MTH 401: Fields and Galois Theory

Semester 1, 2014-2015

Dr. Prahlad Vaidyanathan

Contents

Classical Algebra

(a) Solving Linear Equations:

  (i) $x + 3 = 4$ has solution $x = 1$, in $\mathbb{N}$

  (ii) $x + 4 = 3$ has solution $x = -1$, in $\mathbb{Z}$

  (iii) $3x = 2$ has solution $x = 2/3$, in $\mathbb{Q}$

  For a general linear equation $ax + b = 0$, the solution $x = -b/a$ lies in $\mathbb{Q}$

(b) Solving Quadratic Equations:

  (i) $x^2 = 2$ has solutions $x = \pm\sqrt{2}$, in $\mathbb{R} \setminus \mathbb{Q}$

  (ii) $x^2 + 1 = 0$ has solutions $x = \pm i$, in $\mathbb{C} \setminus \mathbb{R}$

  For a general quadratic equation

$$ax^2 + bx + c = 0$$

  - Divide by a to get

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0$$

  - Complete the squares to get

$$\left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2} = 0$$

  So we get

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

  which lies in $\mathbb{C}$

  Questions: Given a polynomial equation

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

  (i) Do solutions exist?

  (ii) If so, where do they exist?

  (iii) How do we find them?

  Answer:

To the first two questions, the answer is the Fundamental Theorem of Algebra: If $a_i \in \mathbb{Q}$ for all i, then all solutions exist, and they lie in $\mathbb{C}$.

For the last question, let's examine the case of the cubic.

(c) Solving Cubic Equations:

$$ax^3 + bx^2 + cx + d = 0$$

- Divide by a to get
$$x^3 + ax^2 + bx + c = 0$$
- Complete the cube to get
$$y^3 + py + q = 0$$
where $p = f(a, b, c)$ and $q = g(a, b, c)$
- One can then make a substitution $y = s + t$ (See [Stewart, Section 1.4], [Gowers]) to get two quadratic equations
$$s^6 + u_1 s^3 + u_2 = 0 \Rightarrow s^3 = \text{quadratic formula}$$
$$t^6 + v_1 t^3 + v_2 = 0 \Rightarrow t^3 = \text{quadratic formula}$$
and so
$$x = \frac{-a}{3} + \sqrt[3]{s^3} + \sqrt[3]{t^3}$$
This is called Cardano's Formula. It is a formula that involves
  (i) The coefficients of the polynomial
  (ii) $+, -, \cdot, /$
  (iii) $\sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }$, and $\sqrt[5]{\ }$ (Radicals)
  (iv) Nothing else

  Can such a formula exist for a general polynomial?

(d) Solving Quartic Equation:

- First two steps are the same to get
$$y^4 + py^2 + qy + r = 0$$
- One can again make a substitution to reduce it to a cubic
$$\alpha_1 u^3 + \alpha_2 u^2 + \alpha_3 u + \alpha_4 = 0$$
which can be solved using Cardano's formula.

(e) Solving Quintic Equation:

- First two steps are the same to get

$$y^5 + py^3 + qy^2 + ry + s = 0$$

- Now nothing else works.

(f) Many attempts were made until

  (i) Lagrange (1770-71): All the above methods are particular cases of a single method. This method does not work for the quintic.

  (ii) Abel (1825): No method works for the quintic. ie. There is a quintic polynomial that is not *solvable by radicals*.

  (iii) Galois (1830): Explained why this method works for all polynomials of degree ≤ 4, why it does not work for degree 5, and what does one need for any method to work for any polynomial of any degree!

(End of Day 1)

I. Polynomials

1. Ring Theory

1.1. Definition:

  (i) Ring
  (ii) Ring with $1 \neq 0$
  (iii) Commutative ring
  (iv) Integral domain
  (v) Field

  Note: All rings in this course will be commutative with $1 \neq 0$.

1.2. Examples:

  (i) $\mathbb{N}$ is not a ring, $\mathbb{Z}$ is a ring but not a field, and $\mathbb{Q}, \mathbb{R}\, \mathbb{C}$ are fields.
  (ii) For $n > 1$, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ is a ring, and is a field iff n is prime (without proof)
  (iii) Define
  $$F := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$$
  with usual addition and multiplication. Then F is a field (with proof)
  (iv) Define
  $$K := \{a + b\pi : a, b \in \mathbb{Q}\} \subset \mathbb{C}$$
  then K is not a ring, using the fact that π is transcendental.

1.3. Definition:

  (i) Ideal
  (ii) Ring homomorphism
  (iii) Ring isomorphism

  Note: If $\varphi : R \to S$ is a ring isomorphism, then so is $\varphi^{-1} : S \to R$ (HW)

1.4. Examples:

  (i) $\{0\} \lhd R, R \lhd R$ for any ring R
  (ii) For $n \in \mathbb{N}, n\mathbb{Z} \lhd \mathbb{Z}$ and these are the only ideals in $\mathbb{Z}$ (without proof)
  (iii) The inclusion map $\iota : \mathbb{Q} \to \mathbb{C}$ is a ring homomorphism, and it is the only ring homomorphism from $\mathbb{Q}$ to $\mathbb{C}$ (with proof)

(iv) Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ as in Example 1.2(iii), then define

$$j : F \to \mathbb{C} \text{ by } a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

(v) $z \mapsto \overline{z}$ is a ring homomorphism from $\mathbb{C}$ to $\mathbb{C}$

1.5. Lemma: If $\varphi : R \to S$ is a ring homomorphism, then $\ker(\varphi) \lhd R$

1.6. Theorem: If k is a field, then $\{0\}$ and k are the only ideals in k

1.7. Corollary: If $\varphi : k \to K$ is a homomorphism of fields, then φ is injective.

(End of Day 2)

1.8. Theorem: Let R be a ring and $I \lhd R$, then R/I is a ring.

1.9. Theorem: Let R be a ring, and $I \lhd R$, then the homomorphism $\pi : R \to R/I$ given by $a \mapsto a + I$ is a ring homomorphism. This is called the quotient map.

2. Polynomial Rings

Throughout this section, let k be a field.

2.1. Definition:

(i) Polynomial $f(x)$ over k

Note: $f(x) = g(x)$ iff $n = m$ and $a_i = b_i$ for all i.

For instance, $x \neq x^2$ in $\mathbb{Z}_2[x]$

(ii) The polynomial ring $k[x]$ (Check that it is a commutative ring with $1 \neq 0$)

(iii) Degree of a polynomial $\deg(f)$

2.2. Lemma: Let k be a field and $f, g \in k[x]$

(i) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

(ii) $\deg(fg) = \deg(f) + \deg(g)$

2.3. Theorem (Euclidean Division): Let k be a field and $f, g \in k[x]$ with $g \neq 0$, then $\exists t, r \in k[x]$ such that

$$f = tg + r$$

and either $r = 0$ or $\deg(r) < \deg(g)$

2.4. Definition:

(i) Principal ideal

(ii) PID

2.5. Corollary: $k[x]$ is a PID.

(End of Day 3)

2.6. Definition: Let $\alpha \in k$

(i) Evaluation homomorphism $\varphi_\alpha : k[x] \to k$. We write $f(\alpha) := \varphi_\alpha(f)$

(ii) Root of a polynomial

2.7. (Remainder Theorem): If $0 \neq f \in k[x]$ and $\alpha \in k$

(i) $\exists t \in k[x]$ such that $f(x) = (x - \alpha)t(x) + f(\alpha)$

(ii) α is a root of f iff $\exists t \in k[x]$ such that $f(x) = (x - \alpha)t(x)$

2.8. Corollary: If $0 \neq f \in k[x]$, the number of roots of f in k is $\leq \deg(f)$

Note: The inequality might be strict: $x^2 + 1 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$

3. Fundamental Theorem of Algebra

3.1. Definition: The field $\mathbb{C}$ of complex numbers as $\mathbb{R}^2$ with the operations

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

(i) Identify $\mathbb{R}$ with the subset $\{(x, 0) : x \in \mathbb{R}\} \subset \mathbb{C}$

(ii) Let $i := (0, 1)$, then $i^2 = -1$

(iii) Every $z \in \mathbb{C}$ can be expressed uniquely in the form $z = x + iy$ for $x, y \in \mathbb{R}$

(iv) Polar form $z = re^{i\theta}$ of a complex number. Write

(a) $r = |z| = \sqrt{x^2 + y^2}$

(b) $\text{Arg}(z) = \tan^{-1}(y/x)$

Note: If $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$, then $z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$

3.2. (De Moivre's Theorem): Let $0 \neq z = re^{i\theta} \in \mathbb{C}$ and $n \in \mathbb{N}$

(i) $z^n = r^ne^{in\theta}$. In particular

(a) $|z^n| = |z|^n$

(b) $\text{Arg}(z^n) = n\,\text{Arg}(z)$

(ii) The numbers

$$w_k := r^{1/n}e^{i\frac{\theta+2k}{n}}, \quad k \in \{0, 1, \ldots, n-1\}$$

are all the distinct roots of the polynomial

$$x^n - z \in \mathbb{C}[x]$$

3.3. Example: There are exactly n distinct roots of unity, given by

$$w_k := e^{2\pi ik/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$

They form a cyclic group of order n. The generators of this group are called primitive n^{th} roots of unity.

