MTH 401: Fields and Galois Theory

Semester 1, 2016-2017

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

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0$$

(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 with $y = x - a/3$ 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) $\sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }$, etc. (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!

I. Polynomials

1. Ring Theory

1.1. Definition:

(i) A ring R is a set with two binary operations $+$ and $\times$ satisfying:

(a) $(R, +)$ is an abelian group with identity denoted by 0

(b) $\times$ is associative: $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$

(c) The distributive laws hold: For all $a, b, c \in R$

A. $(a + b) \times c = (a \times c) + (b \times c)$

B. $a \times (b + c) = (a \times b) + (a \times c)$

(ii) If R is a ring, an element $e \in R$ is called the identity of R if $a \times e = e \times a = a$ for all $a \in R$.

(iii) A ring R is said to be commutative if $a \times b = b \times a$ for all $a, b \in R$.

(iv) A commutative ring R is said to be an integral domain if $ab = 0$ implies either $a = 0$ or $b = 0$.

(v) A commutative ring is said to be a field if $1 \neq 0$ and for ever $0 \neq a \in R, \exists b \in R$ such that $ab = ba = 1$.

Note: The element $b \in R$ is unique (Check!) and is denoted by a^{-1}.

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.

Proof. Clearly, F is an abelian group and is closed under multiplication. To see that inverses exists, choose $a, b \in \mathbb{Q}$ at least one of which is non-zero, and consider

$$y = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

since $\sqrt{2} \notin \mathbb{Q}$, the denominator is non-zero, and a rational number. Hence, $y \in F$ and is clearly the inverse of $a + b\sqrt{2}$ in F. □

(iv) Define

$$K := \{a + b\pi : a, b \in \mathbb{Q}\} \subset \mathbb{C}$$

then K is not a ring.

Proof. If it were a ring, then $\pi^2 \in K$, which means that π satisfies a quadratic equation over $\mathbb{Q}$. However, π does not satisfy any polynomial over $\mathbb{Q}$. □

(End of Day 1)

1.3. Definition:

(i) A subring S of a ring R is a subset such that

(a) $(S, +)$ is a subgroup of $(R, +)$

(b) S is closed under multiplication.

(ii) An ideal I of a ring R is a subring of R such that if $a \in I, b \in R$ then $ab \in I$. Note: If I is an ideal in R, we write $I \lhd R$.

(iii) Let R and S be two rings. A function $\varphi : R \to S$ is called a ring homomomorphism if

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

(iv) A bijective ring homomorphism is called a ring isomorphism.

Note:

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

(b) Henceforth, we will assume that all rings are commutative with $1 \neq 0$, and that if $\varphi : R \to S$ is a ring homomorphism, then $\varphi(1_R) = 1_S$

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 $\mathbb{C}$

Proof. If $\varphi : \mathbb{Q} \to \mathbb{C}$ is a ring homomorphism, then $\varphi(1) = 1$, so $\varphi(n) = n$ for all $n \in \mathbb{N}$, and hence for all $n \in \mathbb{Z}$. Now for $x = p/q \in \mathbb{Q}$, note that

$$q\varphi(x) = \varphi(qx) = \varphi(p) = p$$

and so $\varphi(x) = x$ for all $x \in \mathbb{Q}$. □

(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.

1.8. Theorem: Let R be a ring and $I \lhd R$, then consider the quotient group $(R/I, +)$. We define a multiplication on R/I by

$$(a + I)(b + I) := ab + I$$

Then this is well-defined, and R/I forms a ring with respect to these operations called the quotient ring. Furthermore, the map $\pi : R \to R/I$ given by $a \mapsto a + I$ is a ring homomorphism, and is called the quotient map.

2. Polynomial Rings

2.1. Definition: Let R be a ring and x an indeterminate.

(i) A polynomial over R is a formal expression

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

where $a_i \in \mathbb{R}$ for all $0 \leq i \leq n$

Note: If $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, then $f(x) = g(x)$ iff $n = m$ and $a_i = b_i$ for all i. For instance, $x \neq x^2$ in $\mathbb{Z}_2[x]$

(ii) We may add and multiply polynomials in the usual way (by collecting *like terms*), and this makes the set $R[x]$ of all such polynomials a ring. This is called the polynomial ring over R in one variable.

Note that $R[x]$ is a commutative ring with $1_{R[x]} = 1_R \neq 0$ (Check!)

(iii) If $f(x) = a_0 + a_x + \ldots + a_n x^n \in \mathbb{R}[x]$ then

$$\deg(f) := \max\{j : a_j \neq 0\}$$

is called the degree of f

2.2. Lemma: Let $f, g \in R[x]$

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

(ii) If R is an integral domain and $f, g \neq 0$, then $\deg(fg) = \deg(f) + \deg(g)$. In particular, $R[x]$ is an integral domain.

Proof. The first part follows trivially from the definition of addition. For part (ii), write

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \text{ and } g(x) = b_0 + b_1 x + \ldots + b_m x^m$$

with $a_n, b_m \neq 0$. Then

$$fg(x) = a_0 b_0 + (a_1 b_0 + b_1 a_0)x + \ldots + a_n b_m x^{n+m}$$

and $a_n b_m \neq 0$ (since R is an integral domain). Hence, $\deg(fg) = n + m$ □

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

$$f = tg + r$$

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

Proof. (a) Existence: Write $f(x) = a_0 + a_1x + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + \ldots + b_mx^m$ with $b_m \neq 0$.

(i) If $f = 0$, then take $t = r = 0$, so we assume $a_n \neq 0$

(ii) If $n < m$, then $t = 0, r = f$ works.

(iii) If $n = m$: Take $t = a_nb_n^{-1}$ (possible since k is a field), so that

$$(f - tg)(x) = \sum_{i=0}^{n-1} c_ix^i \text{ where } c_i = a_i - a_nb_n^{-1}b_i$$

In particular, $\deg(f - tg) \leq n - 1 < \deg(g)$ as required.

(iv) If $n > m$, we assume by induction that the theorem is true for any polynomial $h \in k[x]$ with $\deg(h) < n$. Now take

$$h(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$$

Then, as above $\deg(h) < n$, so by induction hypothesis, $\exists t_1, r_1 \in k[x]$ such that

$$h = t_1g + r_1 \text{ and } \deg(r_1) < \deg(g)$$
$$\Rightarrow f = (a_nb_m^{-1}x^{n-m} + t_1)g + r_1 \text{ and } \deg(r_1) < \deg(g)$$

as required.

(b) Uniqueness: Suppose

$$f = t_1g + r_1 \text{ and } f = t_2g + r_2$$

with r_i as in the statement. Then

$$(t_1 - t_2)g = r_2 - r_1 \qquad (*)$$

So if $t_1 \neq t_2$, then by Lemma 2.2(ii),

$$\begin{aligned}\deg(g) &\leq \deg(t_1 - t_2) + \deg(g)\\ &= \deg((t_1 - t_2)g)\\ &= \deg(r_2 - r_1)\\ &\leq \max\{\deg(r_2), \deg(r_1)\}\\ &< \deg(g)\end{aligned}$$

which is clearly a contradiction. Hence, $t_1 = t_2$ and so $r_2 = r_1$ by $(*)$

□

2.4. Definition:

(i) For $a, b \in R$, we say that b divides a if $\exists c \in R$ such that $bc = a$. If this happens, we write $b \mid a$.

(ii) For $a \in R$, the principal ideal generated by a is the set

$$(a) := \{ax : x \in R\} = \{b \in R : a \mid b\}$$

An ideal I is principal if $\exists a \in R$ such that $I = (a)$. Then, such an element $a \in R$ is called a generator of I. (Note: A generator of a principal ideal is not, in general, unique.)

(iii) A principal ideal domain (PID) is an integral domain each of whose ideals is principal.

(End of Day 2)

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

Proof. $k[x]$ is an integral domain by Lemma 2.2, so it suffices to show that every ideal in $k[x]$ is principal. If $I \lhd k[x]$, then the set $S := \{\deg(f) : f \in I\} \subset \mathbb{N}$ has an minimal element. So $\exists f_0 \in I$ such that

$$\deg(f_0) \leq \deg(f) \quad \forall f \in I$$

We claim that $I = (f_0)$. Since $f_0 \in I$, we have $(f_0) \subset I$. Conversely, suppose $f \in I$, then by Euclidean division, $\exists t, r \in k[x]$ such that

$$f = tf_0 + r$$

where $r = 0$ or $\deg(r) < \deg(f_0)$. Since $r = f - tf_0 \in I$, it follows that $r = 0$ and so $f \in (f_0)$. This is true for any $f \in I$, so $I = (f_0)$ □

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

(i) Define $\varphi_\alpha : R[x] \to R$ by

$$a_0 + a_1x + \ldots + a_nx^n \mapsto a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

Note that φ_α is a ring homomorphism, and is called the evaluation map at α. We write $f(\alpha) := \varphi_\alpha(f)$ for any $f \in R[x]$

(ii) α is said to be a root of $f \in R[x]$ if $f(\alpha) = 0$.

2.7. (Remainder Theorem): Let k be a field. 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 $(x - \alpha) \mid f(x)$ in $k[x]$

Proof. We prove only (i) since (ii) follows trivially. By Euclidean division, $\exists t, r \in R[x]$ such that

$$f(x) = (x - \alpha)t(x) + r(x)$$

with either $r = 0$ or $\deg(r) < \deg(x - \alpha) = 1$. Hence, $r(x) \in R$ is a constant, say c. Applying the evaluation homomorphism, since $\varphi_\alpha(x - \alpha) = 0$, we have

$$f(\alpha) = 0 + r(\alpha) = c$$

completing the proof. □

2.8. Definition: Let R be a ring, $f \in R[x]$ and $\alpha \in R$ be a root of f.

(i) We say that α is a root of multiplicity $m \in \mathbb{N}$ if

$$(x - \alpha)^m \mid f \text{ and } (x - \alpha)^{m+1} \nmid f$$

(ii) A root with multiplicity 1 is said to be a simple root of f

2.9. Corollary: Let k be a field, and $0 \neq f \in k[x]$. Then the number of roots of f in k, counted with multiplicity, is $\leq \deg(f)$.

Proof. If f has n roots $\alpha_1, \alpha_2, \dots, \alpha_n$ with multiplicity $m_1, m_2, \dots, m_n$ respectively, then by induction on the Remainder theorem, $\exists g \in R[x]$ such that

$$f(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \dots (x - \alpha_n)^{m_n} g(x)$$

Since $f \neq 0$, by Lemma 2.2,

$$\deg(f) = m_1 + m_2 + \dots + m_n + \deg(g) \geq \sum_{i=1}^{n} m_i$$

as required. □

3. Fundamental Theorem of Algebra

3.1. Definition: Consider the set $\mathbb{R}^2$ with the operations

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

$$(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$$

These operations make $\mathbb{R}^2$ a field, which is called the field of complex numbers, denoted by $\mathbb{C}$.

(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 express uniquely in the form $z = x + iy$ for $x, y \in \mathbb{R}$

(iv) For $\theta \in \mathbb{R}$, write $e^{i\theta} := \cos(\theta) + i\sin(\theta) \in \mathbb{C}$. Then, for any $z = x + iy \in \mathbb{C}$, set

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

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

Then $z = re^{i\theta}$ is called the polar form of z. Furthermore, if $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, then $z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$

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

(i) $z^n = r^n e^{in\theta}$. 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 call primitive n^{th} roots of unity.

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

Proof. For any $z_1, z_2 \in \mathbb{C}$, we have $||z_1| - |z_2|| \leq |z_1 - z_2|$ [Check!]. Hence, the function

$$F : D \to \mathbb{R} \text{ given by } z \mapsto |f(z)|$$

is continuous. Now use the fact that D is compact by the Heine-Borel theorem. □

3.5. Lemma: Let $f \in \mathbb{C}[x] \setminus \mathbb{C}$ and $r > 0$, then $\exists M > 0$ such that if $|z| > M$, then $|f(z)| > r$.

[Equivalently, $\lim_{|z|\to\infty} |f(z)| = +\infty$]

Proof. Write $f(z) = a^n z^n + a_{n-1}z^{n-1} + \ldots + a_0$, then

$$|f(z)| = |z|^n \left| a_n + \frac{a_{n-1}}{z} + \ldots + \frac{a_0}{z^n} \right|$$

Since $|z_1 + z_2| \geq ||z_1| - |z_2||$ for any two $z_1, z_2 \in \mathbb{C}$ (Why?), we have

$$|f(z)| \geq |z|^n \left[|a_n| - \sum_{k=1}^{n-1} \frac{|a_{n-k}|}{|z|^k} \right]$$

Now for each $1 \leq k \leq n-1, \exists M_k > 0$ such that

$$\frac{|a_{n-k}|}{M_k^k} < \frac{|a_n|}{2(n-1)}$$

and $\exists M_0 > 0$ such that

$$M_0^n \frac{|a_n|}{2} > r$$

Then if $M = \max\{M_0, M_1, \ldots, M_n\}$, then if $|z| > M$, we have

$$\begin{aligned} |f(z)| &\geq M^n \left[|a_n| - \sum_{k=1}^{n-1} \frac{|a_{n-k}|}{M^k} \right] \\ &\geq M^n \left[|a_n| - \sum_{k=1}^{n-1} \frac{|a_n|}{2(n-1)} \right] \\ &\geq M^n \left[|a_n| - \frac{|a_n|}{2} \right] \\ &\geq M^n \frac{|a_n|}{2} \geq r \end{aligned}$$

□

(End of Day 3)

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

Proof. Write $f(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$, then by the previous lemma, $\exists M > 0$ such that if $|z| > M$, then $|f(z)| \geq |a_0|$. Furthermore, on the disc $D = \{z \in \mathbb{C} : |z| \leq M\}$, f attains a minimum at a point $\alpha \in D$ so that

$$|f(\alpha)| \leq |f(z)| \quad \forall z \in D$$

However, $0 \in D$ so $|f(\alpha)| \leq |a_0| \leq |f(z)|$ for all $z \in \mathbb{C} \setminus D$, and so α is a global minimum. □

3.7. (Fundamental Theorem of Algebra): Suppose $f \in \mathbb{C}[x] \setminus \mathbb{C}, \exists \alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. (See [Fefferman])

Proof. (i) Choose $\alpha \in \mathbb{C}$ by the previous lemma so that $|f(\alpha)| \leq |f(z)| \quad \forall z \in \mathbb{C}$. Writing

$$f(z) = f((z-\alpha) + \alpha)$$

and expanding, we may write $f(z) = g(z - \alpha)$ for some polynomial $g \in \mathbb{C}[x]$. Furthermore, $f(\alpha) = g(0)$, so

$$|g(0)| \leq |g(z)| \quad \forall z \in \mathbb{C}$$

Thus, it suffices to show that $g(0) = 0$.

(ii) Write $g(z) = c_0 + c_1 z + \ldots + c_n z^n$ and let $1 \leq j \leq n$ be the smallest number such that $c_j \neq 0$. Hence, we may write

$$g(z) = c_0 + c_j z^j + z^{j+1} R(z)$$

for some polynomial $R \in \mathbb{C}[x]$. Since $c_j \neq 0, \exists \beta \in \mathbb{C}$ such that $\beta^j = -c_0/c_j$ (by De Moivre's theorem). Hence,

$$c_j \beta^j = -c_0$$

(iii) Let $D = \{z \in \mathbb{C} : |z| \leq |\beta|\}$, then D is compact, so $\exists M > 0$ such that

$$|R(z)| \leq M \quad \forall z \in D$$

(iv) Now let $0 < \epsilon < 1$ be arbitrary to be chosen later, then

$$\begin{aligned} |g(\epsilon\beta)| &= |c_0 + \epsilon^j c_j \beta^j + \epsilon^{j+1}\beta^{j+1} R(\epsilon\beta)| \\ &\leq |c_0 + \epsilon^j c_j \beta^j| + \epsilon^{j+1}|\beta|^{j+1}|R(\epsilon\beta)| \\ &\leq |c_0 - \epsilon^j c_0| + \epsilon^{j+1}|\beta|^{j+1} M \\ &= (1-\epsilon^j)|c_0| + \epsilon^{j+1}|\beta|^{j+1} M \\ &= |c_0| - \epsilon^j \left[|c_0| - \epsilon|\beta|^{j+1} M\right] \end{aligned}$$

Hence if $c_0 \neq 0$, then we may choose $0 < \epsilon < 1$ such that

$$\epsilon < \frac{|c_0|}{|\beta|^{j+1} M}$$

so that

$$|g(\epsilon\beta)| < |c_0| = |g(0)|$$

This contradicts step (i), and so $c_0 = 0$ must hold as required.

□

3.8. 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

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

Proof. HW. □

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

Proof. Let $f \in \mathbb{R}[x]$, we induct on $\deg(f)$: If $\deg(f) \leq 2$ then there is nothing to prove. If $\deg(f) > 2$, assume that the theorem is true for any polynomial $g \in \mathbb{R}[x]$ with $\deg(g) < \deg(f)$. By FTA, choose a root $\alpha \in \mathbb{C}$.

(i) If $\alpha \in \mathbb{R}$, then $(x-\alpha) \mid f(x)$ in $\mathbb{R}[x]$, so $\exists g \in \mathbb{R}[x]$ such that

$$f(x) = (x-\alpha)g(x)$$

Now apply the induction hypothesis to g

(ii) If $\alpha \in \mathbb{C} \setminus \mathbb{R}$, then, since $f \in \mathbb{R}[x]$, we have

$$f(\overline{\alpha}) = \overline{f(\alpha)} = 0$$

and so $\overline{\alpha}$ is also a root of f in $\mathbb{C}$. Hence, $h(x) := (x-\alpha)(x-\overline{\alpha}) \in \mathbb{R}[x]$ divides f in $\mathbb{C}[x]$, so $\exists g \in \mathbb{C}[x]$ such that

$$f(x) = h(x)g(x)$$

By induction hypothesis, it suffices to prove that $g \in \mathbb{R}[x]$. Write $h(x) = x^2 + ax + b$ and $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, then

$$f(x) = a_0 + a_1 x + \ldots + a_{m+2}x^{m+2}$$

(a) $b_m = a_{m+2} \in \mathbb{R}$

(b) By (reverse) induction, assume that $b_j \in \mathbb{R}$ for all $m \geq j > k$, and we show that $b_k \in \mathbb{R}$: To see this, note that

$$b_k + ab_{k+1} + bb_{k+2} = a_{k+2}$$

and so $b_k \in \mathbb{R}$ since $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Hence, $g \in \mathbb{R}[x]$ as claimed and we are done by induction.

□

4. Irreducibility over a field

Let k be a field

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

(i) d is monic

(ii) $d \mid f$ and $d \mid g$

(iii) If $h \mid f$ and $h \mid g$, then $h \mid d$

Furthermore, we have

(iv) (Bezout's Identity) $\exists s, t \in k[x]$ such that $d = sf + gt$

Proof. (a) Existence: Set

$$I := \{sf + tg : s, t \in k[x]\}$$

then check that I is an ideal of $k[x]$. Since $k[x]$ is a PID, $\exists d \in k[x]$ such that $I = (d)$.

(i) Multiplying d by a constant, we may assume that d is monic. Since $d \in I$, $\exists s, t \in k[x]$ such that

$$d = sf + tg \qquad (*)$$

We claim that this element d satisfies (ii) and (iii).

(ii) Since $f = 1 \cdot f + 0 \cdot g \in I$, and $I = (d)$ it follows that $d \mid f$. Similarly, $d \mid g$

(iii) If $h \mid f$ and $h \mid g$, then $h \mid (sf + tg) = d$.

(b) Uniqueness: Suppose $d_1, d_2 \in k[x]$ both satisfy properties $(i), (ii)$, and (iii). Then by (ii) we have $d_1 \mid d_2$ and $d_2 \mid d_1$, so $\exists r_1, r_2$ such that

$$r_1 d_1 = d_2 \text{ and } r_2 d_2 = d_1$$

So $r_2 r_1 d_1 = d_1$ and so comparing degrees (by Lemma 2.2), we see that $r_1, r_2 \in k$ are constants. Since d_1 and d_2 are monic, it follows that $r_1 = r_2 = 1$

□

(End of Day 4)

4.2. Definition:

(i) For $f, g \in k[x]$, the polynomial $d \in k[x]$ obtained in Theorem 4.1 is called the greatest common divisor (GCD) of f and g and is denoted by

$$d = (f, g)$$

(ii) Two polynomials $f, g \in k[x]$ are said to be relatively prime if $(f, g) = 1$.

(iii) A polynomial $f \in k[x]$ is said to be irreducible if

(a) $f \notin k$ and,

(b) whenever $h, g \in k[x]$ such that $f(x) = h(x)g(x)$, then either $h \in k$ or $g \in k$.

(iv) Let R be a ring. An ideal $I \lhd R$ is said to be a maximal ideal if

(a) $I \neq R$ and,

(b) for any other ideal $J \lhd R$ such that $I \subset J$ we have either $I = J$ or $J = R$.

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

(i) f is irreducible

(ii) (f) is a maximal ideal in $k[x]$

(iii) $k[x]/(f)$ is a field

Proof.

$(i) \Rightarrow (ii)$: If f is irreducible, let $I = (f)$ and suppose $J \lhd k[x]$ is an ideal such that $I \subset J$. We WTS: $J = I$ or $J = k[x]$.

Since $k[x]$ is a PID, $\exists g \in J$ such that $J = (g)$. Since $I \subset J, \exists s \in k[x]$ such that $f = sg$. Since f is irreducible, it follows that either $s \in k$ or $g \in k$. If $s \in k$, then $I = J$ and if $g \in k$ then $J = k[x]$ since g is a unit.

(ii) ⇒ *(iii)*: Suppose $I = (f)$ is a maximal ideal, then $I \neq k[x]$, so $1 \notin I$. Hence if $R := k[x]/(f)$, then R is a commutative ring with

$$1_R = 1 + I \neq I = 0_R$$

Thus, we WTS: if $g + I \neq I$, then $\exists h \in k[x]$ such that $gh + I = 1 + I$.

To do this, consider $d = (g, f)$, then by 4.1, $d \mid f$, so $f \in J := (d)$, and so $I \subset J$. By maximality, it follows that either $J = I$ or $J = k[x]$.

(i) If $J = I$, then $f \mid d$. But $d \mid g$, so $f \mid g$ and so $g \in I$, which contradicts the fact that $g + I \neq I$

(ii) If $J = k[x]$, then $(d) = (1)$ and so $\exists h, t \in k[x]$ such that $hg + tf = 1$. Applying the quotient map $\pi : k[x] \to R$, we see that

$$(h + I)(g + I) = 1 + I \text{ in } R$$

as required.

(iii) ⇒ *(i)*: HW □

4.4. Examples:

(i) Polynomials of degree 1, but not 0 (since the latter are units)

(ii) If f is irreducible in $k[x]$, then f does not have any roots in k (by the Remainder theorem). However, the converse is not true. For instance, $f(x) = (x^2 + 1)(x^2 + 2) \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$, but is reducible.

(iii) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but not $\mathbb{R}[x]$.

(iv) $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ and $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ (without proof)

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

(vi) By Corollary 3.9, $f \in \mathbb{R}[x]$ 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 $\beta \in \mathbb{R}$

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

Proof. We induct on $\deg(f)$. If $\deg(f) \leq 1$, then there is nothing to prove. So assume that $\deg(f) > 1$ and that the theorem is true for any polynomial $g \in k[x]$ with $\deg(g) < \deg(f)$. If f itself is irreducible, then there is nothing to prove, so suppose f is reducible, then $\exists g, h \in k[x] \setminus k$ such that

$$f(x) = g(x)h(x)$$

Now $\deg(g), \deg(h) < \deg(f)$, so, by the induction hypothesis, both g and h can be expressed as a product of irreducibles. This proves the same for f. □

4.6. (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 $f \mid h$

Proof. (i) If $(f,g) = 1$, then $\exists s, t \in k[x]$ such that $sf + tg = 1$. If $f \mid gh$, then $\exists r \in k[x]$ such that $rf = gh$. Hence,

$$rsf + rtg = r = sgh + rtg = (sh + rt)g$$

Thus, we get

$$gh = rf = (sh + rt)gf$$

Since $k[x]$ is an integral domain, it follows that $h = (sh + rt)f$ and so $f \mid h$

(ii) If f is irreducible, then $(f,g) \mid f$ implies that $(f,g) = 1$ or $(f,g) = cf$ for some $c \in k$. In the former case, $f \mid h$ by part (i), and in the latter case, $f = c^{-1}(f,g) \mid g$

□

(End of Day 5)

4.7. (Unique Factorization - II): If $0 \neq f \in k[x]$, then the factorization of into irreducibles (as in 4.5) is unique upto constant factors and the order in which the factors are written.

Proof. Suppose

$$f = cg_1g_2 \dots g_n = dh_1h_2 \dots h_m \qquad (*)$$

where $g_i, h_j \in k[x]$ are all monic and irreducible, and $c, d \in k$. Then

(i) Comparing coefficients of the leading term of f, we see that $c = d$.

