseteq L$ . Suppose that  $\sigma : M \rightarrow L$  is a homomorphism, and  $\alpha \in L$  is algebraic over  $M$ . Then the number of ways we can extend  $\sigma$  to a homomorphism  $\tau : M(\alpha) \rightarrow L$  is equal to the number of distinct roots of  $\sigma(m_\alpha(M))$  that lie in  $L$ .

## 10 Algebraic Closure II

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

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

**Corollary 16.** 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 30** (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 10.3.**  $K(\alpha) : K$  is normal  $\iff$  all conjugates of  $\alpha$  are contained in  $K(\alpha)$ .

**Theorem 10.4.** 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 31** (Galois group of polynomial). Let  $L = K(\alpha_1, \dots, \alpha_n)$  and let  $P(\alpha_1, \dots, \alpha_n)$  where  $P \in K[\alpha_1, \dots, \alpha_n]$  is an element of  $L$ . Then we define

$$\text{Gal}_K(f) = \{\sigma \in S_n \mid \forall P \in K[\alpha_1, \dots, \alpha_n], \text{ if } P(\alpha_1, \dots, \alpha_n) = 0 \text{ then } P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) = 0\}$$

**Lemma 11.1.** 1.  $\text{Gal}_K(f) \leq S_n$ ;

2. If  $K_1 : K$ , then  $\text{Gal}_{K_1}(f) \leq \text{Gal}_K(f)$ .

**Definition 32.** Let  $L : K$  be a field extension. Then

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

**Definition 33** (Galois automorphism on splitting field). Let  $\sigma \in \text{Gal}_K f$  where  $L$  is a splitting field for  $f$  over  $K$ , and define  $\hat{\sigma} \in \text{Aut}_K(L)$  such that  $\hat{\sigma}(P(\alpha_1, \dots, \alpha_n)) = P(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ .

**Lemma 11.2.** The map  $\psi(\sigma) = \hat{\sigma}$  is a group isomorphism.

**Theorem 11.3.** If  $L : K$  is an algebraic extension and  $\sigma : L \rightarrow L$  is a  $K$ -homomorphism, then  $\sigma \in \text{Aut}(L)$

**Lemma 11.4.** Suppose that  $M : K$  is a normal extension. Then:

- (a) for any  $\sigma \in \text{Gal}(M : K)$  and  $\alpha \in M$ , we have  $\mu_{\sigma(\alpha)}^K = \mu_\alpha^K$ ;
- (b) for any  $\alpha, \beta \in M$  with  $\mu_\alpha^K = \mu_\beta^K$ , there exists  $\tau \in \text{Gal}(M : K)$  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  $\tau : L \rightarrow \overline{K}$ , 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  $(12), (23), \dots, (n-1, n)$ ;
- 4.  $(12)$  and  $(12 \dots n)$ ;
- 5.  $(12)$  and  $(23 \dots n)$ ;
- 6.  $(ij)$  and  $(i \dots i_p)$  where  $p$  is prime.

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

**Note:**  $|\text{Gal}_K(f)| = [L : K]$  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  $G \leq S_p$  such that  $G$  acts transitively on  $\{1, \dots, p\}$ . Then  $G$  contains a cycle of order  $p$ .

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

## 14 Separability

**Definition 34** (Separable). Let  $K$  be a field.

- (i) An irreducible polynomial  $f \in K[t]$  is *separable over  $K$*  if it has no multiple roots, meaning that  $f = \lambda(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_d)$ , where  $\alpha_1, \dots, \alpha_d \in \overline{K}$  are distinct.
- (ii) A non-zero polynomial  $f \in K[t]$  is *separable over  $K$*  if its irreducible factors in  $K[t]$  are separable over  $K$ .
- (iii) When  $L : K$  is a field extension, we say that  $\alpha \in L$  is *separable over  $K$*  when  $\alpha$  is algebraic over  $K$  and  $\mu_\alpha^K$  is separable.
- (iv) An algebraic extension  $L : K$  is a *separable extension* if every  $\alpha \in L$  is separable over  $K$ .

**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  $\alpha$  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  $\sigma : M \rightarrow \overline{M}$  is a homomorphism, then  $\sigma(\mu_\alpha^M)$  is separable over  $\sigma(M) \iff \mu_\alpha^M$  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  $L = K(\alpha_1, \dots, \alpha_n)$  for some  $\alpha_1, \dots, \alpha_n \in L$ . Put  $K_0 = K$ , and for  $1 \leq i \leq n$ , set  $K_i = K_{i-1}(\alpha_i)$ . Finally, let  $\sigma_0 : K \rightarrow \overline{K}$  be the inclusion map.