(End of Day 4)

3.4. Lemma: If $D \subset \mathbb{C}$ is a closed and bounded (compact) set, and $f : D \to \mathbb{R}$ is continuous, then $\exists \alpha \in D$ such that $f(\alpha) \leq f(z)$ for all $z \in D$

3.5. Lemma: Let $f \in \mathbb{C}[x]$, then $\exists \alpha \in \mathbb{C}$ such that $|f(\alpha)| \leq |f(z)|$ for all $z \in \mathbb{C}$

3.6. (Fundamental Theorem of Algebra): Suppose $f \in \mathbb{C}[x]$ is a non-constant polynomial, then $\exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. (See [Fefferman])

3.7. Corollary: If $f \in \mathbb{C}[x]$ is of degree n, then $\exists \beta \in \mathbb{C}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ such that

$$f(x) = \beta(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) \text{ in } \mathbb{C}[x]$$

3.8. Corollary: A real polynomial factorizes into linear and quadratic factors in $\mathbb{R}[x]$

(End of Day 5)

4. Factorization of Polynomials

Let k be a field

4.1. Definition : For $f, g \in k[x]$, $f \mid g$ iff $\exists h \in k[x]$ such that $g = fh$

4.2. (Existence of GCD): Let $f, g \in k[x]$, then $\exists d \in k[x]$ such that

- (i) $d \mid f$ and $d \mid g$
- (ii) If $h \mid f$ and $h \mid g$, then $h \mid d$
- (iii) (Bezout's Identity) $\exists s, t \in k[x]$ such that $d = sf + gt$

4.3. Remark/Definition:

- (i) The d above is unique upto multiplication by a constant. The unique monic polynomial satisfying these properties is called the GCD of f and g
- (ii) Relatively prime.
- (iii) Irreducible polynomial
- (iv) Maximal ideal

4.4. Theorem: For $f \in k[x]$, TFAE :

- (i) f is irreducible
- (ii) (f) is a maximal ideal
- (iii) $k[x]/(f)$ is a field

4.5. Examples:

- (i) Polynomials of degree 1, but not 0 (since the latter are units)
- (ii) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but not $\mathbb{R}[x]$.
- (iii) $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ and $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ (without proof)

(iv) By FTA, $f \in \mathbb{C}[x]$ is irreducible iff $\deg(f) = 1$

(v) By FTA, $f \in \mathbb{R}[x]$ is irreducible iff either $\deg(f) = 1$ or $f(x) = \beta(x-z)(x-\overline{z})$ for some $z \in \mathbb{C} \setminus \mathbb{R}$ and $\beta \in \mathbb{R}$

(End of Day 6)

4.6. (Unique Factorization - I): If $0 \neq f \in k[x]$, then f can be expressed as a product of irreducibles.

4.7. (Euclid's Lemma): Let $f, g, h \in k[x]$ such that $f \mid gh$

(i) If $(f, g) = 1$, then $f \mid h$

(ii) In particular, if $f \in k[x]$ is irreducible, then either $f \mid g$ or $f \mid h$

4.8. (Unique Factorization - II): If $0 \neq f \in k[x]$, then the factorization of into irreducibles (as in 4.6) is unique upto constant factors and the order in which the factors are written.

4.9. Definition: Let $f \in k[x]$ and $\alpha \in k$ be a root of f

(i) Multiplicity of the root α

(ii) Simple root

4.10. Corollary: Let $f \in k[x]$ and $\alpha_1, \alpha_2, \ldots, \alpha_s \in k$ be the roots of f in k of multiplicity $m_1, m_2, \ldots, m_s$ respectively. Then $\exists g \in k[x]$ which has no roots in k such that

$$f(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2} \ldots (x-\alpha_s)^{m_s} g(x)$$

5. Irreducibility of Polynomials

5.1. Remark: If R is an integral domain with $1_R \neq 0$, then

(i) (a) We may define a polynomial f over R as in Definition 2.1.

(b) Also, $R[x]$ is a ring with $1 = 1_R \neq 0$

(c) We may also define the degree of a polynomial.

(d) Since R is an integral domain, $\deg(fg) = \deg(f) + \deg(g)$ and so $R[x]$ is an integral domain as well.

(ii) However, if R is not a field, then

(a) Euclidean division (Theorem 2.3) does not hold.

(b) Furthermore, $R[x]$ is not a PID (See HW 3)

(End of Day 7)

5.2. Remark: If $p \in \mathbb{Z}$ is prime, then the quotient map $\pi : \mathbb{Z} \to \mathbb{Z}_p$ induces a surjective homomorphism $\overline{\pi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ whose kernel is

$$p\mathbb{Z}[x] = \{pf : f \in \mathbb{Z}[x]\}$$

We write $\overline{a} := \pi(a)$ for all $a \in \mathbb{Z}$ and $\overline{f} := \overline{\pi}(f)$ for all $f \in \mathbb{Z}[x]$

5.3. Lemma: Let $p \in \mathbb{Z}$ be a prime number and $g, h \in \mathbb{Z}[x]$ be such that $p \mid gh$ in $\mathbb{Z}[x]$ (ie. $\exists f \in \mathbb{Z}[x]$ such that $pf = gh$), then either $p \mid g$ or $p \mid h$ in $\mathbb{Z}[x]$

5.4. (Gauss' Lemma): Let $f \in \mathbb{Z}[x]$, f is irreducible in $\mathbb{Z}[x]$ iff it is irreducible in $\mathbb{Q}[x]$

Note:

(i) It is obvious that if f is irreducible in $\mathbb{Q}[x]$, then it is irreducible in $\mathbb{Z}[x]$

(ii) Compare Gauss' Lemma with the fact that $(x^2 - 2)$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{R}[x]$.

5.5. (Eisenstein's criterion): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, and suppose there is a prime $p \in \mathbb{Z}$ such that

(i) $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

Then f is irreducible in $\mathbb{Q}[x]$

5.6. Examples:

(i) $x^5 + 10x + 5$ is irreducible over $\mathbb{Q}$

(ii) $\frac{x^4}{9} + \frac{4x}{3} + \frac{1}{3} \in \mathbb{Q}[x]$ is irreducible

(iii) If $p \in \mathbb{Z}$ is prime, then $x^n - p \in \mathbb{Q}[x]$ is irreducible. Hence, $\sqrt[n]{p} \notin \mathbb{Q}$ for $n \geq 2$

(iv) If $p \in \mathbb{Z}$ is prime,

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible in $\mathbb{Q}[x]$ (HW)

(End of Day 8)

5.7. (Reduction mod p) Let $p \in \mathbb{Z}$ be a prime, and let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ be such that $p \nmid a_n$. If $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Z}[x]$.

5.8. Example: $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, but its image is reducible in $\mathbb{Z}_2[x]$. So the converse of 5.7 is not true (HW).

5.9. Definition: Primitive polynomial $f \in \mathbb{Z}[x]$

Note:

(i) Irreducible polynonomial is primitive.

(ii) Primitive polynomial may not be irreducible. Example: $x^2 + 2x + 1$

5.10. Lemma: Let $f, g \in \mathbb{Z}[x]$ such that f is primitive, and $f \mid g$ in $\mathbb{Q}[x]$, then $f \mid g$ in $\mathbb{Z}[x]$ (Proof HW)

5.11. (Rational Root Theorem): Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ have a root $p/q \in \mathbb{Q}$ where $(p, q) = 1$. Then

(i) $p \mid a_0$ and $q \mid a_n$

(ii) In particular, if f is monic, then every rational root of f must be an integer.

5.12. (Euclid's Lemma) Let $f, g, h \in \mathbb{Z}[x]$ such that f is irreducible and $f \mid gh$. Then either $f \mid g$ or $f \mid h$

5.13. (Unique Factorization): If $0 \neq f \in \mathbb{Z}[x]$, then f can be expressed as a product of irreducible polynomials. Furthermore, this product is unique upto multiplication by ± 1 and the order in which the factors are written.

(End of Day 9)

II. Field Extensions

1. Simple Extensions

Motivation: Let $f \in \mathbb{Q}[x]$ and $\alpha \in \mathbb{C}$ be a root of f. We want to know whether α can be obtained from the coefficients of f by algebraic operations, and radicals. To do this, we look at the field

$$\mathbb{Q}(\alpha) = \text{ the smallest field containing } \mathbb{Q} \text{ and } \alpha$$

and understand the relationship between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$

Note: All fields in this section will be subfields of $\mathbb{C}$

1.1. Definition:

(i) Field extension $k \subset L$

(ii) Smallest field $k(X)$ generated by a field $k \subset \mathbb{C}$ and a set $X \subset \mathbb{C}$.

(iii) Simple extension $k(\alpha)$

1.2. Examples:

(i) $\mathbb{Q} \subset \mathbb{R}, \mathbb{Q} \subset \mathbb{C}$ are field extensions, but neither are simple (proof later)

(ii) $\mathbb{R} \subset \mathbb{C}$ is a simple extension. $\mathbb{C} = \mathbb{R}(i)$ (See I.3.1). Note that $\mathbb{C} = \mathbb{R}(i+1)$ as well, so the generator may not be unique.

(iii) By HW 1.4, every subfield $k \subset \mathbb{C}$ contains $\mathbb{Q}$. So $\mathbb{Q} \subset k$ is a field extension.

(iv) Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, then by Example 1.2(iii), F is a field. Hence, $\mathbb{Q} \subset F$ is a field extension. Note that $F = \mathbb{Q}(\sqrt{2})$

(v) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and is hence a simple extension (with proof)

1.3. Definition/Remark: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$

(i) α is algebraic over k.

(ii) α is transcendental over k.

1.4. Examples:

(i) If $\alpha \in k$, then α is algebraic over k

(ii) $\sqrt{2}$ is algebraic over $\mathbb{Q}$

(iii) π is transcendental over $\mathbb{Q}$ (without proof)

(iv) π is algebraic over $\mathbb{R}$

1.5. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Then $\exists$ unique polynomial $f \in k[x]$ such that

(i) f is monic and irreducible

(ii) $f(\alpha) = 0$

Furthermore, if $g \in k[x]$ is any polynomial, then $g(\alpha) = 0$ iff $f \mid g$ in $k[x]$. This is called the minimal polynomial of α over k and is denoted by $m_\alpha := m_{\alpha,k}$.