(ii) Now we assume that $c = d = 1$ and we induct on n. If $n = 1$, then

$$g_1 \mid h_1h_2 \dots h_m$$

So by (induction on) Euclid's lemma, $\exists 1 \leq j \leq m$ such that $g_1 \mid h_j$. Assume WLOG that $j = 1$, then $\exists r_1 \in k[x]$ such that

$$r_1g_1 = h_1$$

Since g_1 is irreducible, $g_1 \notin k$, so since h_1 is irreducible, $r_1 \in k$. Since g_1 and h_1 are both monic, it follows that $r_1 = 1$. Hence, $(*)$ becomes

$$g_1 = g_1h_2h_3 \dots h_m$$

If $m > 1$, then comparing degrees, we see that $h_i \in k$ for all $2 \leq i \leq m$. Since each h_i is irreducible, this cannot happen. Hence, $m = 1$ and we are done.

(iii) Now if $n > 1$, assume that the theorem is true for any polynomial g that can be expressed as a product of $(n-1)$ irreducibles. Then, by the same argument as part (ii), we see that $g_1 = h_1$, so $(*)$ becomes

$$g_1 g_2 \dots g_n = g_1 h_2 \dots h_m$$

Since $k[x]$ is an integral domain, this implies that

$$g := g_2 g_3 \dots g_n = h_2 h_3 \dots h_m$$

By induction, $n-1 = m-1$ and $g_i = h_i$ (upto a change in order). This completes the proof.

□

5. Irreducibility over $\mathbb{Q}$

5.1. Remark:

(i) A polynomial $f \in \mathbb{Z}[x]$ is said to be irreducible over $\mathbb{Z}$ if $f \neq \pm 1$ and if $f(x) = g(x)h(x)$ for some $g, h \in \mathbb{Z}[x]$, then either $g = \pm 1$ or $h = \pm 1$.

(ii) We say that $f \in \mathbb{Z}[x]$ can be properly factored in $\mathbb{Z}[x]$ if $\exists g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ such that $f(x) = g(x)h(x)$.

(iii) Note that

(a) Note that Theorem 4.3 no longer holds over $\mathbb{Z}$. For instance $f(x) = x$ is irreducible over $\mathbb{Z}$, but

$$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$$

which is not a field.

(b) $f(x) = 2x$ is reducible in $\mathbb{Z}[x]$, but cannot be properly factored in $\mathbb{Z}[x]$.

(c) In [Stewart, Definition 3.10], he defines a polynomial in $\mathbb{Z}[x]$ to be irreducible iff it cannot be properly factored. This is incorrect.

(d) If $f \in \mathbb{Z}[x]$ is monic, then it is irreducible in $\mathbb{Z}[x]$ iff it cannot be properly factored.

(iv) 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 $f \in \mathbb{Z}[x]$

5.2. 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 $\mathbb{Z}[x]$

Proof. Consider the map $\overline{\pi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ as above, then by hypothesis

$$\overline{g}\overline{h} = \overline{0}$$

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p[x]$ is an integral domain (by Lemma 2.2), and so either $\overline{g} = \overline{0}$ or $\overline{h} = \overline{0}$. This is the same as saying that either $p \mid g$ or $p \mid h$ in $\mathbb{Z}[x]$. □

5.3. (Gauss' Lemma): Let $f \in \mathbb{Z}[x]$, then f is irreducible in $\mathbb{Q}[x]$ iff it cannot be properly factored in $\mathbb{Z}[x]$

Note: Gauss' Lemma is specific to the pair $(\mathbb{Z}, \mathbb{Q})$. Compare it with the fact that $(x^2 - 2)$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{R}[x]$.

Proof. Note that if f is irreducible in $\mathbb{Q}[x]$, it clearly cannot be properly factored in $\mathbb{Z}[x]$. We now prove the converse: Suppose f cannot be factored in $\mathbb{Z}[x]$, but $\exists g, h \in \mathbb{Q}[x] \setminus \mathbb{Q}$ such that

$$f(x) = g(x)h(x)$$

Multiplying throughout by the common denominator, we may express this equation as

$$n_1 f = g_1 h_1 \qquad (*)$$

for some $n_1 \in \mathbb{Z}$, and $g_1, h_1 \in \mathbb{Z}[x] \setminus \mathbb{Z}$. We claim that $\exists g', h' \in \mathbb{Z}[x] \setminus \mathbb{Z}$ such that $\deg(g') = \deg(g), \deg(h') = \deg(h)$ and

$$f = g'h' \qquad (**)$$

This would contradict the assumption on f. To do this, we induct on $|n_1|$.

(i) If $n_1 = \pm 1$, then the claim clearly holds.

(ii) If $|n_1| > 1$, let $p \in \mathbb{Z}$ be any prime number dividing n_1, $p \mid g_1 h_1$. By Lemma 5.2, either $p \mid g_1$ or $p \mid h_1$. Assume WLOG that $p \mid g_1$, then $\exists g_2 \in \mathbb{Z}[x]$ such that

$$nf = pg_2 h_1$$

Since $\mathbb{Z}[x]$ is an integral domain, we may cancel p on both sides to obtain an equation of the form

$$n_2 f = g_2 h_2$$

Note that $g_2, h_2 \in \mathbb{Z}[x] \setminus \mathbb{Z}$. Furthermore, $|n_2| < |n_1|$. Hence, by induction hypothesis, the claim holds and we are done.

□

(End of Day 6)

5.4. (Eisenstein's criterion): Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$, 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 $\mathbb{Q}[x]$

Proof. By Gauss' lemma, it suffices to show that f cannot be properly factored in $\mathbb{Z}[x]$. Suppose that $\exists g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ such that

$$f(x) = g(x)h(x)$$

Then write $g(x) = b_0 + b_1x + \ldots + b_mx^m$ and $h(x) = c_0 + c_1x + \ldots + c_kx^k$ where $m, k > 0$ and $m + k = n$. Then applying the quotient map $\pi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, we see that

$$\overline{f}(x) = \overline{a_n}x^n = \overline{g}\overline{h}$$

Note that $\mathbb{Z}_p$ is a field and x is irreducible in $\mathbb{Z}_p[x]$. Hence, by Unique Factorization (Theorem 4.7) in $\mathbb{Z}_p[x]$, it follows that $\overline{g}$ and $\overline{h}$ must themselves be constant multiples of some power of x. Since $p \nmid a_n = b_mc_k$, it follows that $p \nmid b_m$ and $p \nmid c_k$. Hence,

$$\overline{g}(x) = \overline{b_m}x^m \text{ and } \overline{h}(x) = \overline{c_k}x^k$$

In particular, since $m, k > 0$,

$$p \mid b_0 \text{ and } p \mid c_0$$

Hence, $p^2 \mid a_0$, contradicting (iii). □

5.5. 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)

5.6. (Reduction mod p) Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ and p a prime such that

(i) $p \nmid a_n$

(ii) $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$ for some prime $p \in \mathbb{Z}$

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

Proof. By Gauss Lemma, it suffices to show that f cannot be properly factored in $\mathbb{Z}[x]$. So write $f(x) = a_0 + a_1x + \ldots + a_nx^n$ and suppose $\exists g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ such that

$$f(x) = g(x)h(x)$$

Write $g(x) = b_0 + b_1x + \ldots + b_mx^m$ and $h(x) = c_0 + c_1x + \ldots + c_kx^k$. Applying the quotient map $\pi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, we get

$$\overline{f} = \overline{g}\overline{h} \text{ in } \mathbb{Z}_p[x]$$

Since $p \nmid a_n$, $\overline{f} \neq \overline{0}$. Since $p \nmid a_n$,

$$p \nmid b_m \text{ and } p \nmid c_k$$

Hence, $\deg(\overline{g}) = m, \deg(\overline{h}) = k$. However, $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$ and so either $\overline{g} \in \mathbb{Z}_p$ or $\overline{h} \in \mathbb{Z}_p$. Assume WLOG that $\overline{g} \in \mathbb{Z}_p$, then $m = 0$ and hence $g \in \mathbb{Z}$. □

5.7. Example:

(i) Let $f(x) = 8x^3 - 6x - 1$, then we have to choose $p \in \mathbb{Z}$ carefully ($p = 2$ does not work). For $p = 5$,

$$\overline{f}(x) = 3x^3 - x - 1$$

Since $\deg(\overline{f}) \leq 3$, to show that $\overline{f}$ is irreducible in $\mathbb{Z}_5[x]$, it suffices to show that it does not have a root in $\mathbb{Z}_5$. This is easy to check since there are only finitely many elements in $\mathbb{Z}_5$

(ii) 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).

5.8. (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.

Proof. Part (ii) follows from part (i), so we only prove (i). If p/q is a root, then $x - p/q$ divides f in $\mathbb{Q}[x]$, so

$$g(x) = qx - p$$

divides f in $\mathbb{Q}[x]$. So, $\exists h \in \mathbb{Q}[x]$ such that $gh = f$. Multiplying by the common denominator, we obtain an equation of the form

$$gh_1 = n_1f$$

If $r \mid n_1$ is any prime, then $r \mid gh_1$, and so by Lemma 5.2, $r \mid g$ or $r \mid h_1$. Since $(p, q) = 1$, it follows that $r \nmid g$ and so $r \mid h_1$. Hence, $\exists h_2 \in \mathbb{Z}[x]$ such that

$$rgh_2 = r\left(\frac{n_1}{r}\right)f$$

Since $\mathbb{Z}[x]$ is an integral domain, we may cancel r to obtain

$$gh_2 = n_2f$$

for some $n_2 \in \mathbb{Z}$ with $|n_2| < |n_1|$. By induction on the number of primes dividing n_1, we finally obtain an equation of the form

$$gh_k = f$$

for some $h_k \in \mathbb{Z}[x]$. From this it follows that $q \mid a_n$ and $p \mid a_0$. □

5.9. Remark:

(i) The same proof as above can be used to prove the following: Let $g, f \in \mathbb{Z}[x]$ be two polynomials such that $g \mid f$ in $\mathbb{Q}[x]$ and the GCD of the coefficients of g is 1. Then $g \mid f$ in $\mathbb{Z}[x]$

(ii) Gauss' Lemma is used to prove that every element $f \in \mathbb{Z}[x]$ can be expressed uniquely as a product of irreducibles.

(End of Day 7)

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 obtain 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) A field extension is a pair of fields (k, L) such that there is a field homomorphism $\iota : k \to L$. We simply write $k \subset L$ to denote such a field extension.

Note: If $\mathcal{F}$ is a non-empty family of fields, then so is

$$\bigcap_{L \in \mathcal{F}} L$$

(ii) Let k be a field and $X \subset \mathbb{C}$. Let $\mathcal{F}$ denote the collection of all fields containing $k \cup X$. Note that $\mathcal{F} \neq \emptyset$ since $\mathbb{C} \in \mathcal{F}$. We write

$$k(X) = \bigcap_{L \in \mathcal{F}} L$$

Note that $k(X)$ is the smallest field containing k and X.

(iii) If $X = \{\alpha\}$ above, then we write $k(\alpha) := k(\{\alpha\})$. The field extension $k \subset k(\alpha)$ is called a simple extension. The element α is called a generator of the simple extension.

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

Proof. Let $F = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, then

(a) $\sqrt{2}+\sqrt{3} \in K$ and K is a field, so $F \subset K$ by definition.

(b) Furthermore, $y := \sqrt{2}+\sqrt{3} \neq 0$, so

$$y^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{2-3} = \sqrt{3}-\sqrt{2} \in F$$

Hence,

$$\frac{y+y^{-1}}{2} = \sqrt{3} \in F \text{ and } \sqrt{2} \in F$$

Hence, $K \subset F$ by definition.

□

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

(i) We say that α is algebraic over k if $\exists f \in k[x]$ such that $f(\alpha) = 0$

(ii) We say that α is transcendental over k if α is not algebraic 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 $\mathbb{R}$

(v) Every complex number 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

(ii) f is irreducible

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

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

Proof. (i) Existence:Let

$$I := \{g \in k[x] : g(\alpha) = 0\}$$

Then I is an ideal (Check!). Hence, $\exists f \in k[x]$ such that $I = (f)$. By multiplying by a constant, we may assume that f is monic. Clearly, $f(\alpha) = 0$ and $g(\alpha) = 0$ iff $f \mid g$. It suffices to show that f is irreducible. So suppose $f = gh$ in $k[x]$, then

$$g(\alpha)h(\alpha) = 0 \text{ in } \mathbb{C} \Rightarrow g(\alpha) = 0 \text{ or } h(\alpha) = 0$$

Assume WLOG that $g(\alpha) = 0$, then $g \in I$, so $f \mid g$. Hence, (why?) $h \in k$ and we are done.

(ii) Uniqueness: Suppose $f_1, f_2 \in k[x]$ satisfying $(i) - (iii)$, then $f_1, f_2 \in I$ where I as above. Hence, following the argument above, $f_1 \mid f_2$ and $f_2 \mid f_1$. Hence, $\exists c \in k$ such that

$$f_2 = cf_1$$

Since both are monic, $c = 1$.

□

1.6. Examples:

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

(ii) If $k = \mathbb{Q}, \alpha = \sqrt{2}$, then $m_\alpha(x) = x^2 - 2$ (because $x^2 - 2$ is irreducible by Eisenstein's criterion)

(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 $m_\omega(x) = \Phi_2(x) = x^2+x+1$ (Since Φ_2 is irreducible, monic and $\Phi_2(\omega) = 0$)

(End of Day 8)

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

(i) A homomorphism of field extensions (or a k-homomorphism) is a field homomorphism $\varphi : L_1 \to L_2$ such that $\varphi|_k = \mathrm{id}_k$

(ii) An isomorphism of field extensions is a bijective homomorphism. If such an isomorphism exists, we write

$$L_1 \cong_k L_2$$

1.8. Examples:

(i) Consider $\mathbb{R} \subset \mathbb{C}$, then the map $z \mapsto \overline{z}$ is a $\mathbb{R}$-homomorphism from $\mathbb{C}$ to $\mathbb{C}$

(ii) The map $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ given by $(a+b\sqrt{2}) \mapsto (a-b\sqrt{2})$ is a $\mathbb{Q}$-homomorphism. In fact, it induces a $\mathbb{Q}$-isomorphism of $\mathbb{Q}(\sqrt{2})$ to itself.

(iii) If $L_1, L_2 \subset \mathbb{C}$ any two fields, then any field homomorphism $\varphi : L_1 \to L_2$ is a $\mathbb{Q}$-homomorphism (by Example I.1.4(iii))

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

Proof. (i) Let $L = k[x]/(m_\alpha)$, then L is a field by I.4.3 and II.1.5. There is a field homomorphism

$$\iota : k \to L \text{ given by } k \hookrightarrow k[x] \xrightarrow{\pi} k[x]/(m_\alpha)$$

(ii) Since $k(\alpha)$ is a field, and $k \subset k(\alpha)$, we may define a homomorphism (by HW 1.5)

$$\psi : k[x] \to k(\alpha) \text{ such that } \psi|_k = \text{id}_k \text{ and } \psi(x) = \alpha$$

Let $I = \ker(\psi)$, then by definition

$$I = \{g \in k[x] : g(\alpha) = 0\}$$

By the proof of Theorem 1.5, $I = (m_\alpha)$, so we have an isomorphism of fields

$$\overline{\psi} : L \to \text{Im}(\psi)$$

Since L is a field, so is $\text{Im}(\psi)$. Since $\text{Im}(\psi)$ contains k and α, $\text{Im}(\psi) = k(\alpha)$, and so

$$L \cong k(\alpha)$$

Now observe that the isomorphism fixes k (since ψ fixes k)

□

1.10. Corollary:

(i) 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 $\alpha \mapsto \beta$.

(ii) 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 $\varphi\,|_k = \text{id}_k$ and $\varphi(\alpha) = \beta$

Proof. We only prove (i): Consider the isomorphisms

$$\varphi : k[x]/(m_\alpha) \to k(\alpha) \text{ and } \psi : k[x]/(m_\beta) \to k(\beta)$$

Note that $\varphi(\overline{x}) = \alpha$ and $\psi(\overline{x}) = \beta$. Since $m_\alpha = m_\beta$, we obtain an isomorphism $\eta := \psi \circ \varphi^{-1} : k(\alpha) \to k(\beta)$, and note that $\eta|_k = \text{id}_k$ and $\eta(\alpha) = \beta$ □

1.11. Definition: Let k be a field. The field of rational functions $k(x)$ over k is defined as the set of formal rational functions over k

$$k(x) = \left\{\frac{f(x)}{g(x)} : f, g \in k[x], g \neq 0\right\}$$

1.12. Remark:

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

(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

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

Proof. Define $\psi : k(x) \to k(\alpha)$ by

$$\psi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)}$$

Since α is transcendental, $g(\alpha) \neq 0$ for any $g \neq 0$, and so this map is well-defined. It is easy to see that it is a field homomorphism (Check!). Since $\text{Im}(\psi)$ contains k and α, ψ is surjective. Since $k(x)$ is a field, ψ is injective (Corollary 1.7), and hence an isomorphism. □

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) The dimension of L as a $k-$vector space is called the degree of the extension and is denoted by $[L : k]$

(ii) If $[L : k] < \infty$, then $k \subset L$ is called a finite extension

2.3. Example:

(i) $[\mathbb{C} : \mathbb{R}] = 2$ (by I.3.1)

(ii) Similarly, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

(iii) If $\mathbb{Q} \subset L$ is a finite extension, then $\exists n \in \mathbb{N}$ such that $L \cong \mathbb{Q}^n$ (as vector spaces). In particular, L must be countable. Hence, $\mathbb{Q} \subset \mathbb{R}$ is not a finite extension.

(iv) If $k \subset \mathbb{C}$ and $\alpha \in \mathbb{C}$ is transcendental over k, then $k \subset k(\alpha)$ is an infinite extension. (Since the set $\{1, \alpha, \alpha^2, \alpha^3, \ldots\}$ is linearly independent over k)

(End of Day 9)

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

Proof. Clearly (i) implies (ii), so we only prove (i): Consider $S := \{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$, then we WTS: S is a basis for $k(\alpha)$ over k

(i) S is linearly independent: If $\exists a_0, a_1, \ldots, a_{n-1} \in k$ such that

$$\sum_{i=0}^{n-1} a_i \alpha^i = 0$$

Then for $f(x) = \sum_{i=0}^{n-1} a_i x^i$, we have $f \in k[x]$ and $f(\alpha) = 0$. Since $\deg(f) < n$, this contradicts the minimality of $n = \deg(m_\alpha)$

(ii) S is a generating set: If $u \in k(\alpha)$, then consider the isomorphism

$$\overline{\psi} : k[x]/(m_\alpha) \to k(\alpha)$$

Since $\overline{\psi}$ is surjective, and $\pi : k[x] \to k[x]/(m_\alpha), \exists g \in k[x]$ such that

$$g(\alpha) = \overline{\psi}(\pi(g)) = u$$

Write $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, then by Euclidean division, $\exists t, r \in k[x]$ such that

$$g = t m_\alpha + r \text{ and } \deg(r) < \deg(m_\alpha) \text{ or } r = 0$$

Now note that $\pi(g) = \pi(r)$, and so

$$g(\alpha) = r(\alpha)$$

Replacing g by r, we may assume WLOG that either $g = 0$ or $\deg(g) < n$. If $g = 0$, then $u = 0$ and there is nothing to show. If $\deg(g) < n$, then

$$u = g(\alpha) = \sum_{i=0}^{m} b_i \alpha^i \in \text{Span}(S)$$

□

2.5. Examples:

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

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

$$2^{2/3} \notin \{a + b2^{1/3} : a, b \in \mathbb{Q}\} =: F$$

so F is not a ring.

(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 3.1), so

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

2.6. Corollary: Let $k \subset K$ be a field extension and $\alpha \in \mathbb{C}$ be algebraic over k. Then

(i) α is algebraic over K

(ii) $[K(\alpha) : K] \leq [k(\alpha) : k]$

Proof. (i) If α is a root of a non-zero $f \in k[x]$, then $f \in K[x]$ as well.

(ii) Let f, g denote the minimal polynomials of α over k and K respectively. Then

(a) g is irreducible in $K[x]$

(b) $f \in K[x]$ and $f(\alpha) = 0$

Hence, by Theorem II.1.5, $g \mid f$ in $K[x]$. In particular, by II.2.5,

$$[K(\alpha) : K] = \deg(g) \leq \deg(f) = [k(\alpha) : k]$$

□

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

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

Proof. Let S and T be bases for $k \subset F$ and $F \subset L$ respectively. Define

$$B = \{xy : x \in S, y \in T\}$$

(i) B is a generating set for $k \subset L$: If $\alpha \in L, \exists a_1, \ldots, a_n \in F$ and $y_1, y_2, \ldots, y_n \in T$ such that

$$\alpha = \sum_{i=1}^{n} a_i y_i$$

For each $a_i \in F, \exists b_1, b_2, \ldots, b_{i,s_i}$ and $x_1, x_2, \ldots, x_{s_i} \in S$ such that

$$a_i = \sum_{j=1}^{s_i} b_j x_j$$

Hence,

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{s_i} b_j (x_j y_i) \in \text{Span}_k(B)$$

(ii) B is k-linearly independent: If $\exists a_1, a_2, \ldots, a_n \in k$ and $z_1, z_2, \ldots, z_n \in B$ such that

$$\sum_{i=1}^{n} a_i z_i = 0$$

Then write $z_i = x_i y_i$ for some $x_i \in S, y_i \in T$, then $b_i = a_i x_i \in F$ and $\{y_1, y_2, \ldots y_n\}$ is F-linearly independent. Hence $b_i = 0$ for all i. But each $x_i \neq 0$ (since S is k-linearly independent) and so $a_i = 0$ for all i

(iii) $|B| = |S||T|$: It suffices to show that the map

$$S \times T \to B \text{ given by } (x,y) \mapsto xy$$

is bijective. By definition, it is surjective, so suppose $x_1y_1 = x_2y_2$ for some $x_i \in S, y_i \in T$. Then

$$x_1y_1 - x_2y_2 = 0 \qquad (*)$$

and $x_i \in S \subset F$. If $y_1 \neq y_2$, then $\{y_1, y_2\}$ is F-linearly independent, and so $x_1 = x_2 = 0$. This is impossible since S is k-linearly independent (and so $0 \notin S$). Hence,$y_1 = y_2$ must hold. But then $(*)$ implies that

$$(x_1 - x_2)y_1 = 0$$

Once again, $y_1 \neq 0$ since $0 \notin T$, and so $x_1 = x_2$ must hold.

□

2.8. Examples:

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

Proof. Let $K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then we have a tower $\mathbb{Q} \subset K \subset L$, and $[K : \mathbb{Q}] = 2$ by Example II.2.3. Hence by the tower law, it suffices to show that

$$[L : K] = 2$$

Since $L = K(\sqrt{3})$, by Corollary II.2.6,

$$[L : K] \leq 2 \text{ and } [L : K] = 1 \text{ iff } \sqrt{3} \in K$$

Suppose $\sqrt{3} \in K$, then $\exists a, b \in \mathbb{Q}$ such that

$$\begin{aligned} \sqrt{3} &= a + b\sqrt{2} \\ \Rightarrow 3 &= a^2 + 2b^2 + 2\sqrt{2}ab \end{aligned}$$

We now have three cases:

(a) If $ab \neq 0$, then $\sqrt{2} \in \mathbb{Q}$, which is impossible. Hence $a = 0$ or $b = 0$.

(b) If $b = 0$, then $\sqrt{3} = a \in \mathbb{Q}$ which is not true.

(c) If $a = 0$, then

$$\sqrt{3} = b\sqrt{2} \Rightarrow \sqrt{6} = 2b \in \mathbb{Q}$$

But $x^2 - 6 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion with $p = 2$.

Hence, $\sqrt{3} \notin K$ and so $[L : K] = 2$. □

(End of Day 10)

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

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

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

Proof. (a) If $k \subset F \subset L$, then $[L : F] \mid [L : k]$.

(b) Since $[L : k]$ is prime, $k \neq L$, so fix $\alpha \in L \backslash k$, then $k(\alpha) \subset L$ by definition, and $k \neq k(\alpha)$. So by part (a), $k(\alpha) = L$.

□

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

2.9. Corollary: Let $k \subset F_1$ and $k \subset F_2$ be two finite 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 compositum of F_1 and F_2 and is denoted by F_1F_2

Proof. (i) Let $S = \{x_1, x_2, \ldots, x_n\}$ be a k-basis for F_1. Let

$$F = \text{Span}_{F_2}(S)$$

- We claim that F is a field:

  (a) If $u = \sum_{i=1}^n a_i x_i, v = \sum_{i=1}^n b_i x_i \in F$ with $a_i, b_j \in F_2$, then

  $$uv = \sum_{i,j} a_i b_j x_i x_j$$

  But $x_i x_j \in F_1 = \text{Span}_k(S)$, and hence $uv \in \text{Span}_{F_2}(S)$, and so F is a ring.