- (i) If  $\alpha_i$  is separable over  $K_{i-1}$  for  $1 \leq i \leq n$ , then there are  $[L : K]$  ways to extend  $\sigma_0$  to a homomorphism  $\tau : L \rightarrow \overline{K}$ .
- (ii) If  $\alpha_i$  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  $\sigma_0$  to a homomorphism  $\tau : L \rightarrow \overline{K}$ .

**Theorem 14.4.** Let  $L : K$  be a finite extension with  $L = K(\alpha_1, \dots, \alpha_n)$ . 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  $\alpha_i$  is separable over  $K_{i-1}$  for  $1 \leq i \leq n$ ;
- (ii) the element  $\alpha_i$  is separable over  $K$  for  $1 \leq i \leq n$ ;
- (iii) the extension  $L : K$  is separable.

**Corollary 17.** Suppose that  $L : K$  is a finite extension. If  $L : K$  is a separable extension, then the number of  $K$ -homomorphism  $\sigma : L \rightarrow \overline{K}$  is  $[L : K]$ , and otherwise the number is smaller than  $[L : K]$ .

**Corollary 18.** 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  $K$ . More generally, suppose that  $L : K$  is a splitting field extension for  $S \subseteq K[t] \setminus K$ . Then  $L : K$  is a separable extension  $\iff$  each  $f \in S$  is separable over  $K$ .

## 15 The Primitive Element Theorem

**Definition 35** (Simple extension). Suppose  $L : K$  is a field extension relative to the embedding  $\varphi : K \rightarrow L$ . We say that  $L : K$  is a *simple extension* if there is some  $\gamma \in L$  such that  $L = \varphi(K)(\gamma)$ .

**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 19.** Suppose that  $L : K$  is an algebraic, separable extension, and suppose that for every  $\alpha \in L$ , the polynomial  $\mu_\alpha^K$  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  $[L : K] \leq n$ .

**Corollary 20.** If  $f \in K[t]$  is irreducible over  $K$ , then  $\text{Gal}_K(f)$  acts transitively on the roots of  $f$ .

## 16 Galois Fields I

**Definition 36** (Formal derivative). We define the *derivative operator*  $\mathcal{D} : K[t] \rightarrow K[t]$  by

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

**Theorem 16.1.** 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 37** (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 16.2.** Suppose  $f \in K[t]$  is irreducible over  $K$ . Then  $f$  is inseparable over  $K \iff \text{char } K = p > 0$  and  $f \in K[t^p]$ .

**Definition 38** (Frobenius map). Suppose that  $\text{char } K = p > 0$ . The *Frobenius map*  $\varphi : K \rightarrow K$  is defined by  $\varphi(\alpha) = \alpha^p$ .

**Theorem 16.3.** Suppose that  $\text{char } K = p > 0$ , 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 39** (Fixed field). Let  $L : K$  be a field extension and  $G \leq \text{Aut}(L)$ . We define the *fixed field of  $G$*  as

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

**Theorem 16.4.** Suppose that  $\text{char } K = p > 0$ , and let  $F$  be the prime subfield of  $K$ . Let  $\varphi : K \rightarrow K$  denote the Frobenius map. Then  $\varphi$  is an injective homomorphism, and  $\text{Fix}_\varphi(K) = F$ .

**Corollary 21.** Suppose that  $\text{char } K = p > 0$  and  $K$  is algebraic over its prime subfield. Then the Frobenius map is an automorphism of  $K$ .

**Corollary 22.** Suppose that  $\text{char } K = p > 0$  and  $K$  is algebraic over its prime subfield. Then all polynomials in  $K[t]$  are separable over  $K$ .

**Corollary 23** (\*\*). Suppose that  $\text{char } K = 0$ . Then all polynomials in  $K[t]$  are separable over  $K$ .

**Theorem 16.5.** Suppose that  $\text{char } K = p > 0$ . 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)  $\text{Gal}(\mathbb{F}_q : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ ;
- (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 40** (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

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

and

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

**Lemma 17.3.** 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  $\text{Tr}(\alpha), \text{Norm}(\alpha) \in \mathbb{F}_p$ ;
2. If  $p \neq 2$ , then  $\exists \alpha_1$  such that  $\text{Tr}(\alpha_1) \neq 0$  and  $\exists \alpha_2 (\neq 0)$  such that  $\text{Norm}(\alpha_2) \neq 1$ .