1.6. Examples:

(i) If $\alpha \in k$, then $m_\alpha(x) = x - \alpha$

(ii) If $k = \mathbb{Q}, \alpha = \sqrt{2}$, then $m_\alpha(x) = x^2 - 2$

(iii) If $k = \mathbb{R}, \alpha = \sqrt{2}$, then $m_\alpha(x) = x - \sqrt{2}$

(iv) If $k = \mathbb{Q}, \omega = e^{2\pi i/3}$, then $m_\omega(x) = \Phi_2(x) = x^2 + x + 1$ (See HW 3.2)

(End of Day 10)

1.7. Definition: Let $k \subset L_1$ and $k \subset L_2$ be field extensions

(i) Homomorphism of field extensions

(ii) Isomorphism of field extensions

1.8. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Then

(i) $k \subset k[x]/(m_\alpha)$ is a field extension

(ii) $k[x]/(m_\alpha) \cong_k k(\alpha)$

1.9. Corollary: Let $k \subset \mathbb{C}$ and $\alpha, \beta \in \mathbb{C}$ be algebraic over k with the same minimal polynomial. Then there is an isomorphism of field extensions $k(\alpha) \cong_k k(\beta)$ which sends $\alpha \mapsto \beta$.

1.10. Remark: Let $k \subset \mathbb{C}$ be a field.

(i) If $p \in k[x]$ is a monic irreducible polynomial, and $\alpha, \beta \in \mathbb{C}$ are two roots of p, then there exists a homomorphism of field extensions $\varphi : k(\alpha) \to \mathbb{C}$ such that $\varphi\mid_k = \mathrm{id}_k$ and $\varphi(\alpha) = \beta$

(ii) Conversely, if $\varphi : k(\alpha) \to \mathbb{C}$ is a homomorphism of field extensions over k, then $\beta := \varphi(\alpha)$ is algebraic over k, and $m_\beta = m_\alpha$ (HW)

1.11. Definition: The field of rational functions $k(x)$ over k.

(End of Day 11)

1.12. Remark:

(i) $k[x] \neq k(x)$ for any field k because x is not invertible in $k[x]$

(ii) The notation $k(x)$ is used because it is the smallest field containing k and x

(iii) $k(x)$ is the field of quotients of the integral domain $k[x]$.

1.13. Theorem: Let k be a field and $\alpha \in \mathbb{C}$ be transcendental over k. Then

$$k(\alpha) \cong_k k(x)$$

2. Degree of an Extension

2.1. Remark:

(i) Let $k \subset L$ be a field extension, then L is a $k-$vector space.

(ii) If $k \subset L_1$ and $k \subset L_2$ are two extensions, then a homomorphism $\varphi : L_1 \to L_2$ of $k-$extensions is a k-linear map of vector spaces.

2.2. Definition: Let $k \subset L$ be a field extension

(i) Degree $[L : k]$ of the extension

(ii) Finite extension

2.3. Example:

(i) $\mathbb{R} \subset \mathbb{C}$ is a finite extension with $[\mathbb{C} : \mathbb{R}] = 2$

(ii) $\mathbb{Q} \subset \mathbb{R}$ is not a finite extension since $\mathbb{Q}$ is countable and $\mathbb{R}$ is not.

(iii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ is a finite extension of degree 2.

(iv) If $k \subset \mathbb{C}$ and $\alpha \in \mathbb{C}$ is transcendental over k, then $k \subset k(\alpha)$ is an infinite extension.

2.4. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Let $m_\alpha \in k[x]$ be the minimal polynomial of α over k, and let $n = \deg(m_\alpha)$. Then

(i) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $k(\alpha)$ over k

(ii) In particular, $[k(\alpha) : k] = \deg(m_\alpha) < \infty$

2.5. Examples:

(i) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, which explains Example I.1.2

(ii) $\mathbb{Q}(\sqrt[3]{2}) = \{a + b2^{1/3} + c2^{2/3} : a, b, c \in \mathbb{Q}\}$ and $2^{2/3} \notin \{a + b2^{1/3} : a, b \in \mathbb{Q}\}$

(iii) $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$ (See I.3.1)

(iv) Let $p \in \mathbb{Z}$ be a prime number and $\zeta_p := e^{2\pi i/p} \in \mathbb{C}$, then Φ_p is the minimal polynomial of ζ_p (See HW 3.2), so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$

(End of Day 12)

2.6. (Tower Law) If $k \subset F$ and $F \subset L$ are two field extensions, then

$$[L : k] = [L : F][F : k]$$

2.7. Examples:

(i) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ (with proof).

(ii) If $[L : k]$ is prime, then

(a) There are no non-trivial intermediate fields $k \subset F \subset L$

(b) $k \subset L$ is a simple extension

(iii) Let $f(x) = x^3 + 6x + 2 \in \mathbb{Q}[x]$. Then f is irreducible over $\mathbb{Q}(\sqrt[4]{2})$ (HW 4.4)

2.8. Corollary: Let $k \subset F_1$ and $k \subset F_2$ be field extensions (all contained in $\mathbb{C}$). Let L denote the smallest field containing both F_1 and F_2. Then

(i) $[L : F_2] \leq [F_1 : k]$

(ii) $[L : k] \leq [F_1 : k][F_2 : k]$

(iii) If $[F_1 : k]$ and $[F_2 : k]$ are relatively prime, then equality holds in part (ii).

L is called the <u>compositum</u> of F_1 and F_2 and is denoted by F_1F_2

(End of Day 13)

2.9. Example: Let $F_1 = \mathbb{Q}(\sqrt[3]{2}), F_2 = \mathbb{Q}(\omega\sqrt[3]{2})$ where $\omega = e^{2\pi i/3}$, then

(i) $F_1F_2 = \mathbb{Q}(\sqrt[3]{2}, \omega)$

(ii) $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6 < 9 = [F_1 : \mathbb{Q}][F_2 : \mathbb{Q}]$

So strict inequality may hold in part (ii) (HW 4.5)

3. Algebraic Extensions

3.1. Definition: Algebraic Extension

3.2. Theorem:

(i) If $k \subset L$ is finite extension, then it is algebraic.

(ii) If $\alpha \in \mathbb{C}$ is algebraic over k, then $k \subset k(\alpha)$ is algebraic.

3.3. Example:

(i) Let $\zeta_5 := e^{2\pi i/5} \in \mathbb{C}$, then $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$ is algebraic. In particular, $\cos(2\pi/5)$ is algebraic over $\mathbb{Q}$

(ii) Let F be the set of algebraic numbers, then

(a) F is a field

(b) $\mathbb{Q} \subset F$ is an infinite extension that is algebraic.

3.4. Definition: Finitely generated extension

3.5. Theorem: $k \subset L$ is a finite extension iff it is algebraic and finitely generated.

(End of Day 14)

3.6. Theorem: Suppose $k \subset F$ and $F \subset L$ are algebraic extensions, then $k \subset L$ is algebraic.

Note: If the extensions were finite, then it would follow from the Tower Law.

3.7. Lemma (HW 5.4): Let $F \subset \mathbb{C}$ be a field, then TFAE:

(i) If $0 \neq f \in F[x]$ is any polynomial, then f has a root in F

(ii) If $f \in F[x]$, then every root of f is in F

(iii) If $F \subset L$ is an algebraic extension, then $F = L$

If these conditions holds, we say that L is algebraically closed.

3.8. Theorem: The field of algebraic numbers (See Example 3.3(ii)) is algebraically closed.

3.9. Remark:

(i) F is called the algebraic closure of $\mathbb{Q}$, and is denoted by $\overline{\mathbb{Q}}$

(ii) F is the smallest subfield of $\mathbb{C}$ that is algebraically closed.

(iii) $\overline{\mathbb{Q}}$ is countable (HW 5.5), so there exist transcendental real numbers.

4. Primitive Element Theorem

(Taken from [Greenberg])

4.1. Definition: Separable polynomial

4.2. Remark: Let $f \in k[x]$, then $D(f)$ denotes the derivative of f

(i) $D(f+g) = Df + Dg$

(ii) $D(fg) = fD(g) + gD(f)$

(iii) If $\lambda \in k$, then $D(\lambda f) = \lambda D(f)$

4.3. Theorem: Let $k \subset \mathbb{C}$ and $f \in k[x]$. Then f is separable iff $(f, D(f)) = 1$ in $k[x]$

(End of Day 15)

4.4. Corollary: Let $k \subset \mathbb{C}$ be a field and $f \in k[x]$ be irreducible, then f is separable.

4.5. (Primitive Element Theorem): Let $k \subset L$ be a finite extension of subfields of $\mathbb{C}$, then it is a simple extension. ie. $\exists \theta \in L$ such that $L = k(\theta)$

This element θ is called a primitive element of the field extension $k \subset L$

4.6. Example:

(i) If $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\theta = \sqrt{2} + \sqrt{3}$ works (See Example II.1.2(v))

(ii) $\mathbb{Q} \subset \overline{\mathbb{Q}}$ is not a simple extension. Hence the primitive element theorem does not hold for infinite algebraic extensions.

4.7. Corollary: Let $k \subset L$ be a finite extension of subfields of $\mathbb{C}$, then there are only finitely many intermediate fields $k \subset F \subset L$

(End of Day 16)

III. Galois Theory

1. The Galois Group

1.1. Examples: List all homomorphisms from $k \to \mathbb{C}$:

(i) $k = \mathbb{Q}$: There is only one map, the inclusion.

(ii) $k = \mathbb{Q}(\sqrt{2})$: There are two maps, $\{i, j\}$ where $j(a + b\sqrt{2}) = a - b\sqrt{2})$

(iii) $k = \mathbb{Q}(\omega)$: There are two maps given by the 2 roots of $x^2 + x + 1$

(iv) $k = \mathbb{Q}(\sqrt[3]{2})$: There are three maps given by the 3 roots of $x^3 - 2$

(v) $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$: There are 4 maps given by $\sqrt{2} \mapsto \pm\sqrt{2}$ and $\sqrt{3} \mapsto \pm\sqrt{3}$

(vi) $k = \mathbb{Q}(\sqrt[3]{2}, \omega)$: There are 6 maps determined by the images of ω and $\sqrt[3]{2}$ from parts (iii) and (iv) respectively.