  (b) If $0 \neq u \in F$, we WTS: $u^{-1} \in F$. To see this, consider the map

  $$T : F \to F \text{ given by } y \mapsto yu$$

  This map is F_2-linear. Also, T is injective, because if $y_1 u = y_2 u$, then $y_1 = y_2$ since $u \neq 0$. Since F is a finite dimensional F_2-vector space, T is also surjective. In particular, $\exists v \in F$ such that

  $$vu = T(v) = 1$$

  Similarly, $\exists w \in F$ such that $uw = 1$. Thus, u is invertible in F

- Now we claim that $L = F$

  (a) Since F is a field, and $k, S \subset F$, we have $F_1 \subset F$. Since $F_2 \subset F$, we have

  $$L \subset F$$

  by definition.

(b) However, since $F_1 \subset L$, we have $S \subset L$. Since $F_2 \subset L$, it follows that $\text{Span}_{F_2}(S) \subset L$

From this claim, it follows that

$$[L : F_2] \leq |S| = [F_1 : k]$$

(ii) By the tower law and part (i)

$$[L : k] = [L : F_2][F_2 : k] \leq [F_1 : k][F_2 : k]$$

(iii) If $m := [F_1 : k]$ and $n := [F_2 : k]$, then by part (ii)

$$[L : k] \leq mn$$

However, $[L : k] = [L : F_2][F_2 : k]$ and so $m \mid [L : k]$. Similarly, $n \mid [L : k]$. Since $(m, n) = 1$, it follows that

$$mn \mid [L : k]$$

and hence $[L : k] = mn$.

□

2.10. 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)

3. Algebraic Extensions

3.1. Definition: A field extension $k \subset L$ is said to be <u>algebraic</u> if every element of L is algebraic over k

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.

Proof. (ii) follows from (i) by Theorem II.2.4, so we only prove (i): Suppose $k \subset L$ is finite, and $\alpha \in L$, then if $n := [L : k]$, we must have that the set

$$\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$$

is k-linearly dependent. Hence, $\exists a_i \in k$ not all zero such that

$$\sum_{i=0}^{n} a_i\alpha^i = 0$$

Now $f(x) = \sum_{i=0}^{n} a_ix^i \in k[x]$ is non-zero and $f(\alpha) = 0$ □

Example: If $\zeta_5 := e^{2\pi i/5} \in \mathbb{C}$, then $\mathbb{Q} \subset \mathbb{Q}(\zeta_5)$ is algebraic. In particular, $\cos(2\pi/5)$ is algebraic over $\mathbb{Q}$. Moreover, by the proof of the theorem, it is clear that $\cos(2\pi/5)$ satisfies a non-zero polynomial of degree ≤ 4 over $\mathbb{Q}$.

(End of Day 11)

3.3. Definition: A field extension $k \subset L$ is said to be finitely generated if $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in L$ such that $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$

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

Proof. (i) If $k \subset L$ is finite, then

(a) $k \subset L$ is algebraic by Theorem 3.2

(b) Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a k-basis for L, then (Check!)

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

Hence $k \subset L$ is finitely generated.

(ii) Conversely, suppose $k \subset L$ is algebraic and finitely generated, write

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

To show: $[L : k] < \infty$, we induct on n.

(a) If $n = 1$, then $L = k(\alpha_1)$ and α_1 is algebraic over k. So $[L : k] < \infty$ by Theorem II.2.4

(b) If $n > 1$, assume the theorem is true for any field extension $k \subset K$ with a generating set S such that $|S| < n$. Now take

$$K = k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

By induction hypothesis, $k \subset K$ is finite. Furthermore, α_n is algebraic over k, so α_n is algebraic over K by II.2.6, so

$$K \subset K(\alpha_n) = L$$

is finite. So by Tower law, $k \subset L$ is finite.

□

3.5. Remark: If $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where each α_i is algebraic over k, then by the proof of the previous theorem,

$$[L : k] \leq \prod_{i=1}^{n} [k(\alpha_i) : k] = \prod_{i=1}^{n} \deg(m_{\alpha_i})$$

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

Proof. Suppose $\alpha \in L$, then WTS: α is algebraic over k. We know that α is algebraic over F, so $\exists f \in F[x]$ non-zero such that

$$f(\alpha) = 0$$

Write $f(x) = a_0 + a_1x + \ldots + a_nx^n$, then each $a_i \in F$. In particular, each a_i is algebraic over k. Write

$$K = k(a_0, a_1, \ldots, a_n)$$

Then $k \subset K$ is algebraic and finitely generated. By Theorem 3.5,

$$k \subset K$$

is finite. Now α is algebraic over K since $f \in K[x]$. Hence,

$$K \subset K(\alpha)$$

is finite by Theorem II.2.4. By the tower law,

$$[K(\alpha) : k] < \infty$$

In particular, by Theorem 3.2, α is algebraic over k. □

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

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

(ii) If $f \in F[x] \setminus F$, then every complex 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.

Proof. We prove $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

(i) ⇒ (ii): If $f \in\in F[x]$, we WTS: every root of f is in F. To do this, we induct on $n := \deg(f)$.

(a) If $n \leq 1$, there is nothing to prove.

(b) If $n > 1$, then assume the statement is true for any polynomial $g \in F[x]$ with $\deg(g) < n$. Now let $\alpha \in \mathbb{C}$ be a root of f. By assumption, f has a root $\beta \in F$. If $\alpha = \beta$, there is nothing to prove, so assume $\alpha \neq \beta$. If not, then by the remainder theorem, $\exists g \in F[x]$ such that

$$f(x) = (x - \alpha)g(x)$$

Hence, $g(\beta) = 0$ and $\deg(g) < n$. So by induction hypothesis, $\beta \in F$.

(ii) ⇒ (iii): If $F \subset L$ is algebraic extension and $\alpha \in L$, then α is algberaic over F, so $\exists f \in F[x]$ such that $f(\alpha) = 0$. By hypothesis, $\alpha \in F$. This is true for any $\alpha \in L$, so $L = F$.

(iii) $\Rightarrow$ (i): If $f \in F[x] \setminus F$, then by FTA, f has a root $\alpha \in \mathbb{C}$. Thus, if $L = F(\alpha)$, then $F \subset L$ is an algebraic extension (by Theorem 3.2). By hypothesis, this implies $L = F$, and so $\alpha \in F$.

□

3.8. Theorem: Let $k \subset \mathbb{C}$ be a field and

$$F := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } k\}$$

Then

(i) F is a field

(ii) F is algebraically closed.

(iii) If L is any other algebraically closed field such that $k \subset L$, then $F \subset L$.

F is called the algebraic closure of k and is denoted by $\overline{k}$

Proof. (i) Suppose $\alpha, \beta \in F$, then

$$[k(\alpha) : k] < \infty \text{ and } [k(\beta) : k] < \infty$$

Hence, by Corollary II.2.9,

$$[k(\alpha, \beta) : k] < \infty$$

By Theorem 3.2, every $\gamma \in k(\alpha, \beta)$ is algebraic over k. In particular, $\alpha+\beta, \alpha\beta$, and, if $0 \neq \alpha$, then α^{-1} are all in F

(ii) If $F \subset L$ is an algebraic extension, then we WTS: $L = F$. But note that $k \subset F$ is algebraic by definition. Hence by Theorem 3.6, $k \subset L$ is algebraic. Hence, every $\alpha \in L$ is algebraic over k. By definition, this implies $\alpha \in F$, and so $F = L$.

(iii) Suppose L is algebraically closed and $k \subset L$, then, for any $\alpha \in F, \alpha$ is algebraic over k. Hence, α is algebraic over L, so

$$L \subset L(\alpha)$$

is an algebraic extension. By 3.7(iii), $L = L(\alpha)$. In particular, $\alpha \in L$. This is true for any $\alpha \in F$, so $F \subset L$.

□

(End of Day 12)

3.9. Remark/Examples:

(i) $\mathbb{C}$ is algebraically closed by FTA.

(ii) $\overline{\mathbb{R}} = \mathbb{C}$

(iii) $\overline{\overline{k}} = \overline{k}$

(iv) $\overline{\mathbb{Q}}$ is the smallest subfield of $\mathbb{C}$ that is algebraically closed (by HW 1.3 and Theorem 3.8(iii))

(v) $\mathbb{Q} \subset \overline{\mathbb{Q}}$ is an infinite algebraic extension. (In particular, the converse of Theorem 3.2(i) is false)

Proof. For each $n \in \mathbb{N}$, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \geq n$ and $\mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}}$. □

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

(vii) If $p \in \mathbb{Z}$ is a prime, then $k = \mathbb{Z}_p =: \mathbb{F}_p$ is a field (not contained in $\mathbb{C}$). However, one can use Zorn's lemma to construct another field L with the properties of Theorem 3.7. This field is unique, and is also called the algebraic closure of $\mathbb{Z}_p$ and is denoted by $\overline{\mathbb{F}_p}$ (See [Garling, Chapter 8])

3.10. Theorem: Let $k \subset F_1$ and $k \subset F_2$ be algebraic extensions, then $k \subset F_1F_2$ is algebraic.

Proof. By definition, $F_1 \subset \overline{k}$ and $F_2 \subset \overline{k}$. Since $\overline{k}$ is a field, $F_1F_2 \subset \overline{k}$ □

4. Primitive Element Theorem

(Taken from [Greenberg]) Throughout this section, let k be a field with $k \subset \mathbb{C}$.

4.1. Definition: A polynomial $f \in k[x]$ is said to be separable if all its roots in $\mathbb{C}$ are distinct. ie. every complex root of f has multiplicity 1 (See Definition I.2.8)

4.2. Remark: Let $f(x) = a_0 + a_1x + \ldots + a_nx^n \in k[x]$, then

$$D(f) := a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$$

is called the formal derivative of f. Note that

(i) $D(f) \in k[x]$

(ii) $D(f+g) = D(f) + D(g)$

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

(iv) $D(fg) = fD(g) + gD(f)$ [Leibnitz' rule]

(v) $\deg(D(f)) < \deg(f)$

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

Proof. Assume $f \in k[x] \setminus k$ and let $\alpha \in \mathbb{C}$ be a root of f. Then $\exists m \in \mathbb{N}$ and $g \in \mathbb{C}[x]$ such that

$$f(x) = (x-\alpha)^m g(x) \text{ and } g(\alpha) \neq 0$$

Then by the Leibnitz rule

$$D(f)(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m D(g)(x)$$

Hence,

$$\begin{aligned} D(f)(\alpha) = 0 &\Leftrightarrow m \geq 1 \\ &\Leftrightarrow \alpha \text{ is a multiple root of } f \qquad (*) \end{aligned}$$

(i) Suppose $d = (f, D(f)) \neq 1$, then $d \in k[x] \setminus k$, so d has a root $\alpha \in \mathbb{C}$. Then

$$f(\alpha) = 0 \text{ and } D(f)(\alpha) = 0$$

So by $(*)$, α is a multiple root of f.

(ii) Conversely, if f is not separable, then f has a multiple root $\alpha \in \mathbb{C}$. Then by $(*)$,

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

So if $m_\alpha \in k[x]$ denote the minimal polynomial for α over k, then it must happen that

$$m_\alpha \mid f \text{ and } m_\alpha \mid D(f) \text{ in } k[x]$$

Hence, $m_\alpha \mid (f, D(f)) \neq 1$ (since m_α is irreducible and hence not in k)

□

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

Proof. If f is irreducible, and $d = (f, D(f))$, then $d \mid f$ so $d = 1$ or $d = cf$ for some $c \in k$. However,

$$d \mid D(f) \Rightarrow \deg(d) \leq \deg(D(f)) < \deg(f)$$

Hence, $d = 1$ and Theorem II.4.3 applies. □

4.5. Lemma: Let $k \subset \mathbb{C}$ be a field and $f, g \in k[x]$ be irreducible polynomials. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ be the set of roots of f and g in $\mathbb{C}$ respectively. Then $\exists \lambda \in k \setminus \{0\}$ such that

$$\alpha_1 + \lambda\beta_1 \neq \alpha_i + \lambda\beta_j \quad \forall 1 \leq i \leq n, 2 \leq j \leq m$$

Proof. In $\mathbb{C}[x]$, write (by I.3.8),

$$f(x) = c\prod_{i=1}^{n}(x - \alpha_i) \text{ and } g(x) = d\prod_{j=1}^{m}(x - \beta_j)$$

Now consider the set

$$S = \left\{\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} : 1 \leq i \leq n, 2 \leq j \leq m\right\}$$

Note that every ratio in S is well-defined since $\{\beta_j\}$ are all distinct by Corollary 4.4.

Since $k \subset \mathbb{C}$, $\mathbb{Q} \subset k$ by HW 1.3, so k is infinite. Since S is a finite set, $\exists \lambda \in k \setminus S$, which works. Note that $\lambda \neq 0$ since $0 \in S$. □

(End of Day 13)

4.6. (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 $k \subset L$

Proof. Since $k \subset L$ is finite, then by Theorem II.3.4, $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in L$ such that

- Each α_i is algebraic over k
- $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$

We induct on n.

(i) If $n = 1$, there is nothing to show.

(ii) If $n > 2$, then note that

$$L = F(\alpha_n) \text{ where } F = k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

If we show that $k \subset F$ is simple, then $\exists \theta_1 \in F$ such that $F = k(\theta_1)$. Then

$$L = k(\theta_1, \alpha_n)$$

Hence, it suffices, by induction to prove the case $n = 2$.

(iii) If $n = 2$, write $L = k(\alpha, \beta)$.

(a) Let $f, g \in k[x]$ denote the minimal polynomials of α, β respectively. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ denote the sets of roots of f and g in $\mathbb{C}$ respectively. Then, with $\alpha = \alpha_1, \beta = \beta_1$, choose $\lambda \in k$ as in Lemma 4.5, and set

$$\theta := \alpha + \lambda\beta$$

We claim that $L = k(\theta)$. First note that $\theta \in L$, so $k(\theta) \subset L$.

(b) For the converse, write $F = k(\theta)$, and note that

$$L = F(\beta) = k(\theta, \beta)$$

since $\alpha = \theta - \lambda\beta$ and $\lambda \in k$. Hence, it suffices to show that $\beta \in F$. So let $p \in F[x]$ denote the minimal polynomial for β over F. Then, we WTS: $\deg(p) = 1$.

(c) Since $g \in F[x]$ is a polynomial with β as a root, it follows that

$$p \mid g \text{ in } F[x]$$

Also, if

$$h(x) = f(\theta - \lambda x) \in F[x]$$

Then

$$h(\beta) = f(\theta - \lambda\beta) = f(\alpha) = 0$$

Hence, $p \mid h$. In particular,

$$T := \{ \text{ roots of } p \text{ in } \mathbb{C}\} \subset \{ \text{ roots of } h \text{ in } \mathbb{C}\} \cap \{\beta_j : 1 \leq j \leq m\} \qquad (*)$$

(d) However, for each $1 \leq i \leq n, 2 \leq j \leq m$,

$$\begin{aligned} \theta = \alpha + \lambda\beta &\neq \alpha_i + \lambda\beta_j \\ \Rightarrow \theta - \lambda\beta_j &\neq \alpha_i \\ \Rightarrow h(\beta_j) = f(\theta - \lambda\beta_j) &\neq 0 \end{aligned}$$

So it follows that $T = \{\beta\}$ and since p is separable (by II.4.4), it follows that $\deg(p) = 1$. Hence,

$$[L : F] = [F(\beta) : F] = 1 \Rightarrow \beta \in F$$

Hence, $L = F = k(\theta)$ as required.

□

4.7. Example:

(i) If $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, then Lemma 4.5 provides a recipe to find the primitive element: Let

$$f(x) = x^2 + x + 1 \text{ and } g(x) = x^3 - 2$$

Then the roots of f and g are

$$\{\omega, \omega^2\} \text{ and } \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$$

respectively. Consider

$$S = \left\{0, \frac{\omega^2 - \omega}{\sqrt[3]{2} - \omega\sqrt[3]{2}}, \frac{\omega^2 - \omega}{\sqrt[3]{2} - \omega^2\sqrt[3]{2}}\right\}$$

In particular, $\lambda = 1 \notin S$, so $\theta = \omega + \sqrt[3]{2}$ is a primitive element.

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

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

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

Proof. Write $L = k(\alpha)$ by the primitive element theorem, and let $f = m_{\alpha,k}$. If $k \subset F \subset L$ is any intermediate field, then $L = F(\alpha)$, so if $g_F = m_{\alpha,F}$, then

$$g_F \mid f \text{ in } F[x] \Rightarrow g_F \mid f \in L[x]$$

Now let

$$\begin{aligned} \mathcal{F} &:= \{ \text{ intermediate fields } k \subset F \subset L\} \\ \mathcal{D} &:= \{ \text{ monic divisors of } f \text{ in } L[x]\} \\ \mu : \mathcal{F} &\to \mathcal{D} \text{ given by } F \mapsto g_F \end{aligned}$$

By the above argument, μ is well-defined, and $\mathcal{D}$ is clearly a finite set. Hence, it suffices to show that μ is injective. So suppose $F_1, F_2 \in \mathcal{F}$ such that

$$g_{F_1} = g_{F_2} = g$$

then let $g(x) = b_0 + b_1x + \ldots + b_mx^m \in L[x]$ and set

$$F_0 = k(b_0, b_1, \ldots, b_m) \subset F_1 \cap F_2$$

By definition, $g_{F_0} \mid g$ in $F_0[x] \subset L[x]$, so

$$\begin{aligned} \deg(g_{F_0}) &\leq \deg(g) \\ &= [L : F_1] \\ &\leq [L : F_0] \qquad \text{(since } F_0 \subset F_1\text{)} \\ &= \deg(g_{F_0}) \end{aligned}$$

Hence, it follows that $[L : F_1] = [L : F_0]$ and so $F_1 = F_0$. Similarly, $F_2 = F_0$, so $F_1 = F_2$ □

4.9. Remark: Note that, in the above proof,

$$F_1 = F_0 = k(a_0, a_1, \ldots, a_n)$$

where the a_i are the coefficients of g_{F_1}. This gives a constructive way of determining all intermediate fields of a simple extension. We illustrate this with an example: Take

$$k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2}) \Rightarrow f(x) = x^4 - 2$$

so the possible monic divisors of f (with $\sqrt[4]{2}$ as a root) in $L[x]$ are multiples of the 4 linear terms

$$(x - \sqrt[4]{2}), (x - i\sqrt[4]{2}), (x + i\sqrt[4]{2}), (x + \sqrt[4]{2})$$

Note that there are $2^3 = 8$ such possibilities in $\mathbb{C}[x]$. However, we must disallow some of them because $i \notin L$ (and hence any polynomial with a coefficient involving i must be disallowed). We list down the remaining polynomials, and the corresponding intermediate field (obtained by adjoining the coefficients of the polynomial to $\mathbb{Q}$) below.

$$\begin{aligned} g_0(x) &= (x - \sqrt[4]{2}) && L \\ g_3(x) &= (x - \sqrt[4]{2})(x + \sqrt[4]{2}) && \mathbb{Q}(\sqrt{2}) \\ g_4(x) &= (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) && \mathbb{Q}(\sqrt[4]{2} + \sqrt{2}, \sqrt[4]{8}) = L \\ g_7(x) &= x^4 - 2 && \mathbb{Q} \end{aligned}$$

Hence, the only possible intermediate fields are

$$\{\mathbb{Q}, \mathbb{Q}(\sqrt{2}), L\}$$

(End of Day 14)

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 (Example I.1.4)

(ii) $k = \mathbb{Q}(\sqrt{2})$: There are two maps, $\{i, j\}$ where $j(a + b\sqrt{2}) = a - b\sqrt{2}$ (HW 1.4)

(iii) $k = \mathbb{Q}(\omega)$: We have the inclusion map

$$\iota : k \to \mathbb{C}$$

Suppose $\varphi : k \to \mathbb{C}$ is another homomorphism, then φ is $\mathbb{Q}$-linear (See Example 1.8). A $\mathbb{Q}$-basis for k is $\{1, \omega\}$. Hence, φ is completely determined by

$$\alpha := \varphi(\omega)$$

Now $\omega^3 = 1$, so $\alpha^3 = 1$, so

$$\alpha \in \{1, \omega, \omega^2\}$$

However, if $\alpha = 1$, then $\varphi(1) = \varphi(\omega)$, which contradicts the fact that φ is injective. Hence,

$$\alpha \in \{\omega, \omega^2\}$$

If $\alpha = \omega$, then $\varphi = \iota$. If $\alpha = \omega^2$, then we get the map

$$j : k \to \mathbb{C} \text{ given by } a + b\omega \mapsto a + b\omega^2$$

Hence, there are atmost two homomomorphisms from $k \to \mathbb{C}$.

(iv) $k = \mathbb{Q}(\sqrt[3]{2})$: We have the inclusion map. Suppose $\varphi : k \to \mathbb{C}$ is any homomorphism, then, as above, φ is determined by its values on the set

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$$

Since $\varphi(1) = 1$ and $\varphi(\sqrt[3]{4}) = \varphi(\sqrt[3]{2})^2$, it follows that φ is completely determined by

$$\alpha := \varphi(\sqrt[3]{2})$$

As above, $\alpha^3 = 2$, so $\alpha \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. Each choice gives a map, so we have atmost 3 maps from $k \to \mathbb{C}$.

(v) $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$: If $\varphi : k \to \mathbb{C}$ is a homomorphism, then φ is determined by its values on the set

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

Since $\varphi(1) = 1$ and $\varphi(\sqrt{6}) = \varphi(\sqrt{2})\varphi(\sqrt{3})$, we only need to determine

$$\alpha := \varphi(\sqrt{2}) \text{ and } \beta := \varphi(\sqrt{3})$$

As in HW 1.4,

$$\alpha = \pm\sqrt{2} \text{ and } \beta = \pm\sqrt{3}$$

so we obtain atmost 4 maps from $k \to \mathbb{C}$

(vi) $k = \mathbb{Q}(\sqrt[3]{2}, \omega)$: Recall that $[k : \mathbb{Q}] = 6$ (HW 4.4), and, in fact,

$$k = F_1F_2 \text{ where } F_1 = \mathbb{Q}(\sqrt[3]{2}) \text{ and } F_2 = \mathbb{Q}(\omega)$$

Hence, by the proof of II.2.9, a $\mathbb{Q}$-basis for k is given by

$$\{1, \omega, \sqrt[3]{2}, \sqrt[3]{4}, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$$

As before, if $\varphi : k \to \mathbb{C}$ is a homomorphism, then φ is determined by two values

$$\alpha := \varphi(\omega) \text{ and } \beta := \varphi(\sqrt[3]{2})$$

Once again, $\alpha \in \{\omega, \omega^2\}$ and $\beta \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. Hence, we have atmost 6 maps from $k \to \mathbb{C}$. We will now show that there are exactly 6.

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.

Proof. (i) Write $f(x) = a_0 + a_1x + \ldots + a_nx^n$, then

$$\varphi(f(\alpha)) = \varphi(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\beta + \ldots + a_n\beta^n$$

since φ fixes all the a_i's.

(ii) Since α is algebraic over k, $\exists 0 \neq f \in k[x]$ such that $f(\alpha) = 0$. By part (i), it follows that $f(\beta) = 0$

(iii) Let $f = m_{\alpha,k}$, then by part (i),

$$f(\beta) = 0$$

But since f is irreducible and monic, it follows by uniqueness (See II.1.5) that $f = m_{\beta,k}$ as well.

□

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

$$\{k\text{-homomorphisms from } k(\alpha) \to \mathbb{C}\} \leftrightarrow \{\text{roots of } m_\alpha \text{ in } \mathbb{C}\}$$

Proof. Let $\mathcal{F}$ and $\mathcal{G}$ denote the LHS and RHS above. Then by the previous Lemma, we have a map

$$\mu : \mathcal{F} \to \mathcal{G} \text{ given by } \varphi \mapsto \varphi(\alpha)$$

We claim that μ is bijective:

(i) Injectivity: Let $n = [k(\alpha) : k]$. If $\varphi(\alpha) = \psi(\alpha)$, then

$$\varphi(\alpha^j) = \psi(\alpha^j) \quad \forall 1 \leq j \leq n-1$$

Since $\varphi(1) = \psi(1)$, this means that φ and ψ agree on the set

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

But this set forms a k-basis of $k(\alpha)$, and φ and ψ are two k-linear maps. Hence, $\varphi = \psi$.

(ii) Surjectivity: If $\beta \in \mathbb{C}$ is a root of m_α, then by Corollary II.1.10, $\exists \varphi : k(\alpha) \to \mathbb{C}$ such that $\varphi|_k = \mathrm{id}_k$ and $\varphi(\alpha) = \beta$. Hence, $\mu(\varphi) = \beta$.