## 19 Fixed Fields

**Definition 41** (Fixed field). Let  $L : K$  be a field extension and  $G \leq \text{Aut}(L)$ . Then the *fixed field* of  $G$  is

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

**Theorem 19.1.** Let  $K, M \subseteq L$  be fields and  $G, H \leq \text{Aut}(L)$ . Then

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

**Definition 42** (Galois Extension). Let  $L : K$  be a field extension. Then  $L : K$  is a *Galois extension* if it is normal and separable.

**Theorem 19.2.** Let  $L : K$  be algebraic. Then  $L : K$  is Galois  $\iff K = \text{Fix}_L(\text{Gal}_K(L))$

**Theorem 19.3.** Suppose that  $L$  is a field,  $G \leq \text{Aut}(L)$  such that  $|G| < \infty$ , and put  $K = \text{Fix}_L(G)$ . Then  $L : K$  is a finite Galois extension with  $[L : K] = |\text{Gal}(L : K)|$ , and furthermore  $G = \text{Gal}_K(L)$ .

**Theorem 19.4.** Let  $L : K$  be finite.

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

**Corollary 24.** Let  $L : M : K$  be a tower such that  $L : K$  is Galois. Then  $L : M$  is Galois.

## 20 Fundamental Theorem of Galois Theory I

**Theorem 20.1** (Fundamental Theorem of Galois Theory, Part 1). Let  $L : K$  be a Galois extension with  $G = \text{Gal}(L : K)$ . 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  $G_P = \text{Aut}_P(L)$ . 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,  $P_1 \subseteq P_2 \iff G_{P_1} \supseteq G_{P_2}$  and  $H_1 \leq H_2 \iff L^{H_1} \supseteq L^{H_2}$ .

## 21 Fundamental Theorem of Galois Theory II

**Theorem 21.1** (Fundamental Theorem of Galois Theory, Part 2). For all  $P \in \mathcal{I}(K, L)$ , we have  $P : K$  is a normal extension  $\iff G_P \triangleleft G$ . Then,  $\text{Gal}_K P \cong G/G_P$ .

**Lemma 21.2.** Let  $K - P - L$  be a tower of fields and  $g \in \text{Aut } L$ . Then  $G_{gP} = gG_P g^{-1}$ .

**Remark 1.** Let  $L : P : K$  be a tower of fields, where  $[L : K] = [L : P][P : K]$ . Then  $\text{Id.} : G_P : G$  is a tower of groups, where  $[G : G_P] \cdot |G_P|$ . That is, for all  $P \leq L$  we have  $[P : K] = [G : G_P]$  and  $[L : P] = |G_P|$ .

## 22 Composita

**Remark 2.** 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:

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

Let  $H_1, H_2 \leq G$ . Then  $H_1 \cap H_2 \leq G$  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 43** (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  $K_1 K_2$ , is the smallest subfield of  $L$  containing both  $K_1$  and  $K_2$ .

**Lemma 22.1.** Let  $K, E, F \subseteq L$ . Then

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

ADD HW PROBLEMS TO ANKI

## 23 Soluble Groups I

**Definition 44** (Soluble group). A group  $G$  is *soluble* if there exists a finite series of subgroups

$$\{Id.\} = G_n \leq G_{n-1} \leq \dots \leq G_0 = G$$

such that

1.  $G_j \triangleleft G_{j-1} \forall 1 \leq j \leq n$  and

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

**Definition 45** (Simple group). A group  $G$  is *simple* if  $G$  has no non-trivial normal subgroups.

**Lemma 23.1.** For  $n \geq 5$  the group  $A_n$  is simple (and hence not soluble).

**Lemma 23.2.** Let  $G$  be a group with  $H \trianglelefteq G$  and  $A \leq G$ . 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 23.3.** 1. If  $G$  is a soluble group with  $A \leq G$ , then  $A$  is soluble.

2. Let  $H \trianglelefteq G$ . Then  $G$  is soluble  $\iff H$  and  $G/H$  are soluble.

**Corollary 25.**  $S_n$  is not soluble for  $n \geq 5$ .

**Corollary 26.** All  $p$ -groups are soluble (i.e. groups  $G$  such that  $|G| = p^n$  for some prime  $p$ )

## 24 Soluble Groups II

**Theorem 24.1** (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

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

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 46** (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 47** (Derived series). The *derived series* of  $G$  is  $G^{(n)} = (G^{(n-1)})'$  and  $\{Id.\} = G^{(n)} \triangleleft G^{(n-1)} \triangleleft \cdots \triangleleft G' \triangleleft G$  (not to be confused with  $G_{n+1} = [G_n, G]$ , the *lower central series*).

**Lemma 24.2.** Let  $\varphi : G \mapsto H$  be an epimorphism. Then  $\varphi(G') = H'$ .

**Definition 48** (Composition series). Let  $G$  be a group. Then a *composition series* of  $G$  is a subnormal series of finite length

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

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

**Theorem 24.3** (Jordan-Hölder). Any 2 composition series of some group  $G$  are equivalent up to permutation and isomorphism.