1.2. Lemma: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k. Let $\varphi : k(\alpha) \to \mathbb{C}$ a homomorphism over k and let $\beta := \varphi(\alpha)$

(i) For any $f \in k[x]$,
$$\varphi(f(\alpha)) = f(\beta)$$

(ii) β is algebraic over k

(iii) The minimal polynomials of α and β over k are the same.

1.3. Theorem: Let $k \subset \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ be algebraic over k with minimal polynomial $m_\alpha \in k[x]$. Then there is a one-to-one correspondence
$$\{k\text{-homomorphisms from } k(\alpha) \to \mathbb{C}\} \leftrightarrow \{\text{roots of } m_\alpha \text{ in } \mathbb{C}\}$$

1.4. Corollary: Let $k \subset L$ be a finite extension, then
$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \mathbb{C} = [L : k]$$

1.5. Definition: $\mathrm{Gal}_k(L)$

(End of Day 17)

1.6. Lemma:

(i) If $k \subset L$ is an algebraic extension, and $\varphi : L \to \mathbb{C}$ is a k-homomorphism such that $\varphi(L) \subset L$, then $\varphi : L \to L$ is bijective.

(ii) In particular, if $L = k(\alpha_1, \alpha_2, \dots, \alpha_n)$, then φ is bijective iff $\varphi(\alpha_i) \in L$ for all $1 \leq i \leq n$.

1.7. Remark :

(i) $\mathrm{Gal}_k(L)$ is a group. One also writes $\mathrm{Aut}_k(L) = \mathrm{Gal}_k(L)$

(ii) By Lemma 1.4, if $k \subset L$ is finite $\Rightarrow |\mathrm{Gal}_k(L)| \leq [L : k]$

(iii) By Lemma 1.6, if $k \subset L = k(\theta)$ is finite $\Rightarrow \mathrm{Gal}_k(L) \leftrightarrow \{\text{roots of } m_\theta \text{ in } L\}$

1.8. Examples:

(i) $\mathrm{Gal}_k(k) = \{\mathrm{id}_k\}$

(ii) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$

(iii) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong \mathbb{Z}_2$

(iv) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}\}$

(v) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (with proof)

(vi) $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega)) \cong S_3$ (with proof)

2. Splitting Fields

2.1. Definition: Let $k \subset L$ be a field extension, and $f \in k[x]$

(i) f splits in L

(ii) L is the splitting field of f.

(End of Day 18)

(iii) Normal extension

2.2. Remark:

(i) If $f \in \mathbb{Q}[x]$, then f splits in $\mathbb{C}$ (in fact, in $\overline{\mathbb{Q}}$), but these are not the splitting fields of f. In fact, the splitting field of f must be a finite extension of $\mathbb{Q}$.

(ii) If L is the splitting field of f over k, then $[L : k] < \infty$

2.3. Theorem: Let $k \subset L$ be a finite extension, then TFAE:

(i) $k \subset L$ is a normal extension

(ii) $\exists f \in k[x]$ such that L is the splitting field of f over k

(iii) $|\mathrm{Gal}_k(L)| = [L : k]$

2.4. Definition: $\mathrm{Gal}_k(L)$ is called the Galois group of f, denoted by $\mathrm{Gal}_k(f)$

2.5. Examples:

(i) If $f \in k[x]$ is linear, then $L = k$ is the splitting field of f over k. Hence $\mathrm{Gal}_k(f) = \{\mathrm{id}_k\}$

(ii) If $f(x) = ax^2+bx+c \in k[x]$ is an irreducible quadratic, then $L = k(\sqrt{b^2 - 4ac})$ is the splitting field of f over k. Hence $\mathrm{Gal}_k(f) \cong \mathbb{Z}_2$

(iii) If $k = \mathbb{Q}, f(x) = x^3 - 2$, then $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Hence $\text{Gal}_k(f) \cong S_3$

(iv) If $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$, then $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\text{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

(v) If $k = \mathbb{Q}, f(x) = x^p - 1$, with $p \in \mathbb{Z}$ prime, then $L = \mathbb{Q}(\zeta_p)$. Hence $\text{Gal}_k(f) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ (HW)

(vi) If $k = \mathbb{Q}, f(x) = x^4 - 2$, then $L = \mathbb{Q}(\sqrt[4]{2}, i)$ and $\text{Gal}_{\mathbb{Q}}(f) \cong D_4$ (proof later)

3. Permutation of Roots

3.1. Definition:

(i) Symmetric group on a set X

(ii) The symmetric group S_n

3.2. Theorem: If $|X| = n$, then $S_X \cong S_n$

3.3. Definition:

(i) Group Action

(ii) Faithful action

(End of Day 19)

3.4. (Permutation Representation) If G acts on a set X, then

(i) There is an induced homomorphism $\varphi : G \to S_X$

(ii) This homomorphism φ is injective iff the action is faithful.

3.5. Theorem: Let $k \subset \mathbb{C}$ be a field and let $f \in k[x]$ be of degree n. Let $G = \text{Gal}(f)$ and let X be the set of roots of f in $\mathbb{C}$. Then

(i) G acts on X faithfully.

(ii) In particular, $G \cong$ to a subgroup of S_n

3.6. Example:

(i) Let $f(x) = x^3 - 2$, then $|\text{Gal}_{\mathbb{Q}}(f)| = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$ and $\text{Gal}_{\mathbb{Q}}(f) < S_3$ (by Theorem 3.5). Hence $\text{Gal}_{\mathbb{Q}}(f) \cong S_3$

(ii) Let $f(x) = x^4 - 2$, then

(a) $|\text{Gal}(f)| = 8$ (by Example 2.5(vi))

(b) Thus $\text{Gal}(f) \cong D_4$

3.7. Definition: Transitive action

3.8. Examples:

(i) If $G = \text{Gal}_{\mathbb{Q}}(x^3 - 2)$, then G acts transitively on $X = \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ (See Example 1.8(vi))

(ii) If $G = \mathrm{Gal}_{\mathbb{Q}}((x^2-2)(x^2-3))$, then G does not act transitively on $X = \{\pm\sqrt{2}, \pm\sqrt{3}\}$. However, G will act transitively on the set of roots of the minimal polynomial of $\sqrt{2}+\sqrt{3}$.

3.9. Theorem: Let $k \subset \mathbb{C}$ be a field and let $f \in k[x]$. Let $G = \mathrm{Gal}(f)$ and let X be the set of roots of f in $\mathbb{C}$. If G acts on X transitively, then f is irreducible.

Note: The converse is also true. We will prove it later.

(End of Day 20)

4. Normal Extensions

4.1. (Extension Lemma): Let $k \subset F \subset L$ be finite field extensions. If $\varphi : F \to \mathbb{C}$ is a k-homomorphism, then $\exists \psi : L \to \mathbb{C}$ such that $\psi\mid_F = \varphi$.

4.2. Theorem: Let $f \in k[x]$, let G be the Galois group of f and let X be the set of roots of f in $\mathbb{C}$. Then G acts transitively on X iff f is irreducible in $k[x]$.

4.3. Remark:

(i) Let $k \subset F \subset L$ be finite extensions such that $k \subset L$ is normal. If $\varphi : F \to \mathbb{C}$, then $\exists \psi \in \mathrm{Gal}_k(L)$ such that $\psi\mid_F = \varphi$.

(ii) In particular, if $k \subset F$ is also normal, then every $\varphi \in \mathrm{Gal}_k(F)$ extends to a $\psi \in \mathrm{Gal}_k(L)$.

4.4. Theorem: Let $k \subset F \subset L$ be finite extensions such that $k \subset F$ and $k \subset L$ are both normal. Then

(i) The restriction map
$$\pi : \mathrm{Gal}_k(L) \to \mathrm{Gal}_k(F)$$
is a well-defined, surjective, group homomorphism.

(ii) $\ker(\pi) = \mathrm{Gal}_F(L)$

(iii) Hence,
$$\mathrm{Gal}_k(L)/\mathrm{Gal}_F(L) \cong \mathrm{Gal}_k(F)$$

(iv) In particular,
$$[F : k] = [\mathrm{Gal}_k(L) : \mathrm{Gal}_F(L)]$$

We visualize this by tower diagrams

$$\begin{tikzcd}
L \arrow[d, dash] & \mathrm{Gal}_k(L) \arrow[d, dash] \\
F \arrow[d, dash] & \mathrm{Gal}_F(L) \arrow[d, dash] \\
k & \{e\}
\end{tikzcd}$$

4.5. Corollary: If $k \subset F \subset L$ be finite extensions such that $k \subset F$ and $k \subset L$ are normal, then

$$\mathrm{Gal}_F(L) \lhd \mathrm{Gal}_k(L)$$

4.6. Remark: Let $k \subset F \subset L$ be a tower of field extensions,

(i) If $k \subset F$ is not normal, then π (defined in Theorem 4.4) may not be well-defined.

(ii) However, $\mathrm{Gal}_F(L) < \mathrm{Gal}_k(L)$ holds, even if it is not normal.