□

1.4. Corollary: Let $k \subset L$ be a finite extension, then

$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \mathbb{C} = [L : k]$$

Proof. By the primitive element theorem, $\exists \alpha \in L$ such that $L = k(\alpha)$. Then by Theorem 1.3,

$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \mathbb{C} = \text{the number of roots of } m_\alpha \text{ in } \mathbb{C}$$

Since m_α is irreducible in $k[x]$, it is separable by II.4.4, so

$$\text{the number of } k\text{-homomorphisms } \varphi : L \to \mathbb{C} = \deg(m_\alpha) = [L : k]$$

by II.2.4. □

(End of Day 15)

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

(i) A k-homomorphism $\varphi : L \to \mathbb{C}$ is said to be a $\underline{k\text{-automorphism}}$ if

$$\varphi(L) = L$$

Note that

(a) φ is already injective, so this means that $\varphi : L \to L$ is bijective.

(b) Hence, we may compose any two k-automorphisms to obtain a third k-automorphism.

(c) The inclusion map $\iota : L \to \mathbb{C}$ is a k-automorphism, and has the property that

$$\iota \circ \varphi = \varphi = \varphi \circ \iota$$

for any k-automorphism φ.

(ii) The Galois group of L over k is set of all k-automorphisms of L. Note that this is a group under composition, and it is denoted by

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

1.6. Lemma: Let $k \subset L$ be an algebraic field extension, and $\varphi : L \to \mathbb{C}$ a k-homomorphism.

(i) If $\varphi(L) \subset L$, then $\varphi : L \to L$ is bijective.

(ii) If $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\varphi(\alpha_i) \in L$ for all $1 \leq i \leq n$, then $\varphi : L \to L$ is bijective.

Proof. (i) Suppose $\varphi(L) \subset L$, then we WTS: $\varphi(L) = L$. So choose $\alpha \in L$, then α is algebraic over k, so consider $f = m_\alpha$. By Lemma 1.2, $\varphi(\alpha)$ is also a root of f and $\varphi(\alpha) \in L$. Hence if

$$R = \{\text{ roots of } f \text{ in } L\}$$

Then φ maps R to R. Since φ is injective, it must map R onto R. In particular, $\exists \beta \in R \subset L$ such that $\varphi(\beta) = \alpha$. Hence $\varphi(L) = L$.

(ii) If $L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is an algebraic extension, and $\varphi(\alpha_i) \in L$ for all $1 \leq i \leq n$, then we WTS: $\varphi(L) \subset L$. For each $1 \leq i \leq n$, let

$$K_i = k(\alpha_1, \alpha_2, \ldots, \alpha_i)$$

Then consider the tower

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

Write

$$S_i = \{1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n_i - 1}\}$$

where $n_i = [K_i : K_{i-1}]$, then S_i is a basis for K_i over K_{i-1}. Hence, by the Tower Law, the set

$$T = \{x_1 x_2 \ldots x_n : x_i \in S_i, 1 \leq i \leq n\}$$

is a basis for L over k. Now if $\varphi(\alpha_i) \in L$ for all $1 \leq i \leq n$, then

$$\varphi(S_i) \subset L \quad \forall 1 \leq i \leq n$$

and hence $\varphi(T) \subset L$. Since φ is k-linear, it follows that

$$\varphi(L) \subset L$$

Now part (i) applies.

□

1.7. Remark :

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

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

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

(iv) Hence, if $k \subset L = k(\theta)$ is a finite, then $|\operatorname{Gal}_k(L)| = [L : k]$ iff every complex root of m_θ is already in L.

1.8. Examples:

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

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

Proof. Note that $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$ contains two maps, the inclusion and $j : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ given by

$$j(a + b\sqrt{2}) = a - b\sqrt{2}$$

Hence, $|\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))| = 2$ so $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$ □

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

Proof. Same proof as part (ii) with $j(a + b\omega) = a + b\omega^2$ □

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

Proof. Note that there are 3 homomorphisms from $L := \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, given by

$$\iota(\sqrt[3]{2}) = \sqrt[3]{2}$$
$$\varphi_1(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$
$$\varphi_2(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$$

But note that $\omega \notin L$ (since $L \subset \mathbb{R}$), and so $\omega\sqrt[3]{2} \notin L$. Similarly, $\omega^2\sqrt[3]{2} \notin L$, and so $\varphi_1, \varphi_2 \notin \operatorname{Gal}_{\mathbb{Q}}(L)$. Hence,

$$\operatorname{Gal}_{\mathbb{Q}}(L) = \{\mathrm{id}_L\}$$

□

(v) $\operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Here, we have 4 possible maps from $L := \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{C}$ given by

$$\begin{aligned} \varphi_0(\sqrt{2}) = \sqrt{2} &\text{ and } \varphi_0(\sqrt{3}) = \sqrt{3} \\ \varphi_1(\sqrt{2}) = \sqrt{2} &\text{ and } \varphi_1(\sqrt{3}) = -\sqrt{3} \\ \varphi_2(\sqrt{2}) = -\sqrt{2} &\text{ and } \varphi_2(\sqrt{3}) = \sqrt{3} \\ \varphi_3(\sqrt{2}) = -\sqrt{2} &\text{ and } \varphi_3(\sqrt{3}) = -\sqrt{3} \end{aligned}$$

Now for each of these maps $\{\varphi_i(\sqrt{2}), \varphi_i(\sqrt{3})\} \subset L$. Hence, by Lemma 1.6, $\varphi_i \in \operatorname{Gal}_{\mathbb{Q}}(L)$ for all $0 \leq i \leq 3$. Hence,

$$|\operatorname{Gal}_{\mathbb{Q}}(L)| = 4 \Rightarrow \operatorname{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ or } \mathbb{Z}_4$$

Now note that for each $1 \leq i \leq 3$,

$$\varphi_i^2(\sqrt{2}) = \varphi_i(\pm\sqrt{2}) = \sqrt{2} \text{ and similarly } \varphi_i^2(\sqrt{3}) = \sqrt{3}$$

Hence, $\varphi_i^2 = \mathrm{id}_L$ for all $1 \leq i \leq 3$. In particular, $\operatorname{Gal}_{\mathbb{Q}}(L)$ does not have an element of order 4. Hence,

$$\operatorname{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

□

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

Proof. As before, we let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, and enumerate the elements of $G = \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega))$.

$$\begin{aligned} \varphi_0(\sqrt[3]{2}) = \sqrt[3]{2} &\text{ and } \varphi_0(\omega) = \omega \\ \varphi_1(\sqrt[3]{2}) = \sqrt[3]{2} &\text{ and } \varphi_1(\omega) = \omega^2 \\ \varphi_2(\sqrt[3]{2}) = \omega\sqrt[3]{2} &\text{ and } \varphi_2(\omega) = \omega \\ \varphi_3(\sqrt[3]{2}) = \omega\sqrt[3]{2} &\text{ and } \varphi_3(\omega) = \omega^2 \\ \varphi_4(\sqrt[3]{2}) = \omega^2\sqrt[3]{2} &\text{ and } \varphi_4(\omega) = \omega \\ \varphi_5(\sqrt[3]{2}) = \omega^2\sqrt[3]{2} &\text{ and } \varphi_5(\omega) = \omega \end{aligned}$$

In each of these cases, by Lemma 1.6, $\varphi_i \in G$. Hence,

$$|G| = 6 \Rightarrow G \cong \mathbb{Z}_6 \text{ or } S_3$$

Hence, it suffices to show that G is non-abelian. Now note that

$$\varphi_1\varphi_3(\sqrt[3]{2}) = \varphi_1(\omega\sqrt[3]{2}) = \varphi_1(\omega)\varphi_1(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$$

However

$$\varphi_3\varphi_1(\sqrt[3]{2}) = \varphi_3(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$

Hence, $\varphi_1\varphi_3 \neq \varphi_3\varphi_1$, and so G is non-abelian. □

(End of Day 16)

(vii) If $p \in \mathbb{Z}$ prime, $\zeta = e^{2\pi i/p}$ and $L = \mathbb{Q}(\zeta)$, then $G := \text{Gal}_{\mathbb{Q}}(L) \cong \mathbb{Z}_p^*$

Proof. (a) Note that Φ_p is the minimal polynomial for ζ, so $[L : k] = p - 1$. Furthermore, a $\mathbb{Q}$-basis for L is

$$\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$$

Hence, if $\varphi : L \to \mathbb{C}$ is a homomorphism, φ is completely determined by $\alpha := \varphi(\zeta)$. By Theorem 1.3, we have $\alpha \in \{\zeta^j : 1 \leq j \leq p-1\}$, and hence we have exactly $p - 1$ maps

$$\varphi_j : L \to \mathbb{C} \text{ such that } \varphi_j(\zeta) = \zeta^j, \qquad 1 \leq j \leq p - 1$$

Note that for each $1 \leq j \leq p - 1, \varphi_j(\zeta) \subset L$, so $\varphi_j \in G$ by Lemma 1.6.

(b) Now note that

$$\varphi_i \circ \varphi_j(\zeta) = \varphi_i(\zeta^j) = \varphi_i(\zeta)^j = \zeta^{ij} = \varphi_{ij}(\zeta)$$

Hence, we define a map

$$\mu : \mathbb{Z}_p^* \to G \text{ given by } [i] \mapsto \varphi_i$$

We claim that μ is an isomorphism

(c) μ is well-defined: If $[i] = [j]$ in $\mathbb{Z}_p^*$, then $p \mid i - j$, so $\exists m \in \mathbb{Z}$ such that $i = j + mp$. Hence,

$$\varphi_i(\zeta) = \zeta^i = \zeta^j(\zeta^p)^m = \zeta^j = \varphi_j(\zeta)$$

Since any homomorphism is determined by its value on ζ, it follows that μ is well-defined

(d) μ is a homomorphism by step (b), and μ is surjective by step (a). Since

$$|G| = p - 1 = |\mathbb{Z}_p^*|$$

μ must also be injective, and hence an isomorphism.

□

1.9. Theorem: If $p \in \mathbb{Z}$ is prime, then $\mathbb{Z}_p^*$ is cyclic.

Proof. Note that $\mathbb{Z}_p^*$ is a finite abelian group. Hence, by the fundamental theorem of finite abelain groups, $\exists n_1, n_2, \ldots, n_k \in \mathbb{N}$ such that

$$n_1 \mid n_2 \mid \ldots \mid n_k$$

and

$$\mathbb{Z}_p^* \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$$

Note that since $|\mathbb{Z}_p^*| = p-1$, $n_k \mid p-1$. We claim that $n_k = p-1$, and hence $k = 1$.

To see this, note that for any $a \in \mathbb{Z}_p^*$,

$$a \mapsto (a_1, a_2, \ldots, a_k)$$

under the above isomorphism. Hence,

$$a^{n_k} \mapsto (n_k a_1, n_k a_2, \ldots, n_k a_k) = (0, 0, 0, \ldots, 0)$$

Hence, $a^{n_k} = 1$ in $\mathbb{Z}_p^*$. Now consider the polynomial

$$f(x) = x^{n_k} - 1 \in \mathbb{Z}_p[x]$$

By Corollary I.2.9, the number of roots in $\mathbb{Z}_p$ is $\leq n_k$. However, every element of $\mathbb{Z}_p^*$ is a root of f. Hence,

$$p - 1 \leq n_k$$

But $n_k \mid p-1$, so $n_k = p-1$ and we are done. □

Review of Chapters I, II and § III.1 for the Mid-Semester Exam.

(End of Day 17)

2. Splitting Fields and Normal Extensions

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

(i) We say that <u>f splits in L</u> if every complex root of f is in L

(ii) If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the set of all complex roots of f, then

$$L := k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

is called the <u>splitting field of f</u>. Equivalently, it is the smallest field containing k in which f splits.

(iii) A field extension $k \subset L$ is said to be <u>normal</u> if, for every k-homomorphism $\varphi : L \to \mathbb{C}$, we have $\varphi(L) = L$.

2.2. Remark:

(i) If $f \in k[x]$, then f splits in $\mathbb{C}$ (in fact, in $\overline{k}$), but these are not the splitting fields of f.

(ii) If L is the splitting field of f over k, then L is a finitely generated algebraic extension of k. Hence, $[L : k] < \infty$ by II.3.4.

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

Proof. We prove (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Suppose $k \subset L$ is a finite normal extension, then by the primitive element theorem, $\exists \alpha \in L$ such that $L = k(\alpha)$. Let f denote the minimal polynomial for α over k, then we claim that L is the splitting field of f over k.

(a) If F denotes the splitting field of f over k, then clearly $L \subset F$

(b) Conversely, if β is a root of f in $\mathbb{C}$, then, by II.1.10, $\exists$ a k-homomorphism

$$\varphi : k(\alpha) \to \mathbb{C} \text{ such that } \varphi(\alpha) = \beta$$

Since $k \subset L$ is normal, it follows that $\beta \in L$. This is true for any root β of f, and so f splits in L. By definition, $F \subset L$

(ii) $\Rightarrow$ (iii): By Remark 1.7(ii),

$$|\operatorname{Gal}_k(L)| \leq [L : k]$$

Now suppose L is the splitting field of f over k, then consider any k-homomorphism $\varphi : L \to \mathbb{C}$, then we WTS: $\varphi(L) = L$. Since

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

where $X = \{a_1, \alpha_2, \ldots, a_n\}$ is the set of complex roots of f, it suffices (by Lemma 1.6) to show that

$$\varphi(\alpha_i) \in L \quad \forall 1 \leq i \leq n$$

Now fix $1 \leq i \leq n$, and let p denote the minimal polynomial of α_i over k. Then, by Theorem 1.3, $\varphi(\alpha_i)$ is another root of p. However, since α_i is a root of f, we must have that $p \mid f$ in $k[x]$. Hence, $\varphi(\alpha_i)$ is another root of f, and so $\varphi(\alpha_i) \in X \subset L$. This is true for each $1 \leq i \leq n$, so $\varphi(L) = L$ by Lemma 1.6

(iii) $\Rightarrow$ (i): Trivial.

□

2.4. Definition: Let $k \subset \mathbb{C}$ be a field and $f \in k[x]$. If L is the splitting field of f over k, then $\operatorname{Gal}_k(L)$ is called the Galois group of f, denoted by $\operatorname{Gal}_k(f)$

2.5. Examples:

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

(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 $\operatorname{Gal}_k(f) \cong \mathbb{Z}_2$

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

(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 $\text{Gal}_k(f) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$

2.6. Corollary: Any extension of degree 2 is a normal extension.

Proof. If $k \subset L$ has degree 2, then by primitive element theorem, write $L = k(\theta)$ for some $\theta \in L$. If m_θ denotes the minimal polynomial of θ over k, then

$$\deg(m_\theta) = 2$$

and so we write $m_\theta(x) = x^2 + bx + c$ for some $b, c \in k$. Hence, the roots of m_θ are

$$\theta = \frac{-b + \sqrt{b^2 - 4c}}{2} \text{ and } \theta' = \frac{-b - \sqrt{b^2 - 4c}}{2}$$

Now since $\theta \in L$, it follows that

$$\sqrt{b^2 - 4c} \in L$$

and hence $\theta' \in L$. Thus, L is the splitting field of m_θ, and so $k \subset L$ is a normal extension by Theorem 2.3. □

(End of Day 18)

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

Proof. By the primitive element theorem, $\exists \alpha \in L$ such that $L = F(\alpha)$. If $\psi : L \to \mathbb{C}$ is a map as above, then ψ is completely determined by

$$\beta := \psi(\alpha)$$

So we wish to choose β appropriately.

(i) Let $F' = \varphi(F) \subset \mathbb{C}$, then $F' \cong F$. Hence, we obtain an isomorphism

$$\overline{\varphi} : F[x] \to F'[x] \text{ given by } \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \varphi(a_i) x^i$$

(ii) Since $F \subset L$ is finite, α is algebraic over F. Set $f = m_{\alpha,F} \in F[x]$, and let $g = \overline{\varphi}(f)$. Then there is an isomorphism (Check!)

$$\widehat{\varphi} : F[x]/(f) \to F'[x]/(g) \text{ such that } h + (f) \mapsto \overline{\varphi}(h) + (g)$$

In particular, g is irreducible in $F'[x]$ (by I.4.3)

(iii) Let $\beta \in \mathbb{C}$ be a root of g, then by II.1.9, $\exists$ an isomorphism

$$\mu : F'[x]/(g) \to F'(\beta) \text{ such that } \mu|_{F'} = \mathrm{id}_{F'} \text{ and } \overline{x} \mapsto \beta$$

Also, there is an isomorphism

$$\eta : F[x]/(f) \to F(\alpha) = L \text{ such that } \eta|_F = \mathrm{id}_F \text{ and } \overline{x} \mapsto \alpha$$

Hence, the map

$$\psi := \mu \circ \widehat{\varphi} \circ \eta^{-1} : L \to F'(\beta) \subset \mathbb{C}$$

is an isomorphism such that $\psi(\alpha) = \beta$. Note that if $z \in F$, then

$$\psi(z) = \mu \circ \widehat{\varphi}(z) = \mu(\varphi(z)) = \varphi(z)$$

□

2.8. Theorem: Let $k \subset L$ be a finite and normal extension, and $f \in k[x]$ be irreducible. Suppose $\exists \alpha \in L$ such that $f(\alpha) = 0$, then f splits in L.

Proof. Suppose $f(\alpha) = 0$, let β be any root of f in $\mathbb{C}$. WTS: $\beta \in L$. By Corollary II.1.10, there is a k-isomorphism

$$\varphi : k(\alpha) \to k(\beta) \text{ such that } \varphi(\alpha) = \beta$$

Since $\alpha \in L, F := k(\alpha) \subset L$. Hence, by the extension lemma, $\exists \psi : L \to \mathbb{C}$ such that

$$\psi|_F = \varphi \text{ and, in particular } \psi(\alpha) = \beta$$

Since $k \subset L$ is a normal extension, $\psi(L) = L$. In particular, $\beta \in L$. This is true for any root β of f in $\mathbb{C}$, and so f splits in L. □

2.9. Remark/Examples:

(i) The above theorem is clearly not true if $k \subset L$ is not normal (for instance, take $k = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$ and $f(x) = x^3 - 2$).

(ii) The theorem is also false if f is not irreducible. For instance, if $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$ and $f(x) = (x^2 - 2)(x^2 + 1)$, then f has a root in L, $k \subset L$ is a finite normal extension, but f does not split in L.

2.10. 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

Proof. (i) By the primitive element theorem, write $F = k(\alpha)$. Let M denote the splitting field of m_α over k, then M satisfies (i) and (ii) by Theorem 2.3 and Remark 2.2(ii).

(ii) Now suppose $k \subset L$ is a finite normal extension satisfying (i) and (ii), then $\alpha \in L$ since $M \subset L$. Hence by the previous theorem, m_α splits in L. Thus, $M \subset L$.

□

2.11. Examples:

(i) If $k \subset F$ is a normal extension, then $M = F$ is the normal closure of F.

(ii) If $k = \mathbb{Q}, F = \mathbb{Q}(\sqrt[3]{2})$, then $M = \mathbb{Q}(\omega, \sqrt[3]{2})$ is the normal closure of F.

3. Permutation of Roots

3.1. Definition: Let X be any set.

(i) A permutation of X is a bijective map $\sigma : X \to X$.

(ii) The set of all such permutations forms a group under composition, called the symmetric group on X, denoted by S_X.

(iii) We write $S_n := S_X$ where $X = \{1, 2, \ldots, n\}$

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

Proof. Let $Y = \{1, 2, \ldots, n\}$, and let $\mu : X \to Y$ be a bijection. Then define

$$\varphi : S_n \to S_X \text{ given by } \sigma \mapsto \mu^{-1} \circ \sigma \circ \mu$$

Then φ is a well-defined function since μ is bijective. Furthermore,

$$\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$$

so φ is a homomorphism. Now clearly, $\psi : S_X \to S_n$ defined by

$$\tau \mapsto \mu \circ \tau \circ \mu^{-1}$$

is a homomorphism such that $\varphi \circ \psi = \mathrm{id}_{S_X}$ and $\psi \circ \varphi = \mathrm{id}_{S_n}$, and so φ is bijective as well. □

3.3. Definition: Let G be a group and X be any set.

(i) A group action of G on X is a function

$$\alpha : G \times X \to X$$

such that, for all $g_1, g_2 \in G, x \in X$

(a) $\alpha(e, x) = x$, where e denotes the identity element of G

(b) $\alpha(g_1g_2, x) = \alpha(g_1, \alpha(g_2, x))$

If G acts on X, we write $g \cdot x := \alpha(g, x)$

(ii) A group action α of G on X is said to be faithful if, for any $g, h \in G$

$$\alpha(g, x) = \alpha(h, x) \quad \forall x \in X \Rightarrow g = h$$

(End of Day 19)

3.4. (Permutation Representation) Let G be a group, X any set, and $\alpha : G \times X \to X$ a group action. For $g \in G$, define

$$\sigma_g : X \to X \text{ by } \sigma_g(x) := \alpha(g, x)$$

(i) Then $\sigma_g \in S_X$

Define $\varphi : G \to S_X$ by

$$g \mapsto \sigma_g$$

(ii) Then φ is a group homomorphism.

(iii) φ is injective iff α is a faithful action.

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

Proof. (i) Note that if $\varphi \in \text{Gal}_k(f)$ and $\theta \in X$, then, by III.1.2

$$f(\varphi(\theta)) = 0$$

and so $\varphi(\theta) \in X$. This gives the map

$$\alpha : G \times X \to X \text{ given by } \alpha(\varphi, \theta) := \varphi(\theta)$$

and it is easy to see that this defines an action of G on X. To see that this action is faithful, note that if $\varphi, \psi \in G$ such that

$$\varphi(\theta) = \psi(\theta) \quad \forall \theta \in X$$

then, since the splitting field of f is $L = k(X)$ and $\varphi|_k = \text{id}_k = \psi|_k$, it follows that

$$\varphi = \psi \text{ on } L \Rightarrow \varphi = \psi \text{ in } G$$

(ii) Now note that the permutation representation gives an injective homomorphism

$$G \hookrightarrow S_X \cong S_k$$

where $k = |X|$. However, $k \leq n$, so S_k is isomorphic to a subgroup of S_n.

□

3.6. Example:

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

(ii) Let $k = \mathbb{Q}(\omega)$ and $f(x) = x^3 - 2 \in k[x]$. Then $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of f over k. Hence, if $G = \operatorname{Gal}_k(f)$, then the action of G on $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ gives an injective homomorphism

$$G \hookrightarrow S_3$$

However, $|G| = [L : k] = 3$, so $G \cong A_3 \cong \mathbb{Z}_3$

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

(a) $|\operatorname{Gal}_{\mathbb{Q}}(f)| = 8$

(b) Thus $\operatorname{Gal}_{\mathbb{Q}}(f) \cong D_4$

Proof. (a) Let $L = \mathbb{Q}(\sqrt[4]{2}, i)$, then $\operatorname{Gal}_{\mathbb{Q}}(f) = \operatorname{Gal}_{\mathbb{Q}}(L)$ and

$$|\operatorname{Gal}_{\mathbb{Q}}(L)| = [L : k] = 8$$

since $F = \mathbb{Q}(\sqrt[4]{2}) \subset L$ and $i \notin F$.

(b) By Theorem 3.5, there is an injective homomorphism

$$\mu : G \to S_4$$

given by the action of G on

$$X := \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\} \leftrightarrow \{1, 2, 3, 4\}$$

Let $\varphi, \psi \in G$ be given by

$$\varphi(\sqrt[4]{2}) = \sqrt[4]{2} \text{ and } \varphi(i) = -i$$
$$\psi(\sqrt[4]{2}) = i\sqrt[4]{2} \text{ and } \psi(i) = i$$

Then under the map μ, we get

$$\mu(\varphi) = (24) \text{ and } \mu(\psi) = (1234)$$

Hence, $o(\varphi) = 2, o(\psi) = 4$ and (Check!)

$$\varphi\psi\varphi^{-1} = \psi^{-1}$$

So $D_4 \cong \langle \varphi, \psi \rangle < G$ but since $|G| = 8$, it must happen that $G \cong D_4$.

□

3.7. Definition: A group G on a set X is said to be transitive if, for any $x, y \in X, \exists g \in G$ such that $g \cdot x = y$.

3.8. Examples:

(i) S_n acts transitively on $\{1, 2, \ldots, n\}$.

(ii) A_n acts transitively on $\{1, 2, \ldots, n\}$.

Proof. If $n = 3$, then $A_3 = \{e, (123), (132)\}$ which clearly acts transitively on $\{1, 2, 3\}$. If $n \geq 3$, then for any $1 \leq i, j \leq n$, we WTS: $\exists \sigma \in A_n$ such that $\sigma(i) = j$. Then choose $1 \leq k, l \leq n$ such that $\{k, l\} \cap \{i, j\} = \emptyset$, then

$$\sigma = (ij)(kl) \in A_4$$

works. □

(iii) 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))

(iv) If $G = \text{Gal}_{\mathbb{Q}}((x^2 - 2)(x^2 - 3))$, then G does not act transitively on $X = \{\pm\sqrt{2}, \pm\sqrt{3}\}$.