**Theorem 24.4.** Let  $K$  be a field with  $\text{char } K \neq 2$  and let  $f \in K[t]$  be a separable polynomial with splitting field  $L$ . Then  $f = 0$  is solvable by *quadratic* radicals  $\iff [L : K] = 2^t$ .

## 25 Solvability by radicals and Galois theory I

**Theorem 25.1.** Let  $K$  be a field with  $\text{char } K = 0$ . Then  $f \in K[t]$  is solvable by radicals  $\iff \text{Gal}_K(f)$  is soluble.

**Lemma 25.2.** Let  $\text{char } K = 0$  and  $R : K$  be a radical extension. Then there exists a tower  $K - R - N$  such that  $N : K$  is normal and radical.

**Definition 49** (Cyclic extension). Let  $L$  be the splitting field of some polynomial  $f$  over  $K$ . If  $\text{Gal}(L : K)$  is a cyclic group, then  $L : K$  is a *cyclic* extension.

**Lemma 25.3.** Let  $\text{char } K = 0$  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  $\text{Gal}(L : K)$  is abelian.

**Theorem 25.4.** Let  $\text{char } K = 0$  and  $L : K$  be Galois. Suppose there exists some extension  $M : L$  such that  $M : K$  is normal. Then  $\text{Gal}(L : K)$  is soluble.

**Corollary 27.** Let  $\text{char } K = 0$ . Then  $f \in K[t]$  is SBR  $\implies \text{Gal}_K(f)$  is soluble.

## 26 Solvability by radicals and Galois theory II

**Lemma 26.1.** Let  $p$  be prime and  $G \leq S_p$  such that  $G$  acts transitively on  $\{1, \dots, p\}$ . Then  $G$  contains a cycle of order  $p$ .

**Theorem 26.2.** Let  $\text{char } K = 0$  and  $f \in K[t] \setminus K$ . Then  $\text{Gal}_K(f)$  is soluble  $\implies f$  is SBR.

**Lemma 26.3** (Wooley 14.8). Let  $\text{char } K = 0$ , 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  $\beta$  is a root of  $t^n - \theta$  over  $L$ , then  $L = K(\beta)$ .

**Theorem 26.4** (Abel-Galois). Let  $\text{char } K = 0$  and  $f \in K[t]$  be irreducible over  $K$  with  $\deg f = p$ . Then following are equivalent

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

**Lemma 26.5.** Let  $\{\text{Id.}\} \neq N \trianglelefteq G \leq S_p$  for  $p$  prime. If  $G$  is a transitive group, then  $N$  is a transitive group.

## 27 Final remarks I

**Definition 50** (Sylvester matrix).

**Definition 51** (Resultant).

**Theorem 27.1.** Let  $\alpha_i$  be roots of  $f$  and  $\beta_j$  be roots of  $g$ . Then

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

**R?**

**Corollary 28.** 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 29.** Let  $f(t) = a_0 t^n + \dots + a_n$ ,  $a_0 \neq 0$ . Then  $R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (\alpha_i - \alpha_j)^2$



## 28 Final remarks II

**Definition 52** (Resolvent invariant). Let  $G \leq S_n$  and  $P \in K[x_1, \dots, x_n]$ . Then  $P$  is *resolvent invariant* for  $G$  if  $P^g = P \iff g \in G$ .

**Lemma 28.1.** 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 30.** Let  $S_n = \sqcup_j a_j G$ . Then  $P$  is resolvent invariant for  $G \iff P^{a_j}$  are distinct.

**Definition 53** (Resolvent). Let  $P$  be a resolvent polynomial for  $G \leq S_n$  and  $S_n = \sqcup_{j=1}^s a_j G$ . Then

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

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

**Lemma 28.2.** Let  $G \leq S_n$ ,  $f \in K[t]$  be a separable polynomial. If  $\text{Gal}_K(f) \leq G$  (and its conjugation), then  $\exists j \in K$  such that  $R_{G,f}(j) = 0$

**Lemma 28.3.** Let  $|K| = \infty$  and  $f \in K[t]$  be a separable polynomial. Then  $\exists c_1, \dots, c_n \in K$  such that for all  $k$ ,

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

has the property

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

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

**Theorem 28.4.** Let  $|K| = \infty$ ,  $f \in K[t]$  be a separable polynomial, and  $G \leq S_n$ . Then there exists a resultant  $R_{G,f}(z)$  with no multiple roots.

**Theorem 28.5.** 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