4.7. Example:

(i) If $k \subset F \subset L$ is finite normal such that $[F : k] = 2$, then $\mathrm{Gal}_F(L) \lhd \mathrm{Gal}_k(L)$. We have towers

$$\begin{array}{ccc} L & & \mathrm{Gal}_k(L) \\ | & & |\,{\scriptstyle 2} \\ F & & \mathrm{Gal}_F(L) \\ |\,{\scriptstyle 2} & & | \\ k & & \{e\} \end{array}$$

(ii) Let $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2}, i)$, then $k \subset L$ is normal and $\mathrm{Gal}_k(L) \cong D_4$ (Example III.3.6) generated by

$$\sigma : \sqrt[4]{2} \to i\sqrt[4]{2} \text{ and } i \mapsto i$$
$$\tau : \sqrt[4]{2} \to \sqrt[4]{2} \text{ and } i \mapsto -i$$

Let $F = \mathbb{Q}(\sqrt{2}, i) \subset L$, then

(a) $\mathbb{Q} \subset F$ is normal. Hence $\mathrm{Gal}_F(L) \lhd D_4$

(b) $|\,\mathrm{Gal}_F(L)| = 2$ and $\mathrm{Gal}_F(L) \cong \langle \sigma^2 \rangle$

(c) We have the towers

$$\begin{array}{ccc} L & & D_4 \\ |\,{\scriptstyle 2} & & |\,{\scriptstyle 4} \\ F & & \langle \sigma^2 \rangle \\ |\,{\scriptstyle 4} & & |\,{\scriptstyle 2} \\ \mathbb{Q} & & \{0\} \end{array}$$

(End of Day 21)

(iii) $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ then $G = \mathrm{Gal}_k(L) \cong S_3$ via the action of G on the set

$$\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\} \leftrightarrow \{1, 2, 3\}$$

Let $F = \mathbb{Q}(\sqrt[3]{2})$, then

$$\mathrm{Gal}_F(L) \cong \{\sigma \in S_3 : \sigma(1) = 1\} = \langle (23) \rangle$$

Hence, $\mathrm{Gal}_F(L)$ is not normal in $\mathrm{Gal}_k(L)$, and so $k \subset F$ is not a normal extension.

5. The Galois Correspondence

5.1. Definition: Let $k \subset L$ be a field extension and $G := \mathrm{Gal}_k(L)$

(i) If $k \subset F \subset L$ is an intermediate field, then

$$\mathrm{Gal}_F(L) < \mathrm{Gal}_k(L)$$

(ii) If $H < G$, then

$$L^H := \{x \in L : \varphi(x) = x \quad \forall \varphi \in H\} \subset L$$

is called the fixed field of H

Note: L^H is a subfield of L containing k.

(iii) We set

$$\begin{aligned} \mathcal{F} &:= \{\text{intermediate fields } k \subset F \subset L\} \\ \mathcal{G} &:= \{\text{ subgroups } H < G\} \\ \Phi : \mathcal{F} \to \mathcal{G}&, \text{ given by } \Phi(F) := \mathrm{Gal}_F(L) \\ \Psi : \mathcal{G} \to \mathcal{F}&, \text{ given by } \Psi(H) := L^H \end{aligned}$$

Note: This may not be a one-to-one correspondence in general.

5.2. Examples:

(i) If $k \subset L$ is any field extension, and $G = \mathrm{Gal}_k(L)$

(a) If $H = \{e\} < G$, then $L^H = L$

However, L^G may not be equal to k (See below)

(b) If $H_1 \subset H_2$ are two subgroups of G, then $L^{H_2} \subset L^{H_1}$. We visualize this by

$$\begin{tikzcd} G \arrow[d, dash] & L^G \supset k \arrow[d, dash] \\ H_2 \arrow[r, "\Psi"] \arrow[d, dash, "\cup"'] & L^{H_2} \arrow[d, dash, "\cap"] \\ H_1 \arrow[r, "\Psi"] \arrow[d, dash] & L^{H_1} \arrow[d, dash] \\ \{e\} & L^{\{e\}} = L \end{tikzcd}$$

(c) If $F = L$, then $\mathrm{Gal}_F(L) = \{e\}$

If $F = k$, then $\mathrm{Gal}_k(L) = G$

(d) If $F_1 \subset F_2$ are two intermediate fields, then $\mathrm{Gal}_{F_2}(L) < \mathrm{Gal}_{F_1}(L)$. We visualize this by the tower diagram

$$\begin{tikzcd}
L \arrow[d, dash] & \{e\} \arrow[d, dash] \\
F_2 \arrow[r, mapsto, "\Phi"] \arrow[d, phantom, "\cup" left] & \mathrm{Gal}_{F_2}(L) \arrow[d, phantom, "\cap" right] \\
F_1 \arrow[r, mapsto, "\Phi"] \arrow[d, dash] & \mathrm{Gal}_{F_1}(L) \arrow[d, dash] \\
k & \mathrm{Gal}_k(L)
\end{tikzcd}$$

(ii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$, then $\mathrm{Gal}_k(L) \cong \mathbb{Z}_2$. So

(a) $\mathcal{F} = \{\mathbb{Q}, \mathbb{Q}(\sqrt{2})\}$ (Example II.2.7)

(b) $\mathcal{G} = \{\{0\}, \mathbb{Z}_2\}$

So we have the diagram

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \{0\} \arrow[d, dash] \\
\mathbb{Q} & \mathbb{Z}_2
\end{tikzcd}$$

(iii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$, then $\mathrm{Gal}_k(L) = \{\mathrm{id}_L\}$, and again we have the diagram

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] & \{\mathrm{id}\} \arrow[d, dash] \\
\mathbb{Q} & \{\mathrm{id}\}
\end{tikzcd}$$

Note that $L^G = L \neq k$

(iv) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then the lattice is

$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \langle (0,0) \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle (0,1) \rangle \arrow[dr, dash] & \langle (1,0) \rangle \arrow[d, dash] & \langle (1,1) \rangle \arrow[dl, dash] \\
& G &
\end{tikzcd}$$

(v) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, then $G \cong S_3$ and the lattice of subfields is

$$\begin{tikzcd}
& L \arrow[ddl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
& \mathbb{Q}(\sqrt[3]{2}) \arrow[dd, dash, "3"] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[ddl, dash, "3"] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[ddll, dash, "3"] \\
\mathbb{Q}(\omega) \arrow[dr, dash, "2"] & & & \\
& \mathbb{Q} & &
\end{tikzcd}$$

and the lattice of subgroups is

$$\begin{tikzcd}
& \{\mathrm{id}\} \arrow[ddl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
& \langle (23) \rangle \arrow[dd, dash, "3"] & \langle (13) \rangle \arrow[ddl, dash, "3"] & \langle (12) \rangle \arrow[ddll, dash, "3"] \\
\langle (123) \rangle \arrow[dr, dash, "2"] & & & \\
& S_3 & &
\end{tikzcd}$$

(End of Day 22)

5.3. Lemma: Let $k \subset L$ be a field extension. Suppose $\exists n \in \mathbb{N}$ such that $[k(\alpha) : k] \leq n$ for all $\alpha \in L$. Then

(i) $\exists \theta \in L$ such that $L = k(\theta)$

(ii) In particular, $[L : k] \leq n$

5.4. Lemma: Let $L \subset \mathbb{C}$ be a field and G be a finite subgroup of $\mathrm{Gal}_{\mathbb{Q}}(L)$. Let $F = L^G$ be the fixed field of G. If $\alpha \in L$, define

$$f_\alpha(x) = \prod_{\varphi \in G} (x - \varphi(\alpha))$$

Then $f_\alpha \in F[x]$

5.5. (Artin's Lemma): Let $L \subset \mathbb{C}$ be a field and G be a finite subgroup of $\mathrm{Gal}_{\mathbb{Q}}(L)$. Let $F = L^G$ be the fixed field of G. Then

(i) $F \subset L$ is finite

(ii) $F \subset L$ is normal

(iii) $\mathrm{Gal}_F(L) = G$

5.6. Remark:

(i) For any intermediate field $k \subset F \subset L$, we have

$$F \subset L^{\mathrm{Gal}_F(L)} = \Psi \circ \Phi(F)$$

(ii) For any subgroup $H < G$, we have

$$H \subset \mathrm{Gal}_{L^H}(L) = \Phi \circ \Psi(H)$$

(End of Day 23)

5.7. (Fundamental Theorem of Galois Theory - I): Let $k \subset L$ be a finite normal extension of subfields of $\mathbb{C}$ with Galois group G. Then

(i) For all $F \in \mathcal{F}$ and $H \in \mathcal{G}$,

$$F = \Psi \circ \Phi(F) \text{ and } H = \Phi \circ \Psi(H)$$

In particular, there is a one-to-one correspondence

$$\mathcal{F} \leftrightarrow \mathcal{G}$$

(ii) If $F \in \mathcal{F}$ is an intermediate field, then

$$[F : k] = [\mathrm{Gal}_k(L) : \mathrm{Gal}_F(L)]$$

5.8. Lemma: let $k \subset L$ be a finite extension, $F \in \mathcal{F}$ be an intermediate field, and $\psi \in \mathrm{Gal}_k(L)$, then

(i) $\psi(F) \in \mathcal{F}$

(ii)
$$\mathrm{Gal}_{\psi(F)}(L) = \psi \,\mathrm{Gal}_F(L) \psi^{-1}$$

5.9. (Fundamental Theorem of Galois Theory - II): Let $k \subset L$ be a finite normal extension of subfields of $\mathbb{C}$ with Galois group G. Then

(i) If $F \in \mathcal{F}$, $k \subset F$ is normal iff $\mathrm{Gal}_F(L) \lhd \mathrm{Gal}_k(L)$.

(ii) In that case, the conclusions of Theorem 4.4 hold.

5.10. Example: Consider $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Then $G = \mathrm{Gal}_k(L) \cong S_3$ via the identification $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\} \leftrightarrow \{1, 2, 3\}$. So if $H = \langle (23) \rangle < G$, then

(i) $L^H = \mathbb{Q}(\sqrt[3]{2})$

(ii) Hence, H is not normal in G.

The other examples in 5.2 can be justified similarly.

5.11. Theorem: Let $k \subset F$ be a finite field extension, then $\exists$ a field M such that

(i) $F \subset M$

(ii) $k \subset M$ is finite and normal

(iii) If L is any other field satisfying (i) and (ii), then $M \subset L$.