3.9. Theorem: Let $f \in k[x]$ be separable, let $G = \text{Gal}_k(f)$ and let X be the set of roots of f in $\mathbb{C}$. Then G acts transitively on X iff f is irreducible in $k[x]$.

Proof. (i) Suppose G acts transitively on X. WTS: f is irreducible. By I.4.7, we may choose a monic irreducible polynomial $p \in k[x]$ such that $p \mid f$. Let α be a root of p, and β be any other root of f. Then by transitivity, $\exists \varphi \in G$ such that

$$\varphi(\alpha) = \beta$$

By III.1.2, this implies that α and β have the same minimal polynomial in $k[x]$, namely p. Hence, every root of f is a root of p. It follows that

$$f(x) = p(x)^n$$

for some $n \in \mathbb{N}, c \in k$. Since f is separable, $n = 1$ must hold and so f is irreducible.

(ii) Conversely, suppose f is irreducible in $k[x]$, and $\alpha, \beta \in X$. WTS: $\exists \psi \in G$ such that $\varphi(\alpha) = \beta$. Let $F := k(\alpha)$, then by III.1.3, $\exists$ a k-homomorphism $\varphi : F \to \mathbb{C}$ such that

$$\varphi(\alpha) = \beta$$

If L denotes the splitting field of f over k, then by the extension lemma, $\exists \psi : L \to \mathbb{C}$ such that $\psi|_F = \varphi$. Since $k \subset L$ is normal by III.2.3, it follows that $\psi \in G$. Finally,

$$\psi(\alpha) = \varphi(\alpha) = \beta$$

as required.

□

(End of Day 20)

4. The Galois Correspondence

4.1. Definition/Remark: Let $k \subset L$ be a field extension with Galois group G

(i) If F is an intermediate field, then

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

(ii) Let

$$\begin{aligned} \mathcal{F} &:= \{\text{intermediate fields } k \subset F \subset L\} \\ \mathcal{G} &:= \{\text{subgroups } H < G\} \end{aligned}$$

Then we have a map

$$\Phi : \mathcal{F} \to \mathcal{G} \text{ given by } F \mapsto \mathrm{Gal}_F(L)$$

Question: Is Φ injective/surjective?

4.2. Remark:

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

If $F = k$, then $\mathrm{Gal}_k(L) = G$. We visualize this with a tower diagram

$$\begin{tikzcd}
L \arrow[d, dash] & \{e\} \arrow[d, dash] \\
k & G
\end{tikzcd}$$

(ii) 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

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

We say that the map $\Phi : \mathcal{F} \to \mathcal{G}$ is inclusion reversing.

4.3. Examples:

(i) 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

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

and Φ is bijective.

(ii) More generally, if $k \subset L$ is a normal extension with $[L : k]$ prime, then we have

(a) $\mathcal{F} = \{k, L\}$ (by II.2.8)

(b) $|G| = [L : k]$, so $G \cong \mathbb{Z}_p$. Hence, $\mathcal{G} = \{\{0\}, \mathbb{Z}_p\}$

and Φ is bijective in this case.

(iii) This is not true if $k \subset L$ is not normal. Beacause, if $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$, then $G = \{\mathrm{id}_L\}$, so

$$\Phi(k) = \Phi(L) = G$$

and so Φ is not injective in general.

(iv) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $G = \{\mathrm{id}_L, \varphi_1, \varphi_2, \varphi_3\}$, where

$$\varphi_1(\sqrt{2}) = \sqrt{2} \text{ and } \varphi_1(\sqrt{3}) = -\sqrt{3}$$
$$\varphi_2(\sqrt{2}) = -\sqrt{2} \text{ and } \varphi_2(\sqrt{3}) = \sqrt{3}$$
$$\varphi_3(\sqrt{2}) = -\sqrt{2} \text{ and } \varphi_3(\sqrt{3}) = -\sqrt{3}$$

Hence, G has 5 subgroups

$$\mathcal{G} = \{\{\mathrm{id}_L\}, \langle\varphi_1\rangle, \langle\varphi_2\rangle, \langle\varphi_3\rangle, G\}$$

And, we have

F	$\Phi(F)$
$\mathbb{Q}$	G
$\mathbb{Q}(\sqrt{2})$	$\langle\varphi_1\rangle$
$\mathbb{Q}(\sqrt{3})$	$\langle\varphi_2\rangle$
$\mathbb{Q}(\sqrt{6})$	$\langle\varphi_3\rangle$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$\{\mathrm{id}_L\}$

Hence, Φ is surjective.

Question: What is $\mathcal{F}$ in this case? Is Φ bijective?

(v) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, then $G = \{\mathrm{id}_L, \varphi_1, \ldots, \varphi_5\}$, where

$$\begin{aligned}
\varphi_1(\sqrt[3]{2}) &= \sqrt[3]{2} \text{ and } \varphi_1(\omega) = \omega^2 \\
\varphi_2(\sqrt[3]{2}) &= \omega\sqrt[3]{2} \text{ and } \varphi_2(\omega) = \omega \\
\varphi_3(\sqrt[3]{2}) &= \omega\sqrt[3]{2} \text{ and } \varphi_3(\omega) = \omega^2 \\
\varphi_4(\sqrt[3]{2}) &= \omega^2\sqrt[3]{2} \text{ and } \varphi_4(\omega) = \omega \\
\varphi_5(\sqrt[3]{2}) &= \omega^2\sqrt[3]{2} \text{ and } \varphi_5(\omega) = \omega^2
\end{aligned}$$

Hence, we have a table

F	$\Phi(F)$
$\mathbb{Q}$	$G \cong S_3$
$\mathbb{Q}(\sqrt[3]{2})$	$\langle\varphi_1\rangle \cong \langle(23)\rangle$
$\mathbb{Q}(\omega)$	$\langle\varphi_2\rangle \cong \langle(123)\rangle$
$\mathbb{Q}(\omega\sqrt[3]{2})$	$\langle\varphi_5\rangle \cong \langle((13)\rangle$
$\mathbb{Q}(\omega^2\sqrt[3]{2})$	$\langle\varphi_2\rangle \cong \langle((12)\rangle$
L	$\{\mathrm{id}_L\}$

Once again, Φ is surjective, but what is $\mathcal{F}$ and is Φ injective?

4.4. Definition: For $H < G$, define the fixed field of H to be

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

Note that $L^H \in \mathcal{F}$. Hence, we get a map

$$\Psi : \mathcal{G} \to \mathcal{F} \text{ given by } H \mapsto L^H$$

4.5. Remark: Let $k \subset L$ be any field extension, and $G = \mathrm{Gal}_k(L)$

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

However, L^G may not be equal to k. If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$, then $G = \{\mathrm{id}_L\}$, so

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

(End of Day 21)

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

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

ie. Ψ is also inclusion reversing.

4.6. Examples:

(i) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$, then

(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

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

and Ψ is bijective (In fact, $\Psi = \Phi^{-1}$) because

$$\begin{aligned}
L^G &= \{\alpha \in L : \varphi(\alpha) = \alpha \quad \forall \varphi \in G\} \\
&= \{a + b\sqrt{2} : a + b\sqrt{2} = a - b\sqrt{2}\} \\
&= \{a + b\sqrt{2} : b = 0\} \\
&= \mathbb{Q}
\end{aligned}$$

(ii) Ψ is not injective in general, by Remark 4.5(i).

(iii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $G = \{\mathrm{id}_L, \varphi_1, \varphi_2, \varphi_3\}$, where

$$\begin{aligned}
\varphi_1(\sqrt{2}) &= \sqrt{2} \text{ and } \varphi_1(\sqrt{3}) = -\sqrt{3} \\
\varphi_2(\sqrt{2}) &= -\sqrt{2} \text{ and } \varphi_2(\sqrt{3}) = \sqrt{3} \\
\varphi_3(\sqrt{2}) &= -\sqrt{2} \text{ and } \varphi_3(\sqrt{3}) = -\sqrt{3}
\end{aligned}$$

Now suppose $H = \langle \varphi_1 \rangle$, then

$$\sqrt{2} \in L^H \Rightarrow \mathbb{Q}(\sqrt{2}) \subset L^H$$

Furthermore, if

$$\begin{aligned}
\alpha := a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\in L^H, \text{ then} \\
\varphi_1(\alpha) &= \alpha \\
\Rightarrow a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
\Rightarrow c\sqrt{3} + d\sqrt{6} &= 0 \\
\Rightarrow c = d &= 0 \\
\Rightarrow \alpha &\in \mathbb{Q}(\sqrt{2})
\end{aligned}$$

Since the set $\{\sqrt{3}, \sqrt{6}\}$ is $\mathbb{Q}$-linearly independent. Hence,

$$L^{\langle \varphi_1 \rangle} = \mathbb{Q}(\sqrt{2})$$

Similarly, we can compute L^H for the other subgroups in $\mathcal{G}$ to obtain the table

H	L^H
G	k
$\langle \varphi_1 \rangle$	$\mathbb{Q}(\sqrt{2})$
$\langle \varphi_2 \rangle$	$\mathbb{Q}(\sqrt{3})$
$\langle \varphi_3 \rangle$	$\mathbb{Q}(\sqrt{6})$
$\{\text{id}_L\}$	L

Hence, Ψ is injective, and $\Phi \circ \Psi(H) = H$ for all $H \in \mathcal{G}$ by Example 4.3(iv). Also, for all the fields listed above,

$$\Psi \circ \Phi(F) = F$$

However, we still do not know $\mathcal{F}$, so we cannot say if Ψ is surjective or not.

(iv) The same is true if $k = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ (See HW 7)

4.7. Remark: Let $k \subset L$ be a field extension with Galois group G. Set

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

Then

(i) $\Phi(k) = G$ and $\Phi(L) = \{\text{id}_L\}$.

$\Psi(\{e\}) = L$, but $\Psi(G) \neq k$ in general.

(ii) Φ and Ψ are both inclusion reversing functions.

(iii) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2})$, then Φ are Ψ are both bijective.

(iv) If $k \subset L$ is a finite normal extension with $[L : k]$ prime, then Φ is bijective, but we do not know if $L^G = k$. Hence, we cannot say if Ψ is bijective or not.

(v) If $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then

$$\Phi \circ \Psi(H) = H \quad \forall H \in \mathcal{G}$$

However, we don't know about $\Psi \circ \Phi$ as yet.

4.8. 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, $[L : k] \leq n$

Note that we do not know, a priori, whether $k \subset L$ is a finite extension, so we cannot directly apply the primitive element theorem.

Proof. Let $m := \sup\{[k(\alpha) : k] : \alpha \in L\}$, then $m \leq n < \infty$, so $\exists \beta \in L$ such that $m = [k(\beta) : k]$. We claim that $L = k(\beta)$: If not, then $\exists \gamma \in L \setminus k(\beta)$, then set $F = k(\beta, \gamma)$. Then $F \subset L$ and

$$[F : k] > [k(\beta) : k] = m$$

However, $[k(\gamma) : k] \leq n$, so by the tower law, $[F : k] \leq mn$ so $k \subset F$ is a finite extension. By the primitive element theorem, $\exists \delta \in F$ such that $F = k(\delta)$. But then

$$[k(\delta) : k] > m$$

which contradicts the definition of m. Hence, $L = k(\beta)$ as required. □

(End of Day 22)

4.9. 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 $f_\alpha \in F[x]$

Proof. Let $\sigma \in G$ and write $f_\alpha(x) = a_0 + a_1 x + \ldots + a_n x^n$, then note that

$$\begin{aligned}(\sigma^* f_\alpha)(x) &:= \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n \\ &= \prod_{\varphi \in G} (x - \sigma(\varphi(\alpha))\end{aligned}$$

But the map $\varphi \mapsto \sigma\varphi$ is a bijection on G, so

$$(\sigma^* f_\alpha)(x) = \prod_{\psi \in G} (x - \psi(\alpha)) = f_\alpha(x)$$

Hence, if $0 \leq i \leq n$, $a_i = \sigma(a_i)$ for all $\sigma \in G$, so $a_i \in L^G = F$. Thus, $f_\alpha \in F[x]$. □

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

Proof. (i) For any $\alpha \in L$, consider f_α as defined in the previous lemma. Then, $f_\alpha \in F[x]$. Since $\deg(f_\alpha) \leq |G|$,

$$[F(\alpha) : F] \leq |G| \quad \forall \alpha \in L$$

So by Lemma 5.3, $F \subset L$ is finite.

(ii) Since every $\varphi \in G$ fixes F by definition, we have $G \subset \mathrm{Gal}_F(L)$. But by Lemma 5.3, $\exists \beta \in L$ such that $L = F(\beta)$, so

$$|\mathrm{Gal}_F(L)| \leq [L : F] = [F(\beta) : F] \leq |G|$$

by part (i). Hence, $G = \mathrm{Gal}_F(L)$

$$|G| = |\mathrm{Gal}_F(L)| = [L : F]$$

so by Theorem 2.3, $F \subset L$ is normal and (iii) holds.

□

4.11. Lemma: Let $k \subset L$ be a field extension with Galois group G. Let $\mathcal{F}, \mathcal{G}, \Phi$, and Ψ be as above.

(i) For any $F \in \mathcal{F}$, we have

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

(ii) For any $H \in \mathcal{G}$, we have

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

Proof. HW. □

4.12. (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 $F \in \mathcal{F}$,

$$F = \Psi \circ \Phi(F)$$

(ii) For all $H \in \mathcal{G}$,

$$H = \Phi \circ \Psi(H)$$

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

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

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

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

We visualize this by a tower diagram

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

Proof. (i) Let $F \in \mathcal{F}$ and $H = \Phi(F) = \mathrm{Gal}_F(L)$. Then $H < G < \mathrm{Gal}_{\mathbb{Q}}(L)$ is a finite group, so let $\widetilde{F} = L^H = \Psi(H)$. By Lemma 4.11,

$$F \subset \widetilde{F}$$

But by Artin's Lemma, $\widetilde{F} \subset L$ is a finite normal extension with

$$\mathrm{Gal}_{\widetilde{F}}(L) = H$$

Since both extensions $F \subset L$ and $\widetilde{F} \subset L$ are normal, by Theorem 2.3,

$$[F : L] = |\,\mathrm{Gal}_F(L)| = |H| = |\,\mathrm{Gal}_{\widetilde{F}}(L)| = [L : \widetilde{F}]$$

So by the tower law applies to $F \subset \widetilde{F} \subset L$, we see that $F = \widetilde{F}$ as required.

(ii) Let $H \in \mathcal{G}$, and $F = \Psi(H) = L^H$. Then by Artin's Lemma, $F \subset L$ is a finite normal extension with

$$\mathrm{Gal}_F(L) = H$$

(iii) If $F \in \mathcal{F}$, then by Tower Law and Theorem 2.3

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

□

4.13. Corollary: Let $k \subset L$ be a finite normal extension with Galois group G. If $\alpha \in L$ is such that

$$\varphi(\alpha) = \alpha \quad \forall \varphi \in G$$

then $\alpha \in k$.

4.14. Examples:

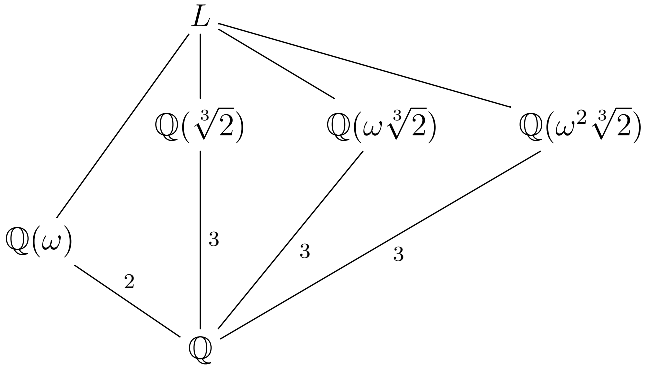
(i) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then the subfields of L are precisely

$$\mathcal{F} = \{\mathbb{Q}, L, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\}$$

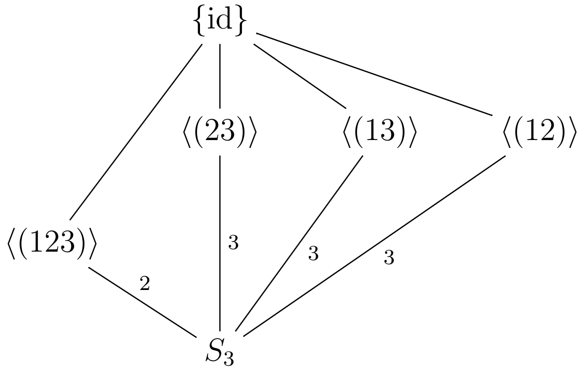
(ii) Similarly, if $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, then the subfields of L are precisely

$$\mathcal{F} = \{\mathbb{Q}, L, \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega^2\sqrt[3]{2}), \mathbb{Q}(\omega)\}$$

The <u>lattice</u> of subfields is


L
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$
$\mathbb{Q}(\omega^2\sqrt[3]{2})$
$\mathbb{Q}(\omega)$
3
3
3
2
$\mathbb{Q}$

and the lattice of subgroups is



(End of Day 23)

5. Normal Extensions

Throughout this section, let $k \subset L$ be a finite normal extension with Galois group G.

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

5.1. Theorem: Let $F \in \mathcal{F}$ such that $k \subset F$ is normal.

(i) The restriction map

$$\pi : \operatorname{Gal}_k(L) \to \operatorname{Gal}_k(F)$$

is a well-defined, surjective, group homomorphism.

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

(iii) Hence,

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

(iv) And, furthermore,

$$\operatorname{Gal}_k(L)/\operatorname{Gal}_F(L) \cong \operatorname{Gal}_k(F)$$

Proof. (i) Let $\varphi \in \operatorname{Gal}_k(L)$, and consider

$$\psi := \varphi|_F : F \to \mathbb{C}$$

Then ψ is a k-homomorphism. Since $k \subset F$ is normal, $\psi(F) = F$, so $\psi \in \operatorname{Gal}_F(L)$. Hence the function

$$\pi : \operatorname{Gal}_k(L) \to \operatorname{Gal}_k(F) \text{ given by } \varphi \mapsto \varphi|_F$$

is well-defined. Furthermore, since both group operations are composition, it is clearly a group homomorphism.

Now suppose $\psi \in \mathrm{Gal}_k(F)$, then consider $\psi : F \to \mathbb{C}$. Since $F \subset L$ is finite (since $k \subset L$ is finite), by the Extension lemma, $\exists \varphi : L \to \mathbb{C}$ such that

$$\varphi|_F = \psi$$

In particular, ψ is a k-homomorphism. Since $k \subset L$ is normal, $\varphi \in \mathrm{Gal}_k(L)$, and clearly, $\pi(\varphi) = \psi$. Hence, π is a surjective group homomorphism.

(ii) Now note that, for $\varphi \in \mathrm{Gal}_k(L)$

$$\begin{aligned} \varphi \in \ker(\pi) &\Leftrightarrow \varphi|_F = \mathrm{id}_F \\ &\Leftrightarrow \varphi \in \mathrm{Gal}_F(L) \end{aligned}$$

Hence,

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

(iii) Since $\mathrm{Gal}_F(L)$ is the kernel of a group homomorphism,

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

(iv) Furthermore, by the first isomorphism theorem,

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

□

5.2. 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)
$$\mathrm{Gal}_{\psi(F)}(L) = \psi\,\mathrm{Gal}_F(L)\psi^{-1}$$

Proof. (i) It is clear that $\psi(F)$ is a field [Check!], and since $\psi|_k = \mathrm{id}_k$ and $\psi(L) \subset L$, it follows that $k \subset \psi(F) \subset L \Rightarrow \psi(F) \in \mathcal{F}$.

(ii) We prove "$\supset$": Let $\varphi \in \mathrm{Gal}_F(L)$, and $\beta \in \psi(F)$, then $\exists \alpha \in F$ such that $\beta = \psi(\alpha)$, so

$$\psi\varphi\psi^{-1}(\beta) = \psi(\varphi(\alpha)) = \psi(\alpha) = \beta$$

and so $\psi\varphi\psi^{-1} \in \mathrm{Gal}_{\psi(F)}(L)$, which proves "$\supset$".

For the inclusion "$\subset$": Let $K = \psi(F) \in \mathcal{F}$, then by the first inclusion with ψ^{-1} playing the role of ψ, we have

$$\psi^{-1}\,\mathrm{Gal}_K(L)\psi \subset \mathrm{Gal}_{\psi^{-1}(K)}(L)$$

Since $\psi^{-1}(K) = F$, we have

$$\Rightarrow \operatorname{Gal}_{\psi(F)}(L) = \operatorname{Gal}_K(L) \subset \psi \operatorname{Gal}_{\psi^{-1}(K)}(L)\psi^{-1} = \psi \operatorname{Gal}_F(L)\psi^{-1}$$

as required.

□

5.3. (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, for any $F \in \mathcal{F}$

$$k \subset F \text{ is normal iff } \operatorname{Gal}_F(L) \lhd \operatorname{Gal}_k(L)$$

Furthermore, in that case, the conclusions of Theorem 5.1 hold.

Proof. If $k \subset F$ is normal, then it follows from Theorem 5.1.

Conversely, if $H := \operatorname{Gal}_F(L) \lhd \operatorname{Gal}_k(L) =: G$, then choose a homomorphism $\varphi : F \to \mathbb{C}$. Since $k \subset F \subset L$ are finite extensions, by the extension lemma, $\exists \psi : L \to \mathbb{C}$ extending ψ. Since $k \subset L$ is normal, $\psi \in \operatorname{Gal}_k(L)$. Since $H \lhd G$, by Lemma 5.3,

$$\psi H \psi^{-1} = H \Rightarrow \operatorname{Gal}_{\psi(F)}(L) = \operatorname{Gal}_F(L)$$

So by FTOG-I, $\psi(F) = F$. But $\psi|_F = \varphi$, so

$$\varphi(F) = F$$

This is true for any homomorphism $\varphi : F \to \mathbb{C}$, so $k \subset F$ is normal. □

5.4. Example: Let $k = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \omega)$

(i) If $F = \mathbb{Q}(\sqrt[3]{2})$, then $k \subset F$ is not normal, and so

$$\operatorname{Gal}_F(L) \cong \langle (23) \rangle$$

is not normal in $\operatorname{Gal}_k(L) \cong S_3$

(ii) If $F = \mathbb{Q}(\omega)$, then $k \subset F$ is normal, so

$$\operatorname{Gal}_F(L) \cong \langle (123) \rangle$$

is normal in S_3

5.5. Definition: A field extension $k \subset L$ is called

(i) abelian if it is finite, normal, and $\operatorname{Gal}_k(L)$ is an abelian group.

(ii) cyclic if it is finite, normal, and $\operatorname{Gal}_k(L)$ is an cyclic group.

5.6. Corollary: Let $k \subset L$ be a field extension

(i) If $k \subset L$ is an abelian extension, then, for any intermediate field F, both $k \subset F$ and $F \subset L$ are abelian.

(ii) If $k \subset L$ is a cyclic extension, then, for any intermediate field F, both $k \subset F$ and $F \subset L$ are cyclic.

(End of Day 24)

5.7. Theorem: Let $n \in \mathbb{N}, \zeta := e^{2\pi i/n}$, then

$$\mathbb{Q} \subset \mathbb{Q}(\zeta)$$

is an abelian extension. Furthermore, it is cyclic if n is prime. These extensions are called cyclotomic extensions

Proof. (i) Note that L is the splitting field of the polynomial $x^n - 1 \in \mathbb{Q}[x]$, so $k \subset L$ is finite and normal. (III.2.3)

(ii) Now suppose $\varphi \in G := \text{Gal}_k(L)$, then φ is completely determined by

$$\varphi(\zeta)$$

As in Example III.1.8, $\exists 1 \leq j \leq n-1$ such that

$$\varphi(\zeta) = \zeta^j$$

(iii) Now suppose $\varphi, \psi \in G$, then $\exists 1 \leq i, j \leq n-1$ such that

$$\varphi(\zeta) = \zeta^i \text{ and } \psi(\zeta) = \zeta^j$$

Hence,

$$\varphi(\psi(\zeta)) = \zeta^{ij} = \psi(\varphi(\zeta))$$

Hence, $\varphi \circ \psi = \psi \circ \varphi$, so G is abelian.

(iv) If $n \in \mathbb{N}$ is prime, then this follows from III.1.9

□

5.8. Theorem: Let $k \subset L$ be finite extensions and $\beta \in \mathbb{C}$ be algebraic over k. 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.