In other words, M is the smallest normal extension of k that contains F. This field M is called the normal closure of F over k

(End of Day 24)

5.12. Corollary: Any extension of degree 2 is a normal extension. (See HW 7)

IV. Solvability by Radicals

1. Radical Extensions

1.1. Example:

(i) Quadratic $f(x) = ax^2 + bx + c \in k[x]$, then

(a) Roots of f are given by the quadratic formula

(b) f splits in the field $k(\sqrt{r})$ where $r = b^2 - 4ac \in k$

(ii) Cubic $f(x) = x^3 - a$, then

(a) Roots of f are given by $\sqrt[3]{a}, \omega\sqrt[3]{a}, \omega^2\sqrt[3]{a}$

(b) f splits in the field $L = k(\sqrt[3]{a}, \omega)$

(iii) Cubic $f(x) = x^3 + px + q$, then

(a) Roots of f are given by Cardano's formula. If

$$A = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$B = \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Then the roots of f are

$$\{A + B, \omega A + \omega^2 B, \omega^2 A + \omega B\}$$

(b) f splits in the field $L = \mathbb{Q}(\omega, A, B)$

1.2. Definition:

(i) A field extension $k \subset L$, is called a <u>simple radical</u> extension of type $n \in \mathbb{N}$ if $\exists \alpha \in L$ such that

(a) $L = k(\alpha)$

(b) $\alpha^n \in k$

Equivalently, if $\exists a \in k$ such that $L = k(\alpha)$ where α is a root of $x^n - a \in k[x]$

(ii) Radical Extension $k \subset L$

(iii) We say $f \in k[x]$ is solvable by radicals if the splitting field F of f over k is contained in a radical extension of k

Note: $k \subset F$ itself need not be a radical extension.

1.3. Example:

(i) $k \subset k$ is simple radical.

(ii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ is simple radical.

(iii) If $k \subset L$ is an extension of degree 2, then

(a) $L = k(\sqrt{r})$ for some $r \in k$ (See HW 4.2)

(b) Hence, $k \subset F$ is a simple radical extension

(c) So any quadratic polynomial $f \in k[x]$ is solvable by radicals.

(iv) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is a simple radical extension.

(v) If $n \in \mathbb{N}$, $\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/n})$ is a simple radical extension. Hence, $x^n - 1$ is solvable by radicals.

(vi) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$ is a radical extension, because if $F = \mathbb{Q}(\sqrt[3]{2})$, then

$$\mathbb{Q} \subset F \subset L$$

is a chain of simple radical extensions. Hence, $f(x) = x^3 - 2$ is solvable by radicals over $\mathbb{Q}$.

(vii) $f(x) = x^3 - 3x + 1$, then

(a) f is solvable by radicals by Cardano's formula

(b) f has all real roots

(c) However, Cardano's formula involves $\sqrt{-3/4}$. So, one needs complex numbers to express these roots as radicals. This phenomenon is called 'Casus Irreducibilis'

(viii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a radical extension, but is not a simple radical extension. (with proof)

(End of Day 25)

1.4. Lemma: If $k \subset L$ is a radical extension, then there is a chain of subfields

$$k = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_n = L$$

such that $K_j \subset K_{j+1}$ is a simple radical extension of prime type for all $0 \leq j \leq n$.

1.5. Lemma: Let $k \subset L$ be a simple radical extension of prime type, then there exists an extension $k \subset L \subset M$ such that $k \subset M$ is finite, normal and radical.

1.6. Theorem: If $k \subset L$ is a radical extension, then there is an extension $k \subset L \subset M$ such that $k \subset M$ is finite, normal and radical.

1.7. Corollary: Let $k \subset \mathbb{C}$ be a field and $f \in k[x]$ with splitting field L. Then f is solvable by radicals iff $\exists$ a field extension $k \subset L \subset M$ such that $k \subset M$ is finite normal and radical.

1.8. Remark: Suppose $k \subset L$ is a simple radical extension of prime degree $p \in \mathbb{N}$. Write

$$L = k(\alpha), \text{ where } a := \alpha^p \in k$$

Let $f(x) = x^p - a$, and let

$$M = k(\sqrt[p]{a}, \zeta) \text{ where } \zeta = e^{2\pi i/p}$$

be the splitting field of f over k. Write $F = k(\zeta)$, then

(i) $k \subset F$ is normal. So $\text{Gal}_F(M) \lhd \text{Gal}_k(M)$

(ii) $G/H \cong \text{Gal}_k(F) = \text{Gal}_k(k(\zeta))$

1.9. Theorem: Let $k \subset L \subset E$ be finite extensions and $\beta \in E$. If $k \subset k(\beta)$ is normal, then

(i) $L \subset L(\beta)$ is finite and normal

(ii) The map

$$\varphi \mapsto \varphi\mid_{k(\beta)} \text{ from } \text{Gal}_L(L(\beta)) \to \text{Gal}_k(k(\beta))$$

is injective.

(End of Day 26)

1.10. Lemma: Let $p \in \mathbb{N}$ be prime, and let $F \subset \mathbb{C}$ be a field containing $\zeta = e^{2\pi i/p}$. Let $a \in F$, and let M be the splitting field field of $x^p - a \in F[x]$. Then

$$\text{Gal}_F(M) \cong \begin{cases} \{e\} & : F = M \\ \mathbb{Z}_p & : F \subsetneq M \end{cases}$$

1.11. Theorem: Let $k \subset \mathbb{C}$ be a field, and let $p \in \mathbb{N}$ be a prime. Let M be the splitting field of $f(x) = x^p - a \in k[x]$, and set $F = k(\zeta) \subset M$ where $\zeta = e^{2\pi i/p}$, then

(i) $\text{Gal}_F(M) \lhd \text{Gal}_k(M)$

(ii) $\text{Gal}_F(M)$ is cyclic

(iii) $\text{Gal}_k(M)/\text{Gal}_F(M)$ is cyclic

2. Solvable Groups

2.1. Definition: A finite group G is said to be <u>solvable</u> if there is a decreasing sequence (G_i) of subgroups of G

$$G = G_0 > G_1 > G_2 > \ldots > G_{n-1} > G_n = \{e\}$$

such that

(i) $G_i \lhd G_{i-1}$ for all $1 \leq i \leq n$

(ii) G_{i-1}/G_i is cyclic for all $1 \leq i \leq n$.

2.2. Examples:

(i) Every cyclic group is solvable.

(ii) $\mathbb{Z}_n \times \mathbb{Z}_m$ is solvable

(iii) S_3 is solvable

(iv) If $|G| = 8$, then G is solvable. (In particular, D_4 is solvable)

(v) S_4 is solvable.

(vi) Let $k \subset \mathbb{C}$, $p \in \mathbb{N}$ prime, and let M be the splitting field of $x^p - a \in k[x]$. Then $\mathrm{Gal}_k(M)$ is solvable (by 1.11)

(End of Day 27)

2.3. Theorem: Let G be a solvable group and $H < G$, then H is solvable.

2.4. Definition: If $A, B \subset G$, $AB = \{ab : a \in A, b \in B\}$

2.5. Lemma: If $H \lhd G$ and $K < G$, then

(i) $HK = KH$

(ii) $HK < G$

2.6. Theorem: Let G be a group, $H \lhd G$ and $K < G$, then

(i) $H \cap K \lhd K$

(ii)
$$\frac{K}{H \cap K} \cong \frac{HK}{H}$$

2.7. Theorem: Let G be a group, $H, K \lhd G$ such that $H \subset K$, then

(i) $H \lhd K$

(ii) $K/H \lhd G/H$

(iii)
$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

2.8. Theorem: Let G be a solvable group, $H \lhd G$, then G/H is solvable.

2.9. Theorem: Let G be a group and $H \lhd G$. Then, G is solvable iff H and G/H are both solvable.

2.10. Theorem: Let $k \subset M$ be a finite normal and radical field extension, then $\mathrm{Gal}_k(M)$ is solvable.

(End of Day 28)

2.11. Corollary: Let $k \subset \mathbb{C}$ be a field and $f \in k[x]$. If f is solvable by radicals, then $\mathrm{Gal}_k(f)$ is a solvable group.

3. An Insolvable Quintic

3.1. Definition: Simple group

3.2. Examples:

(i) $\mathbb{Z}_p$ is simple

(ii) If G is an abelian simple group, then G is finite and $G \cong \mathbb{Z}_p$ for some prime $p \in \mathbb{Z}$

(iii) If G is a solvable simple group, then $\exists p \in \mathbb{Z}$ prime such that $G \cong \mathbb{Z}_p$ (HW)

3.3. Remark:

(i) If $\tau \in S_n$, then τ can be expressed as a product of disjoint cycles. If $\tau = \sigma_1\sigma_2 \ldots \sigma_k$ is the cycle-decomposition of τ, then

$$o(\tau) = \text{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_k))$$

(ii) In particular, if $p := o(\tau)$ is a prime number, then τ is a product of disjoint p-cycles.

(iii) If $\tau \in S_n$, then τ can be expressed as a product of (possibly not disjoint) transpositions.

A_n is the collection of those $\tau \in S_n$ that can be expressed as a product of an even number of transpositions.

(iv) In A_5, define

$$\begin{aligned} C_2 &:= \{\tau \in A_5 : o(\tau) = 2\} = \{(ab)(cd) : \{a, b, c, d\} \text{ are distinct}\} \\ C_3 &:= \{\tau \in A_5 : o(\tau) = 3\} = \{3 - \text{cycles in } S_5\} \\ C_5 &:= \{\tau \in A_5 : o(\tau) = 5\} = \{5 - \text{cycles in } S_5\} \end{aligned}$$

3.4. Lemma: If $p \in \{2, 3, 5\}$, then A_5 is generated by C_p.

3.5. Theorem: A_5 is a simple group.

(End of Day 29)

3.6. Corollary: S_n is not solvable for $n \geq 5$

3.7. Lemma: Let $p \in \mathbb{N}$ be prime and suppose $G < S_p$ is a subgroup that contains a p-cycle and a transposition, then $G = S_p$

3.8. Theorem: Let p be a prime and f an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose f has precisely two non-real roots, then $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$

3.9. Example: Let $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$, then f is not solvable by radicals.

3.10. Remark:

(i) Example 3.9 indicates that the polynomial cannot be solved by radicals. However, the roots can be found by other methods.