Proof. (i) Let $\varphi : L(\beta) \to \mathbb{C}$ be a L-homomorphism. Since $k \subset L$, we may restrict this map to get

$$\varphi|_{k(\beta)} \colon k(\beta) \to \mathbb{C}$$

and this is a k-homomorphism. Since $k \subset k(\beta)$ is normal, $\varphi(k(\beta)) = k(\beta)$. In particular,

$$\varphi(\beta) \in k(\beta) \subset L(\beta)$$

Since β is algebraic over k, it is algebraic over L, and so $L \subset L(\beta)$ is a finite extension. Hence by Lemma III.1.6,

$$\varphi(L(\beta)) = L(\beta)$$

(ii) Consider the map

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

Then this map is well-defined since $k \subset k(\beta)$ is normal. WTS: μ is injective. So suppose $\varphi \in \mathrm{Gal}_L(L(\beta))$ such that $\mu(\varphi) = \mathrm{id}_{k(\beta)}$, then in particular,

$$\varphi(\beta) = \beta$$

But since $L \subset L(\beta)$ is finite and $\varphi|_L = \mathrm{id}_L$, it follows (as in III.1.3) that

$$\varphi = \mathrm{id}_{L(\beta)}$$

□

5.9. Corollary: Let $k \subset \mathbb{C}$ be any field, $n \in \mathbb{N}$ and $\zeta := e^{2\pi i/n}$. Then

(i) $k \subset k(\zeta)$ is an abelian extension.

(ii) If n is prime, then $k \subset k(\zeta)$ is a cyclic extension.

Proof. By Theorem 5.8, with $k = \mathbb{Q}, L = k, \beta = \zeta$, we have that $k \subset k(\zeta)$ is a finite, normal and there is an injective map

$$\mathrm{Gal}_k(k(\zeta)) \to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$$

The result now follows from Theorem 5.7. □

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

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

(See [Stewart, §1.4.3])

(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 simple radical extension if $\exists \alpha \in L, n \in \mathbb{N}$ 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) A field extension $k \subset L$ is called a radical extension if $\exists$ a tower of intermediate fields

$$k = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n = L$$

such that $F_i \subset F_{i+1}$ is a simple radical extension for each $0 \leq i \leq n-1$.

(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 Corollary III.2.6)

(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 $F = \mathbb{Q}(\omega)$, 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) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a radical extension, but is not a simple radical extension.

Proof. Suppose $\exists \alpha \in L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $n \in \mathbb{N}$ such that $a := \alpha^n \in \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$. Let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Then $p(x)$ has a root in L, and $\mathbb{Q} \subset L$ is normal. Hence, by III.2.8, $p(x)$ must split in L. Furthermore, $p(x) \mid x^n - a \in \mathbb{Q}[x]$. Hence, if $\beta \in L$ is any root of $p(x)$, then $z := \beta/\alpha$ satisfies

$$z^n = 1$$

But since $z \in L \subset \mathbb{R}$, it follows that $z = \pm 1$. Hence the only possible roots of $p(x)$ are $\{\pm\alpha\}$. However, $\deg(p) = [L : \mathbb{Q}] = 4$, and p is separable by Corollary II.4.4. This is a contradiction. □

(End of Day 25)

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

Proof. Write

$$k = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_n = L$$

where $L_{i+1} = L_i(\alpha_i)$ and $a_i := \alpha_i^{m_i} \in L_i$. Hence,

$$L = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

Let f_i denote the minimal polynomial of α_i over k, and let

$$f(x) := \prod_{i=1}^{n} f_i(x) \in k[x]$$

and let M denote the splitting field of f over k. Then by Theorem III.2.3, $k \subset M$ is a finite, normal extension. We claim that $k \subset M$ is radical. For this, let $\{\beta_{i,j} : 1 \leq i \leq k_i\}$ be the set of complex roots of f_i in $\mathbb{C}$, then

$$M = k(\{\beta_{i,j}\})$$

and consider the subfields

$$\begin{aligned} &F_0 = k \\ &F_1 = k(\beta_{1,1}, \beta_{1,2}, \ldots, \beta_{1,k_1}) \\ &F_2 = F_1(\beta_{2,1}, \beta_{2,2}, \ldots, \beta_{2,k_2}) \\ &\ldots \\ &F_n = F_{n-1}(\beta_{n,1}, \beta_{n,2}, \ldots, \beta_{n,k_n}) = M \end{aligned}$$

It now suffices to show that $F_{i-1} \subset F_i$ is a radical extension for each $1 \leq i \leq n$. To see this, it suffices to show that

$$\beta_{i,j}^{m_i} \in F_{i-1} \quad \forall 1 \leq j \leq k_i \qquad (*)$$

Now for $1 \leq j \leq k_i$, then there is a k-isomorphism

$$k(\alpha_i) \to k(\beta_{i,j})$$

by Corollary II.1.10. By the Extension lemma, this extends a homomorphism

$$\varphi : F_i \to \mathbb{C} \text{ such that } \varphi|_k = \text{id}_k \text{ and } \varphi(\alpha_i) = \beta_{i,j}$$

Hence,

$$\beta_{i,j}^{m_i} = \varphi(\alpha_i^{m_i}) = \varphi(a_i) \in \varphi(L_i)$$

But $L_i = L_{i-1}(\alpha_{i-1}) \subset F_{i-1}$ (by induction on i). Hence,

$$\beta_{i,j}^{m_i} \in \varphi(F_{i-1})$$

Finally, note that $k \subset F_{i-1}$ is a normal extension since F_{i-1} is splitting field of the polynomial $\prod_{j<i} f_j \in k[x]$. Since φ is a k-homomorphism,

$$\beta_{i,j}^{m_i} \in F_{i-1}$$

This proves $(*)$ and hence $F_{i-1} \subset F_i$ is radical for each i, and so $k \subset M$ is also radical. □

1.5. 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.

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

(i) $k \subset F \subset M$ is a tower of simple radical extensions.

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

(iii) $\text{Gal}_F(M)$ is abelian

(iv) $\text{Gal}_k(M)/\text{Gal}_F(M)$ is abelian

Proof. Let $\alpha \in \mathbb{C}$ be any root of $f(x)$, then

$$M = k(\alpha, \zeta) = F(\alpha)$$

(i) WTS: $\text{Gal}_F(M) \lhd \text{Gal}_k(M)$. By FTOG-II, this is equivalent to showing that

$$k \subset k(\zeta)$$

is normal. This follows from Corollary III.5.9.

(ii) Note that $M = F(\alpha)$. If $\varphi : M \to \mathbb{C}$ is an F-homomorphism, then φ is completely determined by

$$\beta := \varphi(\alpha)$$

Since β is another root of $f(x)$ in $\mathbb{C}$, it follows that $\exists 0 \leq i \leq p-1$ such that

$$\beta = \zeta^i \alpha$$

Now if $\varphi, \psi \in \text{Gal}_F(M)$, then $\exists 0 \leq i, j \leq p-1$ such that

$$\varphi(\alpha) = \zeta^i \alpha \text{ and } \psi(\alpha) = \zeta^j \alpha$$

Since $\zeta \in F, \varphi(\zeta) = \psi(\zeta) = \zeta$, and so

$$\varphi \circ \psi(\alpha) = \zeta^j \varphi(\alpha) = \zeta^{i+j} \alpha = \psi \circ \varphi(\alpha)$$

This implies that $\varphi \circ \psi = \psi \circ \varphi$ in $\text{Gal}_F(M)$, and so $\text{Gal}_F(M)$ is abelian.

(iii) By FTOG-II,

$$\mathrm{Gal}_k(M)/\mathrm{Gal}_F(M) \cong \mathrm{Gal}_k(F)$$

and $F = k(\zeta)$. Now, $k \subset F$ is abelian by Corollary III.5.9.

□

1.7. Examples:

(i) If $f(x) = x^2 - 2$, then $F = k = \mathbb{Q}, M = \mathbb{Q}(\sqrt{2})$, so $\mathrm{Gal}_k(M)$ is itself abelian.

(ii) If $f(x) = x^3 - 2$, then $k = \mathbb{Q}, F = \mathbb{Q}(\omega), M = \mathbb{Q}(\sqrt[3]{2}, \omega)$, so (Example III.1.8)

$$\mathrm{Gal}_F(M) \cong \langle (123) \rangle \lhd S_3$$

Also, A_3 and $S_3/A_3 \cong \mathbb{Z}_2$ are both abelian.

(iii) If $f(x) = x^4 - 2$, then $k = \mathbb{Q}, F = \mathbb{Q}(i), M = \mathbb{Q}(\sqrt[4]{2}, i)$, so (Example III.3.6),

$$\mathrm{Gal}_F(M) \cong \langle (1234) \rangle \lhd D_4 \cong \mathrm{Gal}_k(M)$$

Hence, $\mathrm{Gal}_F(M)$ is abelian, and so is $D_4/\langle (1234) \rangle \cong \mathbb{Z}_2$

2. Solvable Groups

2.1. Definition: Let G be a finite group.

(i) A normal series for G is a tower of subgroups

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

such that $G_i \lhd G_{i-1}$ for all $1 \leq i \leq n$.

(ii) Given a normal series as above, the quotient groups G_{i-1}/G_i are called the factor groups of the series.

(iii) G is said to be solvable if it has a normal series whose factor groups are all abelian.

2.2. Examples:

(i) Every finite abelian group is solvable.

(ii) S_3 is solvable

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

Proof. If $|G| = 8$, then by the Sylow theorems, G has a subgroup H of order 4. Since

$$[G : H] = 2$$

$H \lhd G$. Furthermore, H is abelian, and $G/H \cong \mathbb{Z}_2$ is also abelian. □

(iv) S_4 is solvable.

Proof. Let $G_1 = A_4 \lhd S_4$ and let

$$G_2 = V_4 := \{e, (12)(34), (13)(24), (14)(32)\}$$

Then $G_2 \lhd A_4$ since $G_2 \lhd S_4$ [Check!], and so

$$S_4 > A_4 > V_4 > \{e\}$$

is the required normal series. □

(v) Let $k \subset \mathbb{C}$, $n \in \mathbb{N}$, and let M be the splitting field of $x^n - a \in k[x]$. Then $\text{Gal}_k(M)$ is solvable (by 1.6)

(End of Day 26)

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

Proof. Let

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

be a normal series with abelian factors, then if $H_i := H \cap G_i$, then

(i) $H_i \lhd H_{i-1}$ [Check!]

(ii) Consider

$$\mu : H_{i-1}/H_i \to G_{i-1}/G_i \text{ given by } xH_i \mapsto xG_i$$

Then μ is well-defined because if $xH_i = yH_i$ for some $x, y \in H_{i-1}$, then $x, y \in G_{i-1}$ and

$$y^{-1}x \in H_i \Rightarrow y^{-1}x \in G_i \Rightarrow xG_i = yG_i$$

(iii) Furthermore, μ is injective, because if $x, y \in H_{i-1}$ such that $xG_i = yG_i$, then

$$y^{-1}x \in G_i \text{ and } y^{-1}x \in H \Rightarrow y^{-1}x \in H_i \Rightarrow xH_i = yH_i$$

Hence, the factor groups of the normal series

$$H > H_1 > H_2 > \ldots > H_n = \{e\}$$

are all abelian.

□

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

(i) $HK = KH$

(ii) $HK < G$

Proof. (i) If $h \in H, k \in K$, we WTS: $hk \in KH$. Since, $H \lhd G$, so $k^{-1}hk \in H$, hence $\exists h_1 \in H$ such that

$$k^{-1}hk = h_1 \Rightarrow hk = kh_1 \in KH$$

Hence, $HK \subset KH$. By a similar argument, we see that $KH \subset HK$ as well.

(ii) If $x, y \in HK$, we WTS: $xy^{-1} \in HK$, so write

$$x = h_1k_1, y = h_2k_2 \text{ for } h_1, h_2 \in H, \text{ and } k_1, k_2 \in K$$

Then

$$xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$$

Since $HK = KH, \exists k \in K, h \in H$ such that

$$h_1k_1k_2^{-1} = kh$$

and so

$$xy^{-1} = khh_2^{-1} \in KH = HK$$

Hence, $HK \lhd G$

□

2.5. (Second Isomorphism Theorem): Let G be a group, $H \lhd G$ and $K < G$, then

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

(ii)

$$\frac{K}{H \cap K} \cong \frac{HK}{H}$$

Proof. (i) This is trivial since $H \lhd G$

(ii) Since $K \subset HK$, we may define a map

$$\pi : K \to HK/H \text{ by the composition } K \hookrightarrow HK \xrightarrow{\pi} HK/H$$

Now note that

$$\begin{aligned} x \in \ker(\pi) &\Leftrightarrow x \in K \text{ and } xH = H \\ &\Leftrightarrow x \in K \text{ and } x \in H \\ &\Leftrightarrow x \in H \cap K \end{aligned}$$

Hence by the first isomorphism theorem, we get (ii)

□

2.6. (Third Isomorphism Theorem): Let G be a group, $H, K \lhd G$ such that $H \subset K$, then

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

(ii)

$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

Proof. (i) If $xH \in K/H$ and $yH \in G/H$, then note that

$$x \in K, y \in G \Rightarrow yxy^{-1} \in K$$

and so $(yH)(xH)(yH)^{-1} \in K/H$ since the map $x \mapsto xH$ is a group homomorphism.

(ii) Define $\mu : G/H \to G/K$ given by

$$xH \mapsto xK$$

Note that this map is well-defined because $H \subset K$. Furthermore, it is a surjective group homomorphism, and

$$xH \in \ker(\mu) \Leftrightarrow xK = K \Leftrightarrow x \in K \Leftarrow xH \in K/H$$

Hence, $\ker(\mu) = K/H$ and we are done by the first isomorphism theorem.

□

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

Proof. If G is solvable and $H \lhd G$, then consider a normal series

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

with abelian factors. Since $H \lhd G$, by Lemma 2.5,

$$G_iH < G$$

and $H \lhd G_iH$ since $H \lhd G$. Now consider the groups

$$\overline{G_i} := G_iH/H$$

Then note that $G_iH < G_{i-1}H$. Also, since $H \lhd G$, and $G_i \lhd G_{i-1}$, we have

$$G_iH \lhd G_{i-1}H$$

Hence, by the Third isomorphism theorem

$$\overline{G_i} \lhd \overline{G_{i-1}}$$

Now we claim that $\overline{G_{i-1}}/\overline{G_i}$ is abelian. To prove this, we show that there is a surjective homomorphism

$$G_{i-1}/G_i \to \overline{G_{i-1}}/\overline{G_i}$$

Define $\pi : G_{i-1} \to \overline{G_{i-1}}$ by

$$G_{i-1} \hookrightarrow G_{i-1}H \xrightarrow{\pi} G_{i-1}H/H$$

Then π is surjective [Check!]. Let $\mu : \overline{G_{i-1}} \to \overline{G_{i-1}}/\overline{G_i}$ be the natural quotient map, then μ is also surjective. Hence the composition defines a surjective homomorphism

$$\eta := \mu \circ \pi : G_{i-1} \to \overline{G_{i-1}}/\overline{G_i}$$

Furthermore, if $x \in G_i$, then $\mu \circ \pi(x) = \mu(xH) = \overline{e}$, and hence

$$G_i \subset \ker(\eta)$$

Hence, we get an induced map

$$\overline{\eta} : G_{i-1}/G_i \to \overline{G_{i-1}}/\overline{G_i}$$

which is also surjective. In particular, $\overline{G_{i-1}}/\overline{G_i}$ is abelian, and so

$$G/H > \overline{G_1} > \overline{G_2} > \ldots > \overline{G_n} = \{\overline{e}\}$$

is a normal series for G/H with abelian factors. □

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

Proof. (i) If G is solvable and $H \lhd G$, then H and G/H are solvable by 2.3 and 2.9.

(ii) Conversely, assume that H and G/H are solvable. WTS: G is solvable. By hypothesis, there exist two normal series

$$H = H_0 > H_1 > H_2 > \ldots > H_n = \{e\} \text{ and}$$

$$G/H = T_0 > T_1 > T_2 > \ldots > T_m = \{\overline{e}\}$$

Let $\pi : G \to G/H$ is the natural quotient map, then consider

$$G_i := \pi^{-1}(T_i) = \{x \in G : \pi(x) \in T_i\}$$

Then

$$G = G_0 > G_1 > G_2 > \ldots > G_m = H$$

is a normal series and

$$G_{i-1}/G_i \cong T_{i-1}/T_i \text{ is an abelian group}$$

by the Third isomorphism theorem. Hence, we obtain a normal series

$$G = G_0 > G_1 > G_2 > \ldots > G_m = H = H_0 > H_1 > H_2 > \ldots > H_n = \{e\}$$

each of whose factors is an abelian group.

□

(End of Day 27)

2.9. Definition: Let $k \subset L$ be a simple radical extension. We say that $k \subset L$ is of <u>prime type</u> if $\exists \alpha \in L$ and $p \in \mathbb{N}$ prime such that

$$L = k(\alpha) \text{ and } \alpha^p \in k$$

2.10. Lemma: Let $k \subset L$ be a radical extension, then $\exists$ a tower of intermediate fields

$$k = F_0 \subset F_1 \subset \ldots \subset F_n = L$$

such that each $F_i \subset F_{i+1}$ is a simple radical extension of prime type.

Proof. We may assume WLOG that $k \subset L$ is a simple radical extension, and write $L = k(\alpha)$ such that

$$a := \alpha^n \in k \text{ for some } n \in \mathbb{N}$$

We induct on n.

(i) If n is prime, we are done.

(ii) If n is not prime, then choose $p \in \mathbb{N}$ prime such that $p \mid \mathbb{N}$, then consider

$$\beta := \alpha^{n/p}$$

and $F = k(\beta)$. Then $k \subset F$ is a simple radical extension of prime type, and

$$F \subset L = F(\alpha)$$

is a simple radical extension such that $\alpha^{n/p} \in F$. Since $|n/p| < n$, we may apply the induction hypothesis, and complete the proof.

□

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

Proof. Suppose $k \subset M$ is a finite normal and radical extension, let $G := \mathrm{Gal}_k(M)$. Write a series of intermediate fields

$$k = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n = M$$

such that each intermediate extension $F_i \subset F_{i+1}$ is a simple radical extension of prime type. We proceed by induction on n.

(i) If $n = 1$, then

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

Consider $f(x) := x^p - a \in k[x]$, and let $g(x) \in k[x]$ be the minimal polynomial of α over k.

(a) Assuming WLOG that $\alpha \notin k$, $\deg(g) > 1$, and g has a root α in M. Since $k \subset M$ is normal, g splits in M (III.2.8)

(b) Let $\beta \in M$ be any other root of g in M, then $f(\beta) = 0$ since $g \mid f$ in $k[x]$. Hence,

$$\zeta := \frac{\beta}{\alpha} \in M \text{ and } \zeta^p = 1 \text{ and } \zeta \neq 1$$

(c) Now consider

$$\Gamma := \{\theta \in M : \theta^p = 1\}$$
$$C_p = \{\zeta \in \mathbb{C} : \zeta^p = 1\}$$

Then, C_p is a cyclic group of order p, and $\Gamma < C_p$. By part (b), $\Gamma \neq \{1\}$, and so

$$\Gamma = C_p$$

(d) Hence, f splits in M. Since $M = k(\alpha)$, M is the splitting field of f over k. Thus, $\operatorname{Gal}_k(M)$ is a solvable group by Theorem 1.6

(ii) If $n > 1$, then

(a) Consider
$$F_1 = k(\alpha_1) \text{ with } a := \alpha^p \in k$$
As in part (i), $\zeta = e^{2\pi i/p} \in M$, and so
$$L := F_1(\zeta) \subset M$$
is a finite, radical extension of M which is also normal (since L is the splitting field of $x^p - a \in k[x]$).

(b) Furthermore, $\operatorname{Gal}_k(L)$ is solvable by Theorem 1.6.

(c) Now consider
$$L \subset LF_2 \subset LF_3 \subset \ldots LF_n = M \qquad (*)$$
Then each intermediate step is a simple radical extension of prime type, and $L \subset M$ is normal. Furthermore, there are $n-1$ terms in this series. Hence, by induction hypothesis,
$$\operatorname{Gal}_L(M) \text{ is solvable}$$

(d) However, $k \subset L$ is a normal extension, so by FTOG-II,
$$\operatorname{Gal}_L(M) \lhd \operatorname{Gal}_k(M) \text{ and } \operatorname{Gal}_k(M)/\operatorname{Gal}_L(M) \cong \operatorname{Gal}_k(L)$$
Hence, by Theorem 2.8, $\operatorname{Gal}_k(M)$ is solvable.

□

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

Proof. If f is solvable by radicals, then let L denote the splitting field of $f(x)$, and let M be a field such that
$$k \subset L \subset M$$
and $k \subset M$ is a radical extension (by Corollary 1.5). By Theorem 2.10, $\operatorname{Gal}_k(M)$ is a solvable group. Furthermore, $k \subset L$ is a normal extension (III.2.3), and so $\operatorname{Gal}_L(M) \lhd \operatorname{Gal}_k(M)$ and
$$\operatorname{Gal}_k(M)/\operatorname{Gal}_L(M) \cong \operatorname{Gal}_k(L) = \operatorname{Gal}_k(f)$$
In particular, $\operatorname{Gal}_k(f)$ is a quotient of $\operatorname{Gal}_k(M)$, and so it is solvable by 2.7. □

(End of Day 28)

3. An Insolvable Quintic

3.1. Definition: A group G is said to be simple if it has no normal subgroups other than $\{e\}$ and G.

3.2. Examples:

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

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

Proof. If G is finite abelian, and $p \mid |G|$, then by Cauchy's theorem, $\exists H < G$ such that $|H| = p$. Since G is abelian, $H \lhd G$. Since G is simple, $H = G$ and we are done. □

(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 express 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. Furthermore, if $\tau \in S_p$ has order p, then τ is a p-cycle.

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

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

(iv) Note that $|A_5| = 5!/2 = 60 = 5 \times 3 \times 2^2$. For $p \in \{2, 3, 5\}$, define

$$C_p = \{\tau \in A_5 : o(\tau) = p\}$$

Then $C_p \neq \emptyset$ by Cauchy's theorem. And, by part (ii),

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

(v) Let $\tau \in A_5$, then τ can be expressed as a product of disjoint cycles, whose lengths add up to 5 (including cycles of length 1, ie. fixed points). The only possibilities are:

(a) A 5-cycle

(b) A 3-cycle

(c) A product of 2 disjoint 2-cycles

(d) A 4-cycle

(e) A 2-cycle

Of these, the first 3 are in A_5, while the next two are not. Hence,

$$A_5 = \{e\} \cup C_2 \cup C_3 \cup C_5$$

3.4. Lemma: Let $\{a_1, a_2, \ldots, a_5\} \subset \{1, 2, \ldots, 5\}$, then

$$\begin{aligned}(a_1, a_2, a_3, a_4, a_5) &= (a_1, a_5)(a_1, a_4)(a_1, a_3)(a_1, a_2)\\ (a_1, a_2, a_3) &= (a_1, a_3)(a_1, a_2)\\ (a_1, a_4)(a_2, a_5) &= (a_1, a_2, a_3, a_4, a_5)(a_1, a_3, a_2, a_4, a_5)\\ (a_1, a_3)(a_2, a_4) &= (a_1, a_2, a_3)(a_1, a_2, a_4)\end{aligned}$$

Proof. [Check!] □

3.5. Lemma [See [Online Notes]]: If $p \in \{2, 3, 5\}$, then A_5 is generated by C_p.

Proof. (i) If $p = 2$: Let $H := \langle C_2 \rangle$. Then by Remark 3.3(v), it suffices to show that

$$C_5 \cup C_3 \subset H$$

(a) If $\tau \in C_5$, then write

$$\begin{aligned}\tau &= (a_1, a_2, a_3, a_4, a_5)\\ &= (a_1, a_5)(a_1, a_4)(a_1, a_3)(a_1, a_2)\\ \text{(Lemma 3.4)} &= ((a_1, a_5)(a_2, a_3))((a_2, a_3)(a_1, a_4))((a_1, a_3)(a_4, a_5))((a_4, a_5)(a_1, a_2))\\ &\in H\end{aligned}$$

(b) If $\tau \in C_3$, then write

$$\begin{aligned}\tau &= (a_1, a_2, a_3)\\ &= (a_1, a_2)(a_1, a_3)\\ \text{(Lemma 3.4)} &= ((a_1, a_2)(a_4, a_5))((a_4, a_5)(a_1, a_3))\\ &\in H\end{aligned}$$

(ii) If $p = 3$: Write $K = \langle C_3 \rangle$, then by part (i), it suffices to show that

$$C_2 \subset K$$

But this follows from the fourth formula of Lemma 3.4.

(iii) If $p = 5$, we use the same argument with the third formula in Lemma 3.4.