(ii) Abel-Ruffini proved the existence of an insolvable quintic. Example 3.9 is a constructive proof of this theorem.

(iii) There may be other quintics which *can* be solved by radicals.

(End of Day 30)

4. Galois' Theorem

(Taken from [Rotman] and [Yoshida])

Note: Throughout this section, for each $p \in \mathbb{N}$ prime, write $\zeta_p := e^{2\pi i/p} \in \mathbb{C}$.

4.1. Lemma: Let G be a finite solvable group, then there is a normal series

$$G = G_0 > G_1 > G_2 > \ldots > G_n = \{e\}$$

such that, for each $0 \leq i \leq n-1$

(i) $G_{i+1} \lhd G_i$

(ii) G_i/G_{i+1} is a cyclic group of prime order

Note: Compare this to Lemma 1.4

4.2. Lemma: Let $F \subset L$ be a finite normal field extension and $p \in \mathbb{N}$ prime. Suppose that

(i) $\zeta_p \in F$

(ii) $\sigma \in \text{Gal}_F(L)$ has order p

Considering $\sigma : L \to L$ as an F-linear transformation, ζ_p is an eigen-value of σ.

4.3. (Kummer's Theorem): Let $F \subset L$ be a finite normal extension and $p \in \mathbb{N}$ prime. Suppose that

(i) $\zeta_p \in F$

(ii) $\text{Gal}_F(L) \cong \mathbb{Z}_p$

Then $\exists a \in F$ such that $L = F(\sqrt[p]{a})$

4.4. (Galois' Theorem - Special Case): Let $k \subset L$ be a finite normal extension such that $\text{Gal}_k(L)$ is solvable. Assume that

$$\forall \quad \text{primes } p \mid |\text{Gal}_k(L)|, \quad \zeta_p \in k$$

Then $k \subset L$ is a radical extension.

(End of Day 31)

4.5. (Accessory Irrationalities): Let $k \subset L$ be a finite normal field extension and $\beta \in \mathbb{C}$. Then

(i) $k(\beta) \subset L(\beta)$ is a finite normal extension

(ii) The map

$$\mathrm{Gal}_{k(\beta)}(L(\beta)) \to \mathrm{Gal}_k(L) \text{ given by } \varphi \mapsto \varphi|_L$$

is a well-defined injective homomorphism.

4.6. (Galois' Theorem - General Case): Let $k \subset L$ be a finite normal extension such that $\mathrm{Gal}_k(L)$ is solvable, then $\exists$ a field M such that $k \subset L \subset M$ and $k \subset M$ is radical.

4.7. Corollary: Let $k \subset \mathbb{C}$ and $f \in k[x]$. Then f is solvable by radicals iff $\mathrm{Gal}_k(f)$ is a solvable group.

4.8. Corollary: Let $k \subset \mathbb{C}$ and $f \in k[x]$ have degree ≤ 4, then f is solvable by radicals.

4.9. Corollary (Abel): If $f \in \mathbb{Q}[x]$ has an abelian Galois group, then f is solvable by radicals.

V. Galois Groups of Polynomials

1. Cyclotomic Polynomials

1.1. Definition: Fix $n \in \mathbb{N}$

(i) $\mu_n = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$.

Note: μ_n is a cyclic group of order n.

(ii) Elements of μ_n are called roots of unity. Generators of μ_n are called primitive root of unity.

(iii) $\mathbb{Q}(\mu_n)$ is the splitting field of $x^n - 1$, and is called the n^{th} cyclotomic field.

(iv) If G is a group, then $\text{Aut}(G) = \{\varphi : G \to G : \varphi \text{ is an isomorphism}\}$.

1.2. Theorem: Let $k \subset \mathbb{C}$ be any field, then

(i) $k \subset k(\mu_n)$ is a finite normal extension.

(ii) The map

$$\Gamma : \text{Gal}_k(k(\mu_n)) \to \text{Aut}(\mu_n)$$

given by

$$\varphi \mapsto \varphi|_{\mu_n}$$

is a well-defined injective homomorphism.

1.3. Recall:

(i) If R is a ring, $R^* = \{u \in R : \exists v \in R \text{ such that } uv = 1\}$.

(ii) R^* is a group under multiplication, called the group of units of R.

(iii) If $R = \mathbb{Z}_n$, then

$$R^* = \{\overline{a} \in \mathbb{Z}_n : (a,n) = 1\}$$

1.4. Theorem: $\text{Aut}(\mu_n) \cong \mathbb{Z}_n^*$

(End of Day 32)

1.5. Lemma: Let $n \in \mathbb{N}$ and $\zeta \in \mu_n$ be a primitive n^{th} root of unity. If $(a,n) = 1$, then ζ^a is a primitive n^{th} root of unity. (HW)

1.6. Definition: n^{th} Cyclotomic polynomial

1.7. Lemma: For any $n \in \mathbb{N}, x^n - 1 = \prod_{d|n} \Phi_d(x)$

1.8. Examples:

(i) $\Phi_1(x) = x - 1$

(ii) If $p \in \mathbb{N}$ prime, then $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$

(iii) $\Phi_6(x) = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1$

1.9. Theorem: Φ_n is monic and in $\mathbb{Z}[x]$

1.10. Remark: Let $k = \mathbb{Z}_p$ and $f \in k[x]$, then

(i) f is said to be inseparable if $\exists$ a field extension $k \subset L$ such that f has multiple roots in L.

Note: These roots will not be in $\mathbb{C}$, but in some larger field.

(ii) f is said to be separable if it is not inseparable.

(iii) We may define $D(f)$ as before.

(iv) Theorem II.4.3 holds verbatim: If $f \in k[x]$, then f is separable iff $(f, D(f)) = 1$ in $k[x]$

1.11. Lemma: If $p \in \mathbb{N}$ prime and $n \in \mathbb{N}$ such that $p \nmid n$, then $x^n - 1 \in \mathbb{Z}_p[x]$ is separable.

1.12. Lemma: If $p \in \mathbb{N}$ is prime, then for any $g \in \mathbb{Z}_p[x]$, $g(x)^p = g(x^p)$

1.13. Theorem: Let $n \in \mathbb{N}$ and $\zeta \in \mu_n$ be any primitive n^{th} root of unity. If $(a, n) = 1$, then ζ and ζ^a have the same minimal polynomial over $\mathbb{Q}$

(End of Day 33)

1.14. Corollary: Φ_n is the minimal polynomial of $\zeta = e^{2\pi i/n}$ over $\mathbb{Q}$.

1.15. Corollary: $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\mu_n)) \cong \mathbb{Z}_n^*$

1.16. Remark:

(i) If $\mathbb{Q} \subset k \subset \mathbb{Q}(\mu_n)$ is any intermediate normal extension, then $\mathbb{Q} \subset k$ is an abelian extension (since $\mathbb{Z}_n^*$ is abelian).

(ii) The converse is called the Kronecker-Weber Theorem: If $\mathbb{Q} \subset k$ is any finite normal extension such that $\mathrm{Gal}_{\mathbb{Q}}(k)$ is abelian, then $\exists n \in \mathbb{N}$ such that $k \subset \mathbb{Q}(\mu_n)$.

2. Cubic Polynomials

2.1. Remark: Let $f \in k[x]$ be irreducible of degree n with splitting field L and Galois group G. Then

(i) $G < S_n$ (III.3.5)

(ii) G is a transitive subgroup of S_n (III.4.2)

(iii) $n \mid |G|$ (HW)

(iv) If $\deg(f) = 2$, then $G \cong \mathbb{Z}_2$

(v) If $\deg(f) = 3$, then $G \cong A_3 \cong \mathbb{Z}_3$ or S_3

(vi) If $\deg(f) = 3$ and f has one complex root, then $G \cong S_3$ by Theorem IV.3.8.

But what if f has all real roots? Can we conclude that $G \cong \mathbb{Z}_3$?

2.2. Definition: Let $f \in k[x]$ be of degree n with roots $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

(i) $\Delta := \prod_{i<j}(\alpha_i - \alpha_j)$

(ii) $D_f := \Delta^2$ is called the <u>discriminant</u> of f

Note: Since f is irreducible, it is separable (II.4.4), and hence $D_f \neq 0$

2.3. Example:

(i) $f(x) = ax^2 + bx + c$, then $D_f = (b^2 - 4ac)/2a$

(ii) $f(x) = x^3 + ax + b$, then $D_f = -4a^3 - 27b^2$

(iii) $f(x) = x^3 + ax^2 + bx + c$, then set $h(x) = f(x - a/3) = x^3 + px + q$, then

$$D_h = D_f = -4p^3 - 27q^2$$

2.4. Definition: If $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n \in k[x]$, then

(i) f is called <u>reduced</u> if $a_{n-1} = 0$

(ii) The <u>associated reduced polynomial</u> of f is $\tilde{f}(x) = f(x - a_{n-1}/n)$

Note: $D_{\tilde{f}} = D_f$ and $\text{Gal}_k(f) = \text{Gal}_k(\tilde{f})$

2.5. Theorem: Let $f \in k[x]$ as in Definition 2.2. Then

(i) For any $\varphi \in G \subset S_n$,
$$\varphi(\Delta) = \text{sgn}(\varphi)\Delta$$

(ii) $D_f \in k$

2.6. Corollary: If $f \in k[x]$ be separable with Galois group $G < S_n$, then

(i) $\text{Gal}_{k(\Delta)}(L) = G \cap A_n$

(ii) $k(\Delta) = L^{G \cap A_n}$

2.7. Theorem: Let $f \in k[x]$ be an irreducible cubic with Galois group G and discriminant D_f
$$G \cong \begin{cases} \mathbb{Z}_3 & : \sqrt{D_f} \in k \\ S_3 & : \sqrt{D_f} \notin k \end{cases}$$

(End of Day 34)

2.8. Corollary: Let $f \in k[x]$ be an irreducible cubic with discriminant D_f and roots $\{u, v, w\}$. Then $F = k(u, \sqrt{D_f})$ is the splitting field of f

2.9. Lemma: Let $F \subset \mathbb{R}$ be a field and $p \in \mathbb{N}$ prime, $a \in F$. Then, $[F(\sqrt[p]{a}) : F]$ is either 1 or p

2.10. (Casus Irreducibilis): Let $f \in \mathbb{Q}[x]$ be an irreducible cubic with 3 real roots. If $\mathbb{Q} \subset M$ is any radical extension such that f splits in M, then $M \not\subseteq \mathbb{R}$. In particular, if L is the splitting field of f over $\mathbb{Q}$, then $\mathbb{Q} \subset L$ is not a radical extension.