□

3.6. Lemma: Fix $p \in \{2,3,5\}$. For any $\tau, \sigma \in C_p, \exists \delta \in A_5$ such that

$$\tau = \delta\sigma\delta^{-1}$$

Proof. (i) If $p = 2$, we assume WLOG that $\tau = (12)(34)$. Write

$$\sigma = (a_1, a_2)(a_3, a_4)$$

Then consider $a_5 \in \{1,2,3,4,5\} \setminus \{a_1, a_2, a_3, a_4\}$, and write

$$\theta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \qquad (*)$$

Then [Check!] $\theta^{-1}\sigma\theta = \tau$. Now define

$$\delta := \begin{cases} \theta & : \theta \in A_5 \\ \theta \circ (12) & : \theta \notin A_5 \end{cases}$$

Then $\delta \in A_5$, and

$$\delta\sigma\delta^{-1} = (12)\tau(12) = \tau$$

(ii) If $p = 3$, we assume WLOG that $\tau = (123)$. Write

$$\sigma = (a_1, a_2, a_3)$$

As in part (i), $\exists \theta \in S_5$ such that

$$\theta\sigma\theta^{-1} = \tau$$

Now take

$$\delta := \begin{cases} \theta & : \theta \in A_5 \\ \theta \circ (45) & : \theta \notin A_5 \end{cases}$$

and this δ works.

(iii) If $p = 5$, we assume WLOG that $\tau = (12345)$, and write

$$\sigma = (a_1, a_2, a_3, a_4, a_5)$$

Then θ (as in $(*)$ above) satisfies

$$\theta\sigma\theta^{-1} = \tau$$

However, [Check!] $\theta \in A_5$ and hence $\delta = \theta$ works.

□

3.7. Theorem: A_5 is a simple group. In particular, A_5 is not solvable.

Proof. If $H \lhd A_5$, and $H \neq \{e\}$, then $|H| \mid |A_5| = 60$ implies that for some $p \in \{2, 3, 5\}$,

$$p \mid A_5$$

By Cauchy's theorem, $\exists \tau \in H \cap C_p$. However, any two elements of C_p are conjugate in A_5 by Lemma 3.6. Since $H \lhd A_5$

$$C_p \subset H$$

and so $A_5 = H$ by Lemma 3.5. □

(End of Day 29)

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

Proof. If $n \geq 5$, then $A_5 < S_5 < S_n$, so this follows from Theorems 3.7 and 2.3. □

3.9. 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 $G = S_p$

Proof. If $p = 2$, then $S_2 \cong \mathbb{Z}_2$ and there is nothing to prove. So assume p is an odd prime.

Let $\tau = (a, b), \sigma = (a_1, a_2, \ldots, a_p) \in G$.

(i) By relabelling, we may assume that $\tau = (1, 2)$. Since $\sigma(a_1) = a_2, \sigma^2(a_1) = a_3$ and so on, it follows that, $\exists 1 \leq i \leq p$ such that $\sigma^i(1) = 2$. Since $\sigma^i \in G$, we may assume that $\sigma = (1, 2, a_3, a_4, \ldots, a_p)$. Again, relabelling, we may assume that

$$\tau = (12) \text{ and } \sigma = (1, 2, \ldots, p)$$

(ii) Note that,

$$\sigma\tau\sigma^{-1} = (2, 3)$$
$$\sigma^2\tau\sigma^{-2} = (3, 4)$$

and so on. Hence,

$$\{(1, 2), (2, 3), (3, 4), \ldots, (p-1, p), (p, 1)\} \subset G$$

(iii) Note that,

$$(2, 3)(1, 2)(2, 3) = (1, 3)$$
$$(3, 4)(1, 3)(3, 4) = (1, 4)$$

and so on. Hence,

$$\{(1, 2), (1, 3), (1, 4), \ldots, (1, p)\} \subset G$$

(iv) Note that, if $1 \leq i, j \leq p$ with $i \neq j$, then

$$(i, j) = (1, i)(1, j) \in G$$

and so G contains all transpositions. By Remark 3.3(iii), $G = S_p$

□

3.10. 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 $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$

Proof. Let L denote the splitting field of f, and $G := \text{Gal}_k(f)$

(i) Since f is irreducible, f has exactly p roots, by II.4.4, $\{\alpha_1, \alpha_2, \ldots, \alpha_p\}$ in $\mathbb{C}$, and hence in L. Consider the action of G on the p-roots $\{\alpha_1, \alpha_2, \ldots, \alpha_p\}$ of f given by Theorem III.3.5. This gives an injective homomorphism

$$G \hookrightarrow S_p$$

so we assume $G < S_p$.

(ii) Since f is irreducible, $p \mid |G|$ by HW 6.5. By Cauchy's theorem, G has an element τ of order p. By Remark 3.3(ii), τ is a p-cycle.

(iii) Since f has two non-real roots, consider the map

$$j : \mathbb{C} \to \mathbb{C} \text{ given by } z \mapsto \overline{z}$$

and restrict it to L. Since $\mathbb{Q} \subset L$ is a normal extension, $j(L) = L$, so $j \in \text{Gal}_k(f)$. Note that

$$j^2 = \text{id}_L \text{ and } j \neq \text{id}_L$$

since f has non-real roots. Since f has exactly two non-real roots

$$j \in S_p$$

is a transposition.

(iv) Thus, G contains a transposition and a p-cycle. By Lemma 3.9, $G = S_p$.

□

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

Proof. We claim that $G := \text{Gal}_{\mathbb{Q}}(f) = S_5$.

(i) f is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion with $p = 5$

(ii) $f'(x) = 10x^4 - 20x^3 = 10x^3(x - 2)$. So $f'(x) = 0$ iff $x = 0$ or $x = 2$.

(iii) $f''(x) = 40x^3 - 60x^2 = 20x^2(2x - 3)$. Hence,

$$f''(0) = 0 \text{ and } f''(2) < 0$$

So $x = 2$ gives a local minimum of f, and $f(2) = -11$

(iv) At $x = -\delta$, $f'(x) > 0$ and at $x = +\delta, f'(x) < 0$ (for $\delta > 0$ small). Hence $x = 0$ is a local maximum of f, and $f(0) = 5 > 0$.

(v) Since f is an odd degree polynomial, $\lim_{x\to\pm\infty} f(x) = \pm\infty$. So,

(a) f increases from $-\infty$ to 0, cutting the X-axis once along the way.

(b) f decreases from 0 to 2, cutting the X-axis once along the way.

(c) f increases from 2 to $+\infty$, cutting the X-axis once along the way.

Thus, f has 3 real (and hence 2 non-real roots).

Thus, $\text{Gal}_{\mathbb{Q}}(f) = S_5$ by Theorem 3.10. □

3.12. Remark:

(i) Example 3.11 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 3.11 is a constructive proof of this theorem.

(iii) There may be other quintics which *can* be solved by radicals. (For instance, $x^5 - 2 \in \mathbb{Q}[x]$)

(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 2.10

Proof. Write

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

where each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is abelian. Fix $1 \leq i \leq n$, and we induct on

$$m := |G_i/G_{i+1}|$$

If m is prime, there is nothing to show. If m is not prime, then choose a prime $p \mid m$, then by Cauchy's theorem, $\exists H < G_i/G_{i+1}$ such that $|H| = p$. Since G_i/G_{i+1} is abelian, $H \lhd G_i/G_{i+1}$. Let

$$\pi : G_i \to G_i/G_{i+1}$$

by the quotient map. Then $\widehat{H} := \pi^{-1}(H) < G_i$ and, in fact, $\widehat{H} \lhd G_i$ [Check!]. Now consider the normal series

$$G_i > \widehat{H} > G_{i+1}$$

By the Third isomorphism theorem,

$$[G_i : \widehat{H}] = \frac{|G_i/G_{i+1}|}{|\widehat{H}/G_{i+1}|} = \frac{m}{p}$$

and hence $[\widehat{H} : G_{i+1}] = p$. Since

$$m/p < m$$

we may use the induction hypothesis, to obtain a series

$$G_i/\widehat{H} = K_0 > K_1 > K_2 > \ldots > K_\ell = \{\overline{e}\}$$

such that each $K_{j+1} \lhd K_j$ and $[K_j : K_{j+1}]$ is prime for each $1 \leq j \leq \ell - 1$. Now consider

$$\widehat{K_j} := \pi^{-1}(K_j) \text{ where } \pi : G_i \to G_i/H \text{ is the quotient map}$$

Then it follows that $\widehat{K_{j+1}} \lhd \widehat{K_j}$ and by the Third isomorphism theorem,

$$[\widehat{K_j} : \widehat{K_{j+1}}] \text{ is prime}$$

Finally, note that $\widehat{K_0} = G_i$ and $\widehat{K_\ell} = \widehat{H}$. Hence we get a normal series

$$G_i = \widehat{K_0} > \widehat{K_1} > \ldots > \widehat{K_\ell} = \widehat{H} > G_{i+1}$$

with each factor being of prime order. Repeating this process for each $1 \leq i \leq (n-1)$ gives us the required result. □

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

Then $\exists \alpha \in L^\times$ such that $\sigma(\alpha) = \zeta_p \alpha$.

Proof. (i) Consider $\sigma : L \to L$ as an F-linear transformation. Then, we wish to show that ζ_p is an eigen-value of σ. To this end, let $q \in F[x]$ denote the minimal polynomial of σ. Since

$$\sigma^p = \mathrm{id}_L$$

it follows that

$$q(x) \mid (x^p - 1) \text{ in } F[x]$$

Let Λ denote the set of roots of q in F, then

$$\Lambda \subset \{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\} =: \mu_p$$

We now wish to show that $\zeta_p \in \Lambda$.

(ii) We claim that Λ is a subgroup of μ_p: To see this, fix $\lambda, \mu \in \Lambda$, then $\exists 0 \neq \alpha, \beta \in L$ such that

$$\sigma(\alpha) = \lambda\alpha \text{ and } \sigma(\beta) = \mu\beta$$

Since σ is a field homomorphism,

$$\sigma(\alpha\beta) = \lambda\mu\alpha\beta \text{ and } \sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \lambda^{-1}\alpha^{-1}$$

and so $\lambda\mu, \lambda^{-1} \in \Lambda$, making Λ a multiplicative subgroup of μ_p.

(iii) But $|\mu_p| = p$, so

$$\Lambda = \{1\} \text{ or } \Lambda = \mu_p$$

However, if $\Lambda = \{1\}$, then $q(x) = x - 1$ and so $\sigma = \mathrm{id}_L$ contradicting the assumption that σ has order p in $\mathrm{Gal}_F(L)$. Thus,

$$\Lambda = \mu_p$$

and, in particular, $\zeta_p \in \Lambda$ as required.

□

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

Then $\exists \alpha \in L$ such that $L = F(\alpha)$ and $\alpha^p \in F$.

ie. $F \subset L$ is a simple radical extension of prime type.

Proof. Let σ denote a generator of $\mathrm{Gal}_F(L)$, then by the previous Lemma, $\exists \alpha \in L^\times$ such that $\sigma(\alpha) = \zeta_p\alpha$.

(i) We claim that $L = F(\alpha)$: To see this, let

$$H := \mathrm{Gal}_{F(\alpha)}(L) < \mathrm{Gal}_F(L)$$

and note that

$$\sigma^i(\alpha) = \zeta_p^i \alpha \neq \alpha \quad \forall 1 \leq i \leq p-1$$

Hence,

$$\sigma^i \notin H \quad \forall 1 \leq i \leq p-1$$

Since $\mathrm{Gal}_F(L) = \{\sigma^i : 0 \leq i \leq p-1\}$, it follows that

$$H = \{\mathrm{id}_L\}$$

Since $F(\alpha) \subset L$ and $F \subset L$ is normal, it follows from FTOG-I that

$$F(\alpha) = L^H = L^{\{\mathrm{id}_L\}} = L$$

(ii) We claim that: $a := \alpha^p \in F$. Note that

$$\sigma(a) = \sigma(\alpha^p) = [\sigma(\alpha)]^p = \zeta^p \alpha^p = \alpha^p = a$$

Since $\mathrm{Gal}_F(L) = \langle \sigma \rangle$,

$$\varphi(a) = a \quad \forall \varphi \in \mathrm{Gal}_F(L)$$

By Corollary 4.13, $a \in F$.

□

(End of Day 31)

4.4. (Galois' Theorem - Special Case): Let $k \subset L$ be a finite normal extension such that $\mathrm{Gal}_k(L)$ is solvable. Assume that, for every prime $p \in \mathbb{N}$,

$$p \mid |\mathrm{Gal}_k(L)| \Rightarrow \zeta_p \in k$$

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

Proof. Let $G := \mathrm{Gal}_k(L)$, then we induct on $n := |G|$.

(i) If n is prime, then this is Kummer's theorem.

(ii) If n is not prime, then by Lemma 4.1, there is a normal series

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

such that $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is of prime order. In particular, if $H := G_1$, then

$$p := [G : H]$$

is prime.

(iii) Let $F := L^H$, then we have a tower of extensions

$$k \subset F \subset L$$

Furthermore, since $H \lhd G, k \subset F$ is a normal extension by FTOG-II.

(iv) Since $p \mid |G|, \zeta_p \in k \subset F$ by hypothesis. Furthermore, since

$$G/H \cong \operatorname{Gal}_k(F) \Rightarrow |\operatorname{Gal}_k(F)| = p$$

Hence by Kummer's theorem, $k \subset F$ is a simple radical extension of prime type.

(v) Now note that

$$F \subset L$$

is a normal extension by HW 6.3. Furthermore,

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

and so $\operatorname{Gal}_F(L)$ is solvable by Theorem 2.3. Also,

$$|\operatorname{Gal}_F(L)| = |H| = \frac{|G|}{[G:H]} = \frac{n}{p}$$

Finally, for every prime $q \mid |\operatorname{Gal}_F(L)|$,

$$q \mid |\operatorname{Gal}_k(L)|$$

and so $\zeta_q \in k \subset F$. Hence, the extension $F \subset L$ satisfies the hypothesis of the theorem, so by induction, $F \subset L$ is a radical extension.

(vi) By (iii) and (iv), $k \subset L$ is a radical extension.

□

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

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

(ii) The map

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

is a well-defined injective homomorphism.

Proof. (i) If $\varphi : L(\beta) \to \mathbb{C}$ is a $k(\beta)$-homomorphism, then restriction gives

$$\varphi|_L : L \to \mathbb{C}$$

is a k-homomorphism. Since $k \subset L$ is normal,

$$\varphi(L) = L$$

Since $\beta \in k(\beta)$, $\varphi(\beta) = \beta \in L(\beta)$. Since

$$L(\beta) = \operatorname{span}_L(1, \beta, \ldots, \beta^{n-1}) \qquad (*)$$

we have that $\varphi(L(\beta)) = L(\beta)$ as required.

(ii) Let μ be the map defined in (ii). Then, μ is well-defined since $k \subset L$ is normal (as in part (i)), and is clearly a group homomorphism. Now suppose $\varphi \in \mathrm{Gal}_{k(\beta)} L(\beta)$ is such that

$$\mu(\varphi) = \mathrm{id}_L$$

Then, note that $\varphi(\beta) = \beta$ since $\varphi|_{k(\beta)} = \mathrm{id}_{k(\beta)}$, and so by the description of $L(\beta)$ in $(*)$, we have that

$$\varphi = \mathrm{id}_{L(\beta)}$$

and hence μ is injective.

□

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.

Proof. Let $G := \mathrm{Gal}_k(L), n := |G|$, then consider $\beta := e^{2\pi i/n}$, then β is algebraic over k since $\mathbb{Q} \subset k$. Consider the field extension

$$k(\beta) \subset L(\beta)$$

and let $\widehat{G} := \mathrm{Gal}_{k(\beta)} L(\beta)$, then by Theorem 4.5, $k(\beta) \subset L(\beta)$ is a finite normal extension, and there is an injective homomorphism

$$\widehat{G} \hookrightarrow G$$

Hence, by Theorem 2.3, $\widehat{G}$ is solvable. Furthermore, if $p \in N$ is prime, then

$$p \mid |\widehat{G}| \Rightarrow p \mid |G| \Rightarrow \zeta_p = \beta^{n/p} \in k(\beta)$$

Hence, by Theorem 4.4,

$$k(\beta) \subset L(\beta)$$

is a radical extension. However,

$$k \subset k(\beta)$$

is clearly a simple radical extension. Hence,

$$k \subset L(\beta) =: M$$

is a radical extension □

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.

Proof. Corollary 2.12, and Theorem 4.6 (with L being the splitting field of f) □

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

Proof. By Theorem III.3.5, $\mathrm{Gal}_k(f)$ is isomorphic to a subgroup of S_4. S_4 is solvable by Example 2.2(iv), and so $\mathrm{Gal}_k(f)$ is solvable by Theorem 2.3. Hence, f is solvable by radicals by Theorem 4.6. □

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

Proof. Theorem 4.6 + Example 2.2(i). □

V. Galois Groups of Polynomials

1. Cyclotomic Polynomials

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

(i) $\zeta_n := e^{2\pi i/n}$

(ii) $\mu_n = \{e^{2\pi ik/n} : 0 \leq k \leq n-1\} = \langle \zeta_n \rangle$

Note: μ_n is a cyclic group of order n.

(iii) Elements of μ_n are called roots of unity.

(iv) Generators of μ_n are called primitive root of unity. The set of primitive n^{th} roots of unity is denoted by Λ_n. Hence,

$$\Lambda_n = \{\zeta \in \mu_n : o(\zeta) = n\}$$

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

(vi) 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.

Proof. (i) Since $k(\mu_n) = k(\zeta_n)$, this follows from Corollary III.5.9.

(ii) If $\varphi \in G := \text{Gal}_k(\mu_n)$, then for any $\alpha \in \mu_n$,

$$\varphi(\alpha) \in \mu_n$$

by Lemma II.1.2. Hence, we obtain a map

$$\widehat{\varphi} := \varphi|_{\mu_n} : \mu_n \to \mu_n$$

Since φ is injective, so $\widehat{\varphi}$, and hence, $\widehat{\varphi}$ is also surjective. It is clearly a group homomorphism since φ is a ring homomorphism. Hence, the map Γ is well-defined.

(iii) Furthermore, Γ is injective, because if $\varphi \in G$, then φ is completely determined by $\varphi(\zeta_n) = \widehat{\varphi}(\zeta_n)$. Hence, if $\varphi, \psi \in G$ such that

$$\widehat{\varphi} = \widehat{\psi}$$

Then $\varphi(\zeta_n) = \psi(\zeta_n)$ and so $\varphi = \psi$ (as in Example III.1.8(vii))

□

(End of Day 32)

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, call 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: $\text{Aut}(\mu_n) \cong \mathbb{Z}_n^*$

Proof. If $a \in \mathbb{Z}$ such that $(a,n) = 1$, define

$$\psi_a : \mu_n \to \mu_n \text{ given by } \zeta \mapsto \zeta^a$$

(i) Then, ψ_a is a well-defined homomorphism.

(ii) ψ_a is injective, because $\exists k, \ell \in \mathbb{Z}$ such that

$$ka + \ell n = 1$$

And so if $\lambda, \zeta \in \mu_n$ such that
$$\zeta^a = \lambda^a$$
Then (since $\zeta^n = \lambda^n = 1$), it follows that

$$\zeta = \lambda$$

(iii) Since ψ_a is injective and μ_n is finite, it is also surjective, and hence is an isomorphism.

(iv) Now note that if $\overline{a} = \overline{b}$ in $\mathbb{Z}_n^*$, then $\exists k \in \mathbb{Z}$ such that

$$a = b + kn$$

and so
$$\zeta^a = \zeta^b \quad \forall \zeta \in \mu_n \Rightarrow \psi_a = \psi_b$$

Hence the map
$$\Delta : \overline{a} \to \psi_a \text{ from } \mathbb{Z}_n^* \to \text{Aut}(\mu_n)$$

is well-defined.

(v) Δ is injective: If $\overline{a}, \overline{b} \in \mathbb{Z}_n^*$ such that $\psi_a = \psi_b$, then

$$e^{2\pi i a/n} = e^{2\pi i b/n}$$

and so $\exists k \in \mathbb{N}$ such that

$$\frac{a-b}{n} = k \Rightarrow \overline{a} = \overline{b}$$

and hence Δ is injective.

(vi) Δ is surjective: If $f \in \text{Aut}(\mu_n)$, then $\exists a \in \mathbb{Z}$ such that

$$f(\zeta_n) = \zeta_n^a$$

Similarly, if $g = f^{-1}$, then $\exists b \in \mathbb{Z}$ such that

$$g(\zeta_n) = \zeta_n^b$$

Composing, we see that

$$\zeta_n^{ab} = \zeta_n \Rightarrow \exists k \in \mathbb{Z} \text{ such that } \frac{ab-1}{n} = k$$

Hence, $(a, n) = 1$ and so $\overline{a} \in \mathbb{Z}_n^*$ and $f = \psi_a$ as required.

□

1.5. Corollary: Let $n \in \mathbb{N}$

(i) If $(a, n) = 1$, and $\zeta \in \Lambda_n$, then $\zeta^a \in \Lambda_n$.

(ii)

$$\Lambda_n = \{e^{2\pi i a/n} : a \in \mathbb{Z} \text{ such that } (a, n) = 1\}$$

Proof. HW □

1.6. Definition: The n^{th} Cyclotomic polynomial is defined as

$$\Phi_n(x) = \prod_{\zeta \in \Lambda_n} (x - \zeta) = \prod_{0 \leq a \leq n, (a,n)=1} (x - e^{2\pi i a/n})$$

Note that

$$\deg(\Phi_n) = |\mathbb{Z}_n^*| = \varphi(n)$$

where φ denotes the Euler-Phi function.

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

Proof. If $d \mid n$ and $\zeta \in \mathbb{C}$ is a primitive d^{th} root of unity, then

$$\zeta^d = 1 \Rightarrow \zeta^n = 1$$

Hence,

$$\cup_{d|n} \Lambda_d \subset \mu_n \qquad (*)$$

Conversely, if $\zeta \in \mu_n$, then let $d := o(\zeta)$ as an element of μ_n. Then

$$d \mid |\mu_n| = n$$

and clearly, $\zeta \in \Lambda_d$. Hence, equality holds in $(*)$, and the theorem follows. □

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) $\Phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$

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

(v) $\Phi_8(x) = \frac{x^8-1}{(x-1)(x+1)(x^2+1)} = x^4 + 1$ (See Quiz 2, Question 2)

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

Proof. We induct on n

(i) If $n = 1$, then it is clearly true.

(ii) If $n > 1$, then assume the result is true for $m < n$. Then consider

$$f(x) := \prod_{d|n, d<n} \Phi_d(x)$$

Then $f \in \mathbb{Z}[x]$, and is monic by induction, and by Lemma 1.8,

$$x^n - 1 = f(x)\Phi_n(x) \text{ in } \mathbb{C}[x] \qquad (*)$$

This implies that Φ_n is monic, so write

$\Phi_n(x) = a_0+a_1x+\ldots+a_{m-1}x^{m-1}+x^m$ and $f(x) = b_0+b_1x+\ldots+b_{k-1}x^{k-1}+x^k$

where $m + k = n$. Note that, by induction, we may assume that $b_0 = \pm 1$.

(iii) Note that

$$a_0 b_0 = -1 \text{ and } b_0 = \pm 1 \Rightarrow a_0 \in \mathbb{Z}$$

(iv) So to prove $a_j \in \mathbb{Z}$, we assume by induction that $a_i \in \mathbb{Z}$ for all $0 \leq i < j$. Since $j \leq k - 1$, the coefficient of x^{j+k} is given by

$$a_0 b_{j+k} + a_1 b_{j+k-1} + \ldots + a_{j-1} b_{k+1} + a_j = 0$$

By hypothesis, every other term in the sum is in $\mathbb{Z}$, and so $a_j \in \mathbb{Z}$ as well, since $\mathbb{Z}$ is a ring.

□

(End of Day 33)

1.10. Recall: Let k be any field, $f \in k[x]$, then

(i) Write

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

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

$$D(f)(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$$

Then note that $D(f) \in k[x]$ as well.

(ii) Leibnitz' rule holds here as well: If $f(x) = g(x)h(x)$, then

$$D(f)(x) = D(g)(x)h(x) + g(x)D(h)(x)$$

1.11. Lemma: Let $p \in \mathbb{N}$ prime and $n \in \mathbb{N}$ such that $p \nmid n$.

(i) If $f(x) = x^n - 1$, then

$$(f, D(f)) = 1 \text{ in } \mathbb{Z}_p[x]$$

(ii) If $g(x) \in \mathbb{Z}_p[x]$ such that

$$g^2(x) \mid f(x) \text{ in } \mathbb{Z}_p[x]$$

then $g(x) \in \mathbb{Z}_p$ is a scalar.

Proof. (i) Note that

$$D(f)(x) = nx^{n-1} \neq 0 \text{ since } p \nmid n$$

and $x \in \mathbb{Z}_p[x]$ is irreducible because

$$\mathbb{Z}_p[x]/(x) \cong \mathbb{Z}_p \text{ is a field}$$

Hence, if $h = (f, D(f))$, then $\exists k \in \mathbb{N}$ such that

$$h(x) = x^k$$

Since $h \mid f$, $k \leq n$, and so

$$h \mid (x^n, x^n - 1) \Rightarrow h \mid -1 \Rightarrow \deg(h) = 0$$

and hence $h = 1$

(ii) If $g \in \mathbb{Z}_p[x]$ such that $g^2 \mid f$, then by Leibnitz' rule [Check!],

$$g \mid D(f)$$

and so by part (i), $g \in \mathbb{Z}_p$ is scalar.