Note: This means that any formula for expressing the roots in terms of the coefficients and their radicals must necessarily involve non-real numbers.

2.11. Examples:

(i) $f(x) = x^3 - 2$, then $D_f = -108$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$. Also, f has exactly 2 complex roots, so we may apply Theorem IV.3.8.

(ii) $f(x) = x^3 - 4x + 2$, then $D_f = 202$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$. However, all the roots of f are real (compare with Theorem IV.3.8)

(iii) $f(x) = x^3 - 3x + 1$, then $D_f = 81$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_3$. However, all the roots are real, so by Casus Irreducibilis, any radical extension in which f splits must necessarily contain non-real complex numbers. (See Example IV.1.3(vii))

3. Quartic Polynomials

3.1. Remark: Let $f \in k[x]$ be an irreducible quartic polynomial with Galois group G

(i) Let $\tilde{f}$ be the associated reduced polynomial, then $G = \mathrm{Gal}_k(\tilde{f})$, so we assume WLOG that

$$f(x) = x^4 + qx^2 + rx + s$$

(ii) By HW 10, $4 \mid |G|$ and G is one of the following

(a) $\mathbb{Z}_4 \cong \langle (1234) \rangle$

(b) $V_4 := \{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

(c) $D_4 \cong \langle (1234), (13) \rangle$

(d) A_4

(e) S_4

(iii) By 2.6, $G \subset A_4$ iff $\sqrt{D_f} \in k$. Hence, we have

$$G \cong \begin{cases} V_4 \text{ or } A_4 & : \sqrt{D_f} \in k \\ \mathbb{Z}_4, D_4, \text{ or } S_4 & : \sqrt{D_f} \notin k \end{cases}$$

(iv) As we did with A_4, we want to identify the fixed field of $G \cap V_4$

(End of Day 35)

3.2. Lemma: Let $f \in k[x]$ be an irreducible quartic with roots $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, splitting field L and Galois group $G < S_4$. Then set

$$\begin{aligned} u &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ v &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ w &= \alpha_1\alpha_4 + \alpha_2\alpha_3 \end{aligned}$$

and set $F = k(u, v, w) \subset L$. Then

(i) $\mathrm{Gal}_F(L) = G \cap V_4$

(ii) $L^{G \cap V_4} = F$

(iii) $G = V_4 \Leftrightarrow F = k$

3.3. Theorem: Let $f \in k[x]$ as before and u, v, w as in Lemma 3.2, then

$$g(x) = (x-u)(x-v)(x-w) \in k[x]$$

This polynomial is called the <u>resolvent cubic</u> of f.

3.4. Lemma: The resolvent cubic of $f(x) = x^4 + ax^3 + bx^2 + cx + d \in k[x]$ is

$$g(x) = x^3 - bx^2 + (ac - 4d)x - (a^2 d + c^2 - 4bd)$$

3.5. Lemma: If $f \in k[x]$ is an irreducible cubic and $g \in k[x]$ is the resolvent cubic of f, then

(i) $D_f = D_g$

(ii) $k(u, v, w) = k(u, \sqrt{D_f})$

3.6. Theorem: Let $f \in k[x]$ be an irreducible quartic as above, then the Galois group G can be described in the following table :

Case No.	$\sqrt{D_f} \in k$	g irreducible in $k[x]$	G
I	Y	Y	A_4
II	Y	N	V_4
III	N	Y	S_4
IV	N	N	D_4 or $\mathbb{Z}_4$

(End of Day 36)

3.7. Examples:

(i) $f(x) = x^4 - x - 1 \in \mathbb{Q}[x]$, then

(a) f is irreducible in $\mathbb{Q}[x]$ since it is irreducible in $\mathbb{Z}_2[x]$ (using I.5.7)

(b) The resolvent cubic of f is $g(x) = x^3 + 4x - 1$.

(c) g has no roots in $\mathbb{Q}$ (by the rational root theorem), so it is irreducible.

(d) The discriminant of f is $D_f = D_g = -283$, so $\sqrt{D_f} \notin \mathbb{Q}$.

(e) Hence,

$$G \cong S_4$$

(ii) $f(x) = x^4 + 8x + 12 \in \mathbb{Q}[x]$, then

(a) f is irreducible in $\mathbb{Q}[x]$ since it has no roots in $\mathbb{Q}$ (by the rational root theorem) and it cannot be factored into two quadratic factors in $\mathbb{Z}[x]$. So f is irreducible in $\mathbb{Z}[x]$, and so in $\mathbb{Q}[x]$ by Gauss' Lemma.

(b) The resolvent cubic of f is $g(x) = x^3 - 48x - 64$

(c) g is irreducible in $\mathbb{Q}[x]$ since it is irreducible in $\mathbb{Z}_5[x]$ (using I.5.7)

(d) The discriminant of f is $D_f = D_g = 576^2 \Rightarrow \sqrt{D_f} \in \mathbb{Q}$.

(e) Hence,
$$G \cong A_4$$

(iii) $f(x) = x^4 + 1 \in \mathbb{Q}[x]$, then

(a) f is irreducible (HW 3.3)

(b) The resolvent cubic of f is
$$g(x) = x^3 - 4x = x(x-2)(x+2)$$
which is reducible in $\mathbb{Q}$

(c) The discriminant is $D_f = D_g = [(0+2)(0-2)(2+2)]^2$, so $\sqrt{D_f} \in \mathbb{Q}$

(d) Hence,
$$G \cong V_4$$
[Compare this with Quiz 2. Also, $f = \Phi_8$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$]

3.8. Theorem: Let $f \in k[x]$ be an irreducible quartic such that Case IV applies. Then $G \cong D_f$ iff f is irreducible over $k(\sqrt{D_f})$ (and $G \cong \mathbb{Z}_4$ otherwise).

3.9. Theorem: If $f \in \mathbb{Q}[x]$ be an irreducible quartic with Galois group $\mathbb{Z}_4$, then $D_f > 0$.

3.10. Examples:

(i) $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, then

(a) f is irreducible by Eisenstein's criterion with $p = 2$

(b) The resolvent cubic of f is $g(x) = x^3 + 8x = x(x - 2\sqrt{2}i)(x + 2\sqrt{2}i)$

(c) So $D_f = D_g = [(2\sqrt{2}i)(-2\sqrt{2}i)(2\sqrt{2}i + 2\sqrt{2}i)]^2 < 0 \Rightarrow \sqrt{D_f} \notin \mathbb{Q}$, so Case IV applies.

(d) But $D_f < 0$, so by 3.10,
$$G \cong D_4$$

(ii) $f(x) = x^4 + 5x + 5$, then

(a) f is irreducible by Eisenstein's criterion with $p = 5$

(b) The resolvent cubic of f is $g(x) = (x-5)(x^2 + 5x + 5)$ whose roots are
$$\{5, \frac{-5+\sqrt{5}}{2}, \frac{-5-\sqrt{5}}{2}\}$$

(c) Hence, $D_f = D_g = 5 \times 55^2$, so $\sqrt{D_f} \notin \mathbb{Q}$. Hence, Case IV applies.

(d) f factors over $\mathbb{Q}(\sqrt{D_f}) = \mathbb{Q}(\sqrt{5})$ as

$$f(x) = \left(x^2 + \sqrt{5}x + \frac{5-\sqrt{5}}{2}\right)\left(x^2 - \sqrt{5}x + \frac{5+\sqrt{5}}{2}\right)$$

Hence

$$G \cong \mathbb{Z}_4$$

(End of Day 37)

VI. Instructor Notes

0.1. The main goal was to prove Theorem IV.4.7 and Example IV.3.9. All choices I made were designed towards that. Furthermore, many choices were dictated by the fact that the incoming Integrated PhD students had a somewhat weaker background than the existing IISER students.

0.2. I started the course following [Stewart], while Chapter IV and V were mostly from [Rotman]. The Primitive element theorem was moved up front - this turned out to be an extremely good decision as it greatly simplified many subsequent theorems.

0.3. Throughout the course,we only discussed subfields of $\mathbb{C}$ to simplify the exposition. Therefore, I did not discuss finite fields (except briefly in §V.1) and separability also got short shrift. I had hoped to discuss finite fields at the end of the course, but ran out of time.

0.4. I did not discuss ruler and compass constructions. Nor did I prove that π and e were transcendental. I do not consider this a major loss.

Bibliography

[Stewart] Ian Stewart, *Galois Theory (3rd Ed.)*

[Garling] DJH Garling, *A Course in Galois Theory*

[Rotman] Joseph Rotman, *Galois Theory (2nd Ed.)*

[Gowers] T. Gowers, https://www.dpmms.cam.ac.uk/~wtg10/cubic.html

[Fefferman] C. Fefferman, *An Easy Proof of the Fundamental Theorem of Algebra*, http://www.jstor.org/stable/2315823

[Greenberg] R. Greenberg, *The Primitive Element Theorem*, http://www.math.washington.edu/~greenber/PrimElemThm.pdf

[Yoshida] T. Yoshida, *Galois Theory Notes*, https://www.dpmms.cam.ac.uk/~ty245/Yoshida_2012_Galois.pdf