□

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

Proof. (i) If $a, b \in \mathbb{Z}_p$, we have

$$\begin{aligned}(a+b)^p &= a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \\ &= a^p + b^p\end{aligned}$$

by HW 3.1(b).

(ii) Furthermore, by Fermat's theorem, for all $a \in \mathbb{Z}_p$, we have

$$a^p = a \pmod p$$

(iii) Now write

$$\begin{aligned} g(x) &= a_0 + a_1 x + \ldots + a_n x^n \\ \Rightarrow g(x)^p &= (a_0 + a_1 x + \ldots + a_n x^n)^p \\ &= a_0^p + a_1^p x^p + \ldots + a_n^p x^{np} \\ &= a_0 + a_1 x^p + \ldots + a_n x^{np} \\ &= g(x^p) \end{aligned}$$

□

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 $\mathbb{Q}$

Proof. (i) Assume first that $p = a$ is prime, so that $p \nmid n$.

(a) Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of ζ, then

$$f(x) \mid (x^n - 1) \text{ in } \mathbb{Q}[x]$$

By Gauss' lemma, it follows [Check!] that $f(x) \in \mathbb{Z}[x]$. Similarly, if $g(x) \in \mathbb{Q}[x]$ is the minimal polynomial of ζ^p, then $g(x) \in \mathbb{Z}[x]$. We now assume that

$$f(x) \neq g(x)$$

(b) Then

$$g(\zeta^p) = 0$$

and so $f(x) \mid g(x^p)$ in $\mathbb{Q}[x]$ and hence $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$ by HW 3.4. So let $h(x) \in \mathbb{Z}[x]$ such that

$$g(x^p) = f(x)h(x)$$

(c) Let $\overline{f}(x) \in \mathbb{Z}_p[x]$ denote the image of f under the quotient map

$$\pi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

Then applying π to the above equation, we obtain, by Lemma 1.12, that

$$\overline{g}^p = \overline{fh} \qquad (*)$$

(d) Now note that $f(x) \mid (x^n - 1)$ in $\mathbb{Q}[x]$, and also $g(x) \mid (x^n - 1)$ in $\mathbb{Q}[x]$. Since f and g are irreducible, and $f \neq g$, it follows that

$$f(x)g(x) \mid (x^n - 1) \text{ in } \mathbb{Q}[x]$$

Once again, by Gauss' lemma, $f(x)g(x) \mid (x^n - 1)$ in $\mathbb{Z}[x]$, so $\exists t(x) \in \mathbb{Z}[x]$ such that

$$f(x)g(x)t(x) = (x^n - 1)$$

Applying π to this equation, we get

$$\overline{f}\overline{g}\overline{t} = \overline{x^n - 1} \qquad (**)$$

(e) From $(**)$, we see that

$$\overline{f}^p\overline{g}^p\overline{t}^p = \overline{x^n - 1}^p$$

By Lemma 1.12 and $(*)$, this implies

$$\overline{f}^{p+1}\overline{h}\overline{t}^p = \overline{x^{np} - 1}$$

In particular,

$$\overline{f}^2 \mid \overline{x^{np} - 1}$$

By Lemma 1.11, $\deg(\overline{f}) = 0$. But since f is monic, this implies that

$$\deg(f) = 0$$

which contradicts the assumption that f is irreducible in $\mathbb{Q}[x]$.

(ii) Now suppose $a \in \mathbb{Z}$ is any number such that $(a, n) = 1$, then write

$$a = p_1p_2\ldots p_k$$

with $p_i \in \mathbb{N}$ prime. Now fix $\zeta \in \Lambda_n$, then by part (i),

$$\zeta^{p_1} \in \Lambda_n$$

Replacing ζ by ζ^{p_1} in part (i), we see that

$$\zeta^{p_1p_2} \in \Lambda_n$$

Hence, by induction on k, we finally obtain $\zeta^a \in \Lambda_n$ as well.

□

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

Proof. Let $f \in \mathbb{Q}[x]$ denote the minimal polynomial of ζ, then since $\Phi_n(\zeta) = 0$, it follows that

$$f(x) \mid \Phi_n(x) \text{ in } \mathbb{Q}[x]$$

By Lemma 1.13 and Corollary 1.5, f is the minimal polynomial for all elements of Λ_n. Hence,

$$\deg(f) \geq |\Lambda_n| = \varphi(n) = \deg(\Phi_n)$$

Hence, $\deg(f) = \deg(\Phi_n)$, and since both are monic, it follows that $f = \Phi_n$. □

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

Proof. By Theorem 1.2, the map

$$\Gamma : \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\mu_n)) \to \mathrm{Aut}(\mu_n) \cong \mathbb{Z}_n^*$$

is injective. However, by Corollary 1.14,

$$|\,\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\mu_n))| = [\mathbb{Q}(\mu_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n) = |\mathbb{Z}_n^*|$$

and so Γ is surjective as well. □

(End of Day 34)

1.16. Examples:

(i) If n is prime, this is simply Example III.1.8(vii).

(ii) $\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$, so

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_6)) \cong \mathbb{Z}_2$$

and $\zeta_6 = e^{\pi i/3}$

(iii) $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. However,

$$\overline{3}^2 = \overline{9} = \overline{1}$$

and similarly, every element of $\mathbb{Z}_8^*$ has order 2. Hence,

$$\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Also, by Example 1.8,

$$\Phi_8(x) = x^4 + 1$$

and $\zeta_8 = e^{\pi i/4}$. Hence,

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_8)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Compare this with Question 2 on Quiz 2.

1.17. 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 $k \subset \mathbb{C}$ be a field, $f \in k[x]$ 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 6.5)

(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 call the discriminant 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 $D_f = -4a^3 - 27b^2$

Proof. Note that

$$x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

and hence

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= a \\ \alpha_1\alpha_2\alpha_3 &= -b \end{aligned}$$

□

Now compute both

$$-4a^3 - 27b^2 \text{ and } [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2$$

and check that they are equal.

(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 reduced if $a_{n-1} = 0$

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

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

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

(i) For any $\varphi \in G \subset S_n$,

$$\varphi(\Delta) = \mathrm{sgn}(\varphi)\Delta$$

(ii) $D_f \in k$

Proof. (i) Consider $G = \mathrm{Gal}_k(f) < S_n$ as in Theorem III.3.5. Then for any $\varphi \in G$, we may write φ as a product of transpositions. Hence, it suffices to show the theorem if $\varphi \in S_n$ is a transposition. In this case, it is clear that

$$\varphi(\Delta) = -\Delta$$

(ii) Now that, by part (i),

$$\varphi(D_f) = D_f \quad \forall \varphi \in G$$

Now apply Corollary III.4.13

□

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

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

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

Proof. Note that (ii) follows from (i) by the Galois correspondence. So let

$$F = k(\Delta)$$

Then, for all $\varphi \in G$,

$$\begin{aligned} \varphi \in G \cap A_n &\Leftrightarrow \varphi \in G \text{ and } \mathrm{sgn}(\varphi) = 1 \\ &\Leftrightarrow \varphi \in G \text{ and } \varphi(\Delta) = \Delta \\ &\Leftrightarrow \varphi \in G \text{ and } \varphi|_F = \mathrm{id}_F \\ &\Leftrightarrow \varphi \in \mathrm{Gal}_F(L) \end{aligned}$$

□

2.7. Theorem: Let $f \in k[x]$ be an irreducible cubic with Galois group G and discriminant D_f

$$G \cong \begin{cases} \mathbb{Z}_3 & : \sqrt{D_f} \in k \\ S_3 & : \sqrt{D_f} \notin k \end{cases}$$

Proof. By Remark 2.1, $G \cong A_3$ or S_3. Note that

$$\begin{aligned} G \cong A_3 &\Leftrightarrow G \subset A_3 \\ &\Leftrightarrow G \cap A_3 = G \\ &\Leftrightarrow k(\Delta) = L^G \\ &\Leftrightarrow k(\Delta) = k \\ &\Leftrightarrow \Delta \in k \\ &\Leftrightarrow \sqrt{D_f} \in k \end{aligned}$$

□

(End of Day 35)

2.8. Examples:

(i) $f(x) = x^3 - 2$, then $D_f = -108$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$, as we know.

(ii) $f(x) = x^3 - 3x + 1$, then $D_f = 81$, so $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_3$.

(iii) $f(x) = x^3 - 4x + 2$, 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.3.10)

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

Proof. Let $F := k(u, \sqrt{D_f})$, and L denote the splitting field of f over k. Then

(i) $u \in L$, and

$$\Delta = \sqrt{D_f} = (u - v)(u - w)(v - w) \in L$$

and hence, $F \subset L$

(ii) Conversely, since $u \in F$, we write

$$f(x) = (x - u)g(x)$$

for some $g \in F[x]$. Note that $\{v, w\}$ are the roots of g, so

$$g(x) = (x - v)(x - w) \text{ in } \mathbb{C}[x]$$

In particular, since $u \in F$,

$$g(u) = (u - v)(u - w) \in F$$

Since f is separable, $g(u) \neq 0$, so

$$(v - w) = \frac{\sqrt{D_f}}{g(u)} \in F$$

On the other hand, $v + w$ is a coefficient of g, and so

$$v + w \in F$$

Hence $v, w \in F$ and so f splits in F. Hence, $L \subset F$ as well.

□

2.10. Lemma: Let $k \subset \mathbb{C}$ be a field, $a \in k$ and $p \in \mathbb{N}$ prime. Set

$$f(x) = x^p - a$$

Then f is irreducible in $k[x]$ iff f does not have a root in k.

Proof. $\Rightarrow$: If f is irreducible in $k[x]$, it cannot have a root in k (by the remainder theorem).

$\Leftarrow$: Conversely, suppose f is reducible in k, WTS: f has a root in k. So write

$$f(x) = g(x)h(x)$$

for some polynomials $g, h \in k[x]$ with $\deg(g), \deg(h) < p$. Let L denote the splitting field of f over k, then g and h split in L. So write

$$g(x) = (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_k) \text{ in } L[x]$$

Hence,

$$\alpha := \prod_{i=1}^{k} \lambda_i \in k \qquad (*)$$

where $k = \deg(p)$. Now,

$$\alpha^p = \prod_{i=1}^{k} (\lambda_i)^p = \prod_{i=1}^{k} a = a^k$$

Note that $k = \deg(g) < p$ and p is prime, so $\exists s, t \in \mathbb{Z}$ such that

$$sk + tp = 1$$

Hence,

$$a = a^{sk+tp} = (a^k)^s (a^t)^p = (\alpha^p)^s (a^t)^p = (\alpha^s a^t)^p$$

Hence, if $\beta := \alpha^s a^t$, we have $\beta \in k$ by $(*)$ and

$$\beta^p = a$$

and hence f has a root in k.

□

2.11. (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.

Proof. Let $\{u, v, w\}$ denote the roots of f and D_f denote its discriminant. Since $\{u, v, w\} \subset \mathbb{R}$, we have $\Delta \in \mathbb{R}$, so

$$D_f = \Delta^2 > 0$$

Suppose $\mathbb{Q} \subset M$ is a radical extension in which f splits, then by Corollary 2.8,

$$L = \mathbb{Q}(u, \sqrt{D_f}) \subset M$$

Now suppose $M \subset \mathbb{R}$, we will obtain a contradiction.

(i) If $F = \mathbb{Q}(\sqrt{D_f})$, then

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

Since $\mathbb{Q} \subset M$ is radical, we have a tower of extensions

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \ldots \subset K_n = M$$

such that $K_i \subset K_{i+1}$ is simple radical. Hence, the tower

$$F \subset FK_1 \subset FK_2 \subset \ldots \subset FK_n = M$$

is a tower where $FK_i \subset FK_{i+1}$ is a simple radical extension. Hence,

$$F \subset M$$

is a radical extension.

(ii) By Lemma IV.2.10, there is a tower of extensions

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots F_n = M$$

such that $F_i \subset F_{i+1}$ is of prime type.

(iii) Now, note that $[F : \mathbb{Q}] \in \{1, 2\}$ (since $D_f \in \mathbb{Q}$, by Theorem 2.5) and f is a cubic, so f is irreducible in $F[x]$ [Why?]. Furthermore, f splits in M. Hence, $\exists 1 \leq j \leq n$ such that

- f is irreducible in $F_j[x]$
- f is not irreducible in $F_{j+1}[x]$

(iv) Now consider $F_j \subset F_{j+1}$. By hypothesis, $\exists p \in \mathbb{N}$ prime and $a \in F_j$ such that

$$F_{j+1} = F_j(\alpha) \text{ such that } \alpha^p = a$$

Let $g(x) := x^p - a \in F_j[x]$. By part (iii), $F_{j+1} \neq F_j$, and so $\alpha \notin F_j$. However, since g has only one real root, it follows that g does not have a root in F_j. Hence, by Lemma 2.10, g is irreducible in $F_j[x]$.

(v) Now note that f is not irreducible in $F_{j+1}[x]$. Since $\deg(f) = 3$, f has a root, say, $u \in F_{j+1}$. Since $\sqrt{D_f} \in F_0 \subset F_{j+1}$, it follows by Corollary 2.8, that f splits in F_{j+1}. Let L denote the splitting field of f over F_j, then $L = F_j(u)$, and by part (iii),

$$F_j \subset L \subset F_{j+1}$$

However, since $g \in F_j[x]$ is irreducible, monic, and $g(\alpha) = 0$, it follows that

$$[F_{j+1} : F_j] = [F_j(\alpha) : F_j] = \deg(m_{\alpha,F_j}) = \deg(g) = p$$

Hence, $F_j \subset F_{j+1}$ has no non-trivial intermediate extensions. Since $F_j \neq L$, it follows that

$$L = F_{j+1}$$

In particular, F_{j+1} is the splitting field of f over F_j. Hence, $F_j \subset F_{j+1}$ is a normal extension.

(vi) However, $g \in F_j[x]$ is irreducible and has a root in F_{j+1}. By Theorem III.2.8, g splits in F_{j+1}. In particular,

$$\alpha, e^{2\pi i/p}\alpha \in F_{j+1}$$

and hence $e^{2\pi i/p} \in F_{j+1} \subset M$. Hence, $M \not\subseteq \mathbb{R}$.

□

2.12. Examples: If $f(x) = x^3 - 3x + 1$, then all the roots of f are real (draw the graph using Calculus), so by Casus Irreducibilis, any radical extension in which f splits must necessarily contain non-real complex numbers.

(End of Day 36)

3. Quartic Polynomials

(See [Conrad])

Throughout this section, let $k \subset \mathbb{C}$ be a field, $f \in k[x]$ be an irreducible quartic polynomial with splitting field L and Galois group G

3.1. Remark:

(i) By HW 6.5, $4 \mid |G|$ 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

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

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

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

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

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

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

Proof. (i) Once again, for any $\varphi \in G$, note that

$$\begin{aligned} \varphi \in G \cap V_4 &\Rightarrow \varphi(u) = u, \varphi(v) = v, \varphi(w) = w \\ &\Rightarrow \varphi|_F = \text{id}_F \\ &\Rightarrow \varphi \in \text{Gal}_F(L) \end{aligned}$$
$$\Rightarrow G \cap V_4 \subset \text{Gal}_F(L)$$

Conversely, if $\varphi \in \text{Gal}_F(L)$, then consider the possible options for $\varphi \in S_4$

(a) φ is a transposition: Assume WLOF that $\varphi = (12)$ since the other cases are similar. Then $\varphi(v) \neq v$ because

$$\begin{aligned} \alpha_1\alpha_3 + \alpha_2\alpha_4 &= \alpha_2\alpha_3 + \alpha_1\alpha_4 \\ \Leftrightarrow (\alpha_1 - \alpha_2)\alpha_3 &= (\alpha_1 - \alpha_2)\alpha_4 \\ \Leftrightarrow \alpha_3 &= \alpha_4 \end{aligned}$$

which is impossible since f is separable.

(b) φ is a 3-cycle: Assume WLOG that $\varphi = (123)$, then once again it follows that $\varphi(v) \neq v$

(c) φ is a product of disjoint 2 cycles: Here $\varphi \in V_4$, so there is nothing to check.

(d) φ is a 4-cycle: Assume WLOG that $\varphi = (1234)$, then once again it is clear that $\varphi(w) \neq w$.

Hence, it follows that if $\varphi \in \text{Gal}_F(L)$, then $\varphi \in V_4$, and this completes the proof.

(ii) Follows from (i) by FTOG-I.

(iii) Note that, by Remark 3.1,

$$\begin{aligned} G = V_4 &\Leftrightarrow G \subset V_4 \\ &\Leftrightarrow G \cap V_4 = G \\ &\Leftrightarrow L^{G \cap V_4} = L^G \\ &\Leftrightarrow F = k \end{aligned}$$

□

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 call the <u>resolvent cubic</u> of f.

Proof. Let g as above. If $\varphi \in G$, then consider the induced map

$$\varphi_* : L[x] \to \mathbb{C}[x] \text{ given by } \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \varphi(a_i) x^i$$

Then

$$\varphi_*(g)(x) = (x - \varphi(u))(x - \varphi(v))(x - \varphi(w))$$

But note that $\varphi|_{\{u,v,w\}}\colon \{u, v, w\} \to \{u, v, w\}$ is a permutation. Hence,

$$\varphi_*(g)(x) = g(x)$$

and so every coefficients of g satisfies Corollary III.4.13, and is therefore in k. Hence, $g \in k[x]$. □

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

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

Proof. Write

$$x^4 + ax^3 + bx^2 + cx + d = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \qquad (**)$$

and expand it out to obtain equations relating α_j's and the coefficients of x. Now compute each coefficients on the RHS of $(*)$. For instance, by $(**)$

$$\begin{aligned} b &= \text{coeff of } x^2 \\ &= (\alpha_1\alpha_2 + \alpha_3\alpha_4) + (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ &= \alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_4 + \alpha_2\alpha_3 \\ &= u + v + w \end{aligned}$$

and hence the coefficient of x^2 in $g(x)$ must be $-b$. (See [Conrad] for further details) □

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

(i) $D_f = D_g$

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

Proof. (i) Check that

$$u - v = \alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$

and similar calculations will show that

$$(u-v)(v-w)(u-w) = \prod_{i<j}(\alpha_i - \alpha_j)$$

and hence $D_g = D_f$ by squaring.

(ii) Note that g is separable by part (i), and hence Corollary V.2.8 applies.

□

(End of Day 37)

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 $\mathbb{Z}_4$

Proof. We have the following cases:

(i) $\sqrt{D_f} \in k$ and g is irreducible over k: Then,

$$G \subset A_4 \Rightarrow G = V_4 \text{ or } A_4$$

Since g is irreducible over k,

$$[k(u) : k] = 3$$

But $k(u) \subset L$, and so $3 \mid [L : k] = |G|$. Since $3 \nmid |V_4|$, we have

$$G = A_4$$

(ii) $\sqrt{D_f} \in k$ and g is not irreducible over k: Then,

$$G \subset A_4 \Rightarrow G = V_4 \text{ or } A_4$$

Now since g is reducible over k, and it is cubic, it has a root $u \in k$ (HW 2.3). But since $\sqrt{D_f} \in k$, it follows that

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

by Lemma 3.5. Hence, $G = V_4$ by Lemma 3.2.

(iii) $\sqrt{D_f} \notin k$ and g is irreducible over k: Then

$$G \cong \mathbb{Z}_4, D_4 \text{ or } S_4$$

But g is irreducible, so once again (as above), $3 \mid |G|$. Hence, $G \cong S_4$

(iv) $\sqrt{D_f} \notin k$ and g is not irreducible over k: Then by Lemma 3.5,

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

Since $D_f \in k$,

$$[k(u,v,w) : k] = 2$$

By Lemma 3.2 and FTOG-I, $[G : G \cap V_4] = 2$. But by Remark 3.1,

$$G \cong \mathbb{Z}_4, D_4 \text{ or } S_4$$

Since

$$[S_4 : S_4 \cap V_4] = [S_4 : V_4] = \frac{24}{4} = 6$$

it follows that $G \neq S_4$, and hence $G \cong \mathbb{Z}_4$ or D_4. Note that in both these cases

$$[G : G \cap V_4] = 2$$

□

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.5.6)

(b) The resolvent cubic of f is $g(x) = x^3 + 4x - 1$ (by Lemma 3.4)

(c) g has no roots in $\mathbb{Q}$ (by the rational root theorem), so it is irreducible (by HW 2.3)

(d) The discriminant of f is $D_f = D_g = -283$ (by Example 2.3(ii)), 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 has no roots in $\mathbb{Q}$ (by the rational root theorem) and it cannot be factor into two quadratic factors in $\mathbb{Z}[x]$ (Check!). So f cannot be properly factored in $\mathbb{Z}[x]$, and so f is irreducible in $\mathbb{Q}[x]$ by Gauss Lemma.

(b) The resolvent cubic of f is $g(x) = x^3 - 48x - 64$ (by Lemma 3.4)

(c) g is irreducible in $\mathbb{Q}[x]$ since it is irreducible in $\mathbb{Z}_5[x]$ (using I.5.6)

(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 by HW 3.2.

(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 Example 1.16(iii)]

3.8. Theorem: Let $f \in k[x]$ be an irreducible quartic such that Case IV applies in Theorem 3.6. Then $G \cong D_4$ iff f is irreducible over $k(\sqrt{D_f})$ (and $G \cong \mathbb{Z}_4$ otherwise).

Proof. Since we are in Case IV, $G \cong D_4$ or $\mathbb{Z}_4$.

$\Rightarrow$: Assume f is irreducible over $F := k(\sqrt{D_f})$. Since Case IV applies, $\sqrt{D_f} \notin k$, and so

$$[F : k] = 2$$

Hence, if α is any root of f, then

$$[F(\alpha) : F] = \deg(f) = 4$$

and so by the Tower Law

$$[F(\alpha) : k] = 8$$

Since $\sqrt{D_f}, \alpha \in L$, it follows that $[L : k] \geq 8$, and so

$$|G| \geq 8 \Rightarrow G \cong D_4$$

$\Leftarrow$: Assume $G \cong D_4$, then by Corollary 2.6,

$$\mathrm{Gal}_F(L) = G \cap A_4$$

But $D_4 \cap A_4 = V_4$ (Check!), and so $\mathrm{Gal}_F(L)$ acts transitively on the set $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of roots of f. By Theorem III.3.9, it follows that f is irreducible in $F[x]$.

□

(End of Day 38)

3.9. Theorem: If $f \in \mathbb{Q}[x]$ be an irreducible quartic with Galois group $\mathbb{Z}_4$, then $D_f > 0$. In particular, if Case IV applies in Theorem 3.6 and $D_f < 0$, then $G \cong D_4$

Proof. Suppose $G \cong \mathbb{Z}_4$, then $|G| = [L : k] = 4$, and so if $\alpha = \alpha_1$ is any root of f, then

$$L = \mathbb{Q}(\alpha)$$

(i) Suppose f has a real root, then we may choose $\alpha \in \mathbb{R}$, so $L \subset \mathbb{R}$, and so

$$\alpha_1, \alpha_2, \alpha_2, \alpha_3 \subset \mathbb{R} \Rightarrow \Delta \in \mathbb{R} \Rightarrow D_f > 0$$

(ii) Now suppose f does not have a real root, then the non-real roots must occur in conjugate pairs $\{z, \overline{z}, w, \overline{w}\}$, and so

$$\begin{aligned}\Delta &= (z-\overline{z})(z-w)(z-\overline{w})(\overline{z}-w)(\overline{z}-\overline{w})(w-\overline{w})\\ &= (z-\overline{z})(w-\overline{w})|z-w|^2|z-\overline{w}|^2\\ &= (2i\mathrm{Im}(z))(2i\mathrm{Im}(w))|z-w|^2|z-\overline{w}|^2 \in \mathbb{R}\end{aligned}$$

Hence, $D_f = \Delta^2 > 0$

□

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 3.9,

$$G \cong D_4$$

(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 39)

Review of all the chapters

(End of Day 40)

Discussion of HW and Quiz/Mid-Sem problems

(End of Day 41)

VI. Instructor Notes

0.1. The goals of the course were exactly as it was two years ago, and the execution was very similar. All in all, the plan is solid, although I would like to make two changes the next time aroung.

0.2. I feel that Chapter V could be moved up before Chapter IV, thereby giving an immediate application of the Fundamental theorems of Galois theory, while also setting up the discussion of solvable groups by talking about cyclotomic extensions in some detail (instead of the adhoc discussion in Section III.5)

0.3. Also, I would like to discuss finite fields and their Galois groups, at least perfunctorily. At the moment, not discussing finite fields is the major drawback of this structure.

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*, https://www.math.washington.edu/~greenber/MATH404-PrimElem.pdf

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

[Online Notes] http://www.uio.no/studier/emner/matnat/math/MAT2200/v13/obliglosning.pdf

[Conrad] K. Conrad, *Expository notes*, http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf