MATH 4108: Abstract Algebra II

Frank Qiang
Instructor: Jennifer Hom

Georgia Institute of Technology
Spring 2024

Contents

Lecture 1

Jan. 8 — Rings and Fields

1.1 Lots of Definitions

Recall the definitions of a ring and a field:

Definition 1.1 (Ring)**.** A *ring* $R = (R, +, \cdot)$ is a non-empty set R together with two binary operations $+$ and $\cdot$, called addition and multiplication respectively, which satisfy:

(R1) *Associative law for addition*: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(R2) *Commutative law for addition*: $a + b = b + a$ for all $a, b \in R$.

(R3) *Existence of zero*: There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

(R4) *Existence of additive inverses*: For all $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.[1]

(R5) *Associative law for multiplication*: $(ab)c = a(bc)$ for all $a, b, c \in R$.

(R6) *Distributive laws*: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

Definition 1.2 (Commutative ring)**.** In this class, we will mostly be interested in *commutative rings*, which satisfy the following additional property for multiplication:

(R7) *Commutative law for multiplication*: $ab = ba$ for all $a, b \in R$.

Definition 1.3 (Ring with unity)**.** A ring *with unity* satisfies the additional property that

(R8) *Existence of unity*: There exists $1 \neq 0 \in R$ such that and $a1 = 1a = a$ for $a \in R$.

Note that a ring need not be commutative to have a unity.

Definition 1.4 (Domain)**.** A commutative ring with unity is called a *(integral) domain* if it has the following cancellation property:

(R9) *Cancellation*: For all $a, b \in R$ and $c \neq 0$, $ca = cb$ implies $a = b$.

(R9') *No zero divisors*: For all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

The conditions (R9) and (R9') are equivalent.

Definition 1.5 (Field)**.** A commutative ring with unity is called a *field* if it has the following additional property for multiplicative inverses:

(R10) *Existence of multiplicative inverses*: For all $a \neq 0 \in R$, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

[1] Note that we'll usually write $a - b$ in place of $a + (-b)$.

Example 1.5.1. Some examples of rings are $\mathbb{Z}/2\mathbb{Z}$, which also happens to be a field. The ring $\mathbb{Z}$ is a domain. The set $M_{2\times2}(\mathbb{R})$ is a non-commutative ring with unity, and has zero divisors. The ring $\mathbb{Q}$ is a field.[2] The real polynomials in a single variable $\mathbb{R}[x]$ form a ring, which is a domain but not a field. The complex numbers $\mathbb{C}$ and the real numbers $\mathbb{R}$ both form a field. The even integers $2\mathbb{Z}$ form a commutative ring without unity. In general, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity, and is a field if and only if n is prime (and has zero divisors otherwise, if n is composite).

Remark. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group. If $(K, +, \cdot)$ is a field, then $(K^*, \cdot)$ is an abelian group, where $K^* = K \setminus \{0\}$.

Definition 1.6 (Group of units)**.** Let R be a commutative ring with unity. The *group of units* of R is

$$U = \{u \in R \mid \text{there exists } v \in R \text{ such that } uv = 1\}.$$

Exercise 1.1. Show that U is in fact a group under multiplication.

Definition 1.7 (Associate)**.** If $a, b \in R$ such that $a = ub$ for some $u \in U$, then a and b are called *associates*, denoted by $a \sim b$.

Exercise 1.2. Show that $\sim$ is in fact an equivalence relation.

Example 1.7.1. The group of units of $\mathbb{Z}$ is $\{1, -1\}$. The group of units of a field K is $K^* = K \setminus \{0\}$.

Exercise 1.3. Let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Check the following:

1. R is a commutative ring with unity.
2. The group of units of R is $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}, |a^2 - 2b^2| = 1\}$.

Definition 1.8 (Divisor)**.** Let D be an integral domain, $a \in D \setminus \{0\}$, $b \in D$. Then a divides b, or a is a *divisor* or *factor* of b, denoted by $a|b$, if there exists $z \in D$ such that $az = b$. We write $a\nmid b$ if a does not divide b. We say that a is a *proper divisor* or that a *properly divides* b if z is not a unit.

Remark. Equivalent, a is a proper divisor of b if and only if $a|b$ and $b\nmid a$.

Definition 1.9 (Subring)**.** A *subring* U of a ring R is a non-empty subset of R with the property that for all $a, b \in R$, $a, b \in U$ implies $a + b \in U$ and $ab \in U$, and $a \in U$ implies $-a \in U$.

Remark. Equivalently, U is a subring of R if and only if $a, b \in U$ implies $a - b \in U$ and $ab \in U$.

Remark. We automatically have $0 \in U$ since we can pick any $a \in U$, and then $0 = a - a \in U$.

Definition 1.10 (Subfield)**.** A *subfield* of a field K is a subset E containing at least two elements such that $a, b \in E$ implies $a - b \in E$ and $a \in E, b \in E \setminus \{0\}$ implies $ab^{-1} \in E$. If E is a subfield and $E \neq K$, then we say E is a *proper* subfield.

Remark. As before, we can replace the last condition with the equivalent statement that $a, b \in E$ implies $ab \in E$ and $a \in E \setminus \{0\}$ implies $a^{-1} \in E$.

Definition 1.11 (Ideal)**.** An *ideal* of R is a non-empty subset I of R with the properties that $a, b \in I$ implies $a - b \in I$ and $a \in I, r \in R$ implies $ra \in I$.

Remark. All ideals are subrings, but the converse is not true in general.

Example 1.11.1. The integers $\mathbb{Z}$ form a subring of $\mathbb{R}$ but not an ideal.

[2] In fact, $\mathbb{Q}$ is somehow the smallest field containing $\mathbb{Z}$.

Remark. We trivially have that $\{0\}$ and R are both ideals of R. An ideal I is called *proper* if $\{0\} \subsetneq I \subsetneq R$.

Theorem 1.1. *Let $A = \{a_1, \ldots, a_n\}$ be a finite subset of a commutative ring R. Then the set*

$$Ra_1 + \cdots + Ra_n = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in R\}$$

is the smallest ideal of R containing A.

Proof. See Howie. Check this is indeed an ideal and is contained in any other ideal containing A. □

Definition 1.12 (Ideals generated by elements of a ring)**.** The set $Ra_1 + \cdots + Ra_n$ is the *ideal generated by* $a_1, \ldots, a_n$, denoted by $\langle a_1, \ldots, a_n \rangle$. If the ideal is generated by a single element $a \in R$, then we say that $Ra = \langle a \rangle$ is a *principal ideal*.

Example 1.12.1. In $\mathbb{Z}$, the ideal $\langle 2 \rangle = 2\mathbb{Z}$ are the even numbers. We have $\langle 2, 3 \rangle = \mathbb{Z}$, but $\langle 6, 8 \rangle = \langle 2 \rangle$.

Theorem 1.2. *Let D be an integral domain with group of units U and let $a, b \in D \setminus \{0\}$. Then*

1. *$\langle a \rangle \subseteq \langle b \rangle$ if and only if $b|a$,*
2. *$\langle a \rangle = \langle b \rangle$ if and only if $a \sim b$,*
3. *$\langle a \rangle = D$ if and only if $a \in U$.*

Proof. See Howie. □

Definition 1.13 (Homomorphism of rings)**.** A *homomorphism* from a ring R to a ring S is a mapping $\varphi : R \to S$ such that $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Example 1.13.1. The zero mapping $\varphi(a) = 0$ is always a homomorphism. The inclusion map $\iota : 2\mathbb{Z} \to \mathbb{Z}$ or $\iota : \mathbb{Z} \to \mathbb{Q}$ is a homomorphism.

Theorem 1.3. *Let R, S be rings and $\varphi : R \to S$ a homomorphism. Then*

1. *$\varphi(0_R) = 0_S$,*
2. *$\varphi(-r) = -\varphi(r)$ for all $r \in R$,*
3. *the image $\varphi(R)$ is a subring of S.*

Proof. See Howie. □

Definition 1.14 (Monomorphism)**.** Let $\varphi : R \to S$ be a homomorphism. If φ is injective, we say that φ is a *monomorphism* or an *embedding*.

Example 1.14.1. The inclusion map $\varphi : \mathbb{Z} \to \mathbb{R}$ given by $\varphi(n) = n$ is an embedding.

Lecture 2

Jan. 10 — Field of Fractions, Polynomials

2.1 Isomorphisms

Definition 2.1 (Isomorphism)**.** If a homomorphism $\varphi : R \to S$ is both one-to-one and onto, then φ is an *isomorphism* and we say R and S are *isomorphic*, denoted $R \cong S$.

Definition 2.2 (Automorphism)**.** An isomorphism $\varphi : R \to R$ is called an *automorphism*.

Example 2.2.1. For any ring R, the identity map $\varphi : R \to R$ with $\varphi = \mathrm{id}$ is an automorphism.

Exercise 2.1. The complex conjugation $\varphi : \mathbb{C} \to \mathbb{C}$ with $\varphi(z) = \overline{z}$ is an automorphism.

Definition 2.3 (Kernel)**.** Let $\varphi : R \to S$ be a homomorphism. The *kernel* of φ is

$$\ker \varphi = \phi^{-1}(0_S) = \{a \in R : \varphi(a) = 0_S\}.$$

Exercise 2.2. For any homomorphism φ, $\ker \varphi$ is an ideal.

Definition 2.4 (Residue class)**.** Let I be an ideal of a ring R and $a \in R$. The set

$$a + I = \{a + x \mid x \in I\}$$

is the *residue class* of a modulo I.

Exercise 2.3. The set R/I of residue classes modulo I forms a ring with respect to the operations

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I)(b + I) = ab + I.$$

Exercise 2.4. The map $\theta_I : R \to R/I$ with $\theta_I(a) = a + I$ is a surjective homomorphism onto R/I with kernel I. This map θ_I is called the *natural homomorphism* from R to R/I.

Example 2.4.1. Consider $\mathbb{Z}$ and $I = \langle n \rangle = n\mathbb{Z}$. Then $\theta_I : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $\theta_I(a) = a + \langle n \rangle$ is the natural homomorphism. There are n residue classes, which are

$$\langle n \rangle, \quad 1 + \langle n \rangle, \quad \ldots, \quad (n-1) + \langle n \rangle.$$

Theorem 2.1. *Let $n \in \mathbb{Z}_{>0}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Proof. See Howie. □

Remark. If $n = 0$, then $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.

Theorem 2.2. *Let $\varphi : R \to S$ be a surjective homomorphism with kernel K. Then there is an isomorphism $\alpha : R/K \to S$ such that the following diagram commutes (i.e. $\varphi = \alpha \circ \theta_K$):*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\theta_K"'] & S \\ R/K \arrow[ur, "\alpha"] & \end{tikzcd}$$

Proof. See Howie. But the general idea is to define $\alpha : R/K \to S$ by $\alpha(a+K) = \varphi(a)$. Then need to check that α is well-defined and an isomorphism. □

2.2 Field of Fractions

The motivating question is: How do we get from $\mathbb{Z}$ to $\mathbb{Q}$? Recall that

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\},$$

where $a/c = b/d$ if $ad = bc$. We add and multiply fractions by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

How do we do this more generally (construct a field out of an arbitrary integral domain)?

Definition 2.5 (Field of fractions of a domain)**.** Let D be an integral domain and

$$P = D \times (D \setminus \{0\}) = \{(a, b) \mid a, b \in D, b \neq 0.\}$$

Define an equivalence relation $\equiv$ on P by $(a, b) \equiv (a', b')$ if $ab' = a'b$. Then the *field of fractions* of D is

$$Q(D) = P/\equiv.$$

We denote the equivalence class $[a, b]$ by a/b, i.e. $a/b = c/d$ if $ad = bc$. We define addition and multiplication on $Q(D)$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Exercise 2.5. Do the following:

1. Check that $\equiv$ is an equivalence relation.
2. Check that these operations are well-defined.
3. Check that $Q(D)$ is a commutative ring with unity.
   - The zero element is $0/b$ for $b \neq 0$.
   - The unity element is a/a for $a \neq 0$.
   - The negative of a/b is $(-a)/b$ or equivalently $a/(-b)$.
   - The multiplicative inverse of a/b is b/a for $a, b \neq 0$.
4. Complete the previous exercise and check that $Q(D)$ is a field.

Exercise 2.6. The map $\varphi : D \to Q(D)$ defined by $\varphi(a) = a/1$ is a monomorphism. In particular, the field of fractions $Q(D)$ contains D as a subring and $Q(D)$ is the smallest field containing D, in the sense that if K is a field with the property that there exists a monomorphism $\theta : D \to K$, then there exists a monomorphism $\psi : Q(D) \to K$ such that the following diagram commutes:

$$\begin{tikzcd} D \arrow[r, "\theta"] \arrow[d, "\varphi"'] & K \\ Q(D) \arrow[ur, "\psi"] & \end{tikzcd}$$

2.3 The Characteristic of a Field

Note that for $a \in R$, we might write $a + a$ as $2a$ and $a + a + \cdots + a$ (n times) as na. Furthermore, $0a = 0_R$ and $(-n)a = n(-a)$ for $n \in \mathbb{Z}_{>0}$. Thus na has meaning for all $n \in \mathbb{Z}$.[1]

Exercise 2.7. For $a, b \in R$ and $m, n \in \mathbb{Z}$, we have $(ma)(nb) = (mn)(ab)$.

Definition 2.6 (Characteristic of a ring)**.** For an arbitrary ring R, there are two possibilities:

1. $m1_R$ for $m \in \mathbb{Z}$ are all distinct. In this case, we say that R has *characteristic* 0.
2. There exists $m, n \in \mathbb{N}$ such that $m1_R = (m + n)1_R$. In this case, we say that R has *characteristic* n, where n is the least positive n for which this property holds.

We denote the characteristic of R by $\operatorname{char} R$. If $\operatorname{char} R = n$, then $na = 0_R$ for all $a \in R$ since

$$na = (n1_R)a = 0a = 0.$$

Example 2.6.1. We have $\operatorname{char} \mathbb{Z}/n\mathbb{Z} = n$.

Theorem 2.3. *The characteristic of a field is either* 0 *or a prime.*

Proof. Let K be a field and suppose $\operatorname{char} K = n \neq 0$ and n is not prime. Then we can write $n = rs$ where $1 < r, s < n$. The minimal property of n implies that $r1_K \neq 0$ and $s1_K \neq 0$. But then

$$r1_K \cdot s1_K = rs1_K = n1_K = 0,$$

which is impossible since K is a field and thus has no zero divisors. □

Remark. Note the following:

1. If K is a field with $\operatorname{char} K = 0$, then K has a subring isomorphic to $\mathbb{Z}$, i.e. elements of the form $n1_K$ for $n \in \mathbb{Z}$, and K has a subfield isomorphic to $\mathbb{Q}$, i.e.

   $$P(K) = \{m1_K/n1_K \mid m, n \in \mathbb{Z}, n \neq 0\}.$$

   This is the *prime subfield* of K, and any subfield of K must contain $P(K)$.
2. If K is a field with $\operatorname{char} K = p$, then the prime subfield of K is

   $$P(K) = \{1_K, 2 \cdot 1_K, \ldots, (p-1) \cdot 1_K\},$$

   which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

[1]This is saying that any abelian group is naturally a *module* over the integers $\mathbb{Z}$.

Remark. In other words, every field of characteristic 0 is an *extension* of $\mathbb{Q}$ (contains $\mathbb{Q}$ as a subfield), and every field of characteristic p is an *extension* of $\mathbb{Z}/p\mathbb{Z}$ (contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield).

Remark. If $\operatorname{char} K = 0$, then writing $a/n1_K$ as a/n is fine. But if $\operatorname{char} K = p$, then a/n does not make sense when $p|n$ (since $p \cdot 1_K = 0$).

Theorem 2.4. *If K is a field with $\operatorname{char} K = p$, then for all $x, y \in K$, $(x+y)^p = x^p + y^p$.*

Proof. See Howie. Uses the binomial theorem. □

2.4 Polynomials

Let R be a ring, then we have the polynomial ring over R

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{N}\}.$$

If $f \in R[X]$, then it has *degree* n if the last nonzero element in the sequence $\{a_0, a_1, \dots\}$ is a_n, denoted $\partial f = n$. By convention, the zero polynomial has degree $-\infty$. The coefficient a_n is called the *leading coefficient*, and if $a_n = 1$, then f is *monic*. Addition and multiplication work as expected:

$$(a_0 + a_1X + \cdots + a_mX^m) + (b_0 + b_1X + \cdots + b_nX^n) = (a_0 + b_0) + (a_1 + b_1)X + \dots$$

and

$$(a_0 + a_1X + \cdots + a_mX^m)(b_0 + b_1X + \cdots + b_nX^n) = c_0 + c_1X + \dots$$

where

$$c_k = \sum_{i+j=k}^{k} a_ib_j.$$

The ground ring R sits inside of the polynomial ring $R[X]$. Take the monomorphism $\theta : R \to R[X]$ by $\theta(a) = a$, i.e. an element a maps to the constant polynomial a.

Theorem 2.5. *Let D be an integral domain. Then*

1. *$D[X]$ is an integral domain.*
2. *If $p, q \in D[X]$, then $\partial(p+q) \le \max(\partial p, \partial q)$.*
3. *If $p, q \in D[X]$, then $\partial(pq) = \partial p + \partial q$.*
4. *The group of units of $D[X]$ coincides with the group of units of D.*

Proof. Statements (2) and (3) are left as exercises.

(1) We need to show that $D[X]$ has no zero divisors. For this, suppose that p, q are nonzero polynomials with leading coefficients a_m and b_n respectively. Then the leading coefficient of pq is a_mb_n, which is nonzero since D is an integral domain and thus has no zero divisors. So pq is nonzero.

(4) Let $p, q \in D[X]$ and suppose $pq = 1$. Since $\partial(pq) = \partial(1) = 0$, we must have $\partial p = \partial q = 0$. Thus $p, q \in D$ and $pq = 1$ if and only if p and q are in the group of units of D. □

Since $D[X]$ is a domain, we can consider polynomials in the variable Y with coefficients in $D[X]$:

$$D[X, Y] = (D[X])[Y].$$

We can repeat this to get polynomials in n variables: $D[X_1, X_2, \dots, X_n]$, which is an integral domain.

Lecture 3

Jan. 17 — Irreducible Polynomials

3.1 Principal Ideal Domains and Irreducibile Polynomials

Definition 3.1. The field of fractions of $D[X]$ consists of *rational forms*

$$\frac{a_0 + a_1X + \cdots + a_mX^m}{b_0 + b_1X + \cdots + b_nX^n}$$

where $b_0 + b_1X + \cdots + b_nX^n \neq 0$, denoted by $D(X)$.

Definition 3.2. A domain D is a *principal ideal domain* (PID) if all of its ideals are principal.[1]

Example 3.2.1. The integers $\mathbb{Z}$ is a PID, since every ideal is of the form $\langle n \rangle$.

Definition 3.3. A non-zero, non-unit element p in a domain D is *irreducible* if it has no proper factors.

Definition 3.4. A domain D is a *unique factorization domain* (UFD) if every non-unit $a \neq 0$ in D has an essentially unique[2] factorization into irreducible elements.

Example 3.4.1. Again $\mathbb{Z}$ is a UFD, e.g. $12 = 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot (-3)$.

Theorem 3.1. *Every PID is a UFD.*

Proof. See Howie. $\square$

Theorem 3.2. *If K is a field, then $K[X]$ is a PID.*

Proof. See Howie. $\square$

Theorem 3.3. *Let p be an element in a PID D. Then the following are equivalent:*

1. *p is irreducible.*
2. *$\langle p \rangle$ is maximal.*
3. *$D/\langle p \rangle$ is a field.*

In particular if $f \in K[X]$, then $K[X]/\langle f \rangle$ is a field if and only if f is irreducible.

Proof. See Howie. $\square$

[1] Recall that a principal ideal is one generated by a single element.
[2] As in, unique up to use of associates or adding in units.

Definition 3.5. Let D be a domain and $\alpha \in D$. Let $\sigma_\alpha : D[X] \to D$ defined by

$$\sigma_\alpha(a_0 + a_1 X + \cdots + a_n X^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Note that we often write $\sigma_\alpha(f)$ as $f(\alpha)$. If $f(\alpha) = 0$, we say α is a *root* of f, or a *zero*.

Exercise 3.1. Check that σ_α is a homomorphism.

Theorem 3.4. *Let K be a field, $\beta \in K$ and f a non-zero polynomial in $K[X]$. Then β is a root of f if and only if $X - \beta | f$.*

Proof. See Howie. □

Example 3.5.1. We have $X^2 + 1$ in $\mathbb{R}[X]$ is irreducible, so $\mathbb{R}[X]/\langle X^2 + 1\rangle$ is a field. In fact this field is isomorphic to the complex numbers $\mathbb{C}$.

Exercise 3.2. Do the following:

1. Show that $\varphi : \mathbb{R}[X] \to \mathbb{C}$ given by

$$\varphi(a_0 + a_1 X + \cdots + a_n X^n) = a_0 + a_1 i + \cdots + a_n i^n$$

   is a surjective homomorphism.[3]

2. Show that $\ker\varphi = \langle X^2 + 1\rangle$.

So by the first isomorphism theorem we can conclude that $\mathbb{R}[X]/\langle X^2 + 1\rangle = \mathbb{R}/\ker\varphi \cong \varphi(\mathbb{R}[X]) = \mathbb{C}$.

Theorem 3.5. *Let K be a field and $g \in K[X]$ an irreducible polynomial. Then $K[X]/\langle g\rangle$ is a field containing K up to isomorphism.*

Proof. Since g is irreducible, $K[X]/\langle g\rangle$ is a field. Now define $\varphi : K \to K[X]/\langle g\rangle$ by

$$\varphi(a) = a + \langle g\rangle.$$

(Left as an exercise to check that φ is a homomorphism.) We need to show that φ is injective. For this, take $a, b \in K$. If $a + \langle g\rangle = b + \langle g\rangle$, then $a - b \in \langle g\rangle$. But K is a field, so this happens precisely when $a = b$. Thus φ embeds K into $K[X]/\langle g\rangle$, as desired. □

3.2 Irreducible Polynomials over $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$

Our goal now is to study irreducible polynomials. Note that linear polynomials are irreducible, and recall that every polynomial in $\mathbb{C}$ factorizes, essentially uniquely, into linear factors. Furthermore, complex roots of real polynomials come in conjugate pairs, hence

$$g = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{R}[X]$$

factors as

$$g = a_n(X - \beta_1)\dots(X - \beta_r)(X - \gamma_1)(X - \overline{\gamma}_1)\dots(X - \gamma_3)(X - \overline{\gamma}_s)$$

[3] Note that there's some technicality about this φ not being a σ_α since we defined σ_α for α in the base domain, and i is kind of somewhere else.

in $\mathbb{C}[X]$, where $\beta_1, \dots, \beta_r \in \mathbb{R}$ and $\gamma_1, \dots, \gamma_s \in \mathbb{C} \setminus \mathbb{R}$ and $r + 2s = n$. Thus over $\mathbb{R}[X]$, g factors as

$$g = a_n(X - \beta_1)\dots(X - \beta_r)(X^2 - (\gamma_1 + \overline{\gamma}_1)X + \gamma_1\overline{\gamma}_1)\dots(X^2 - (\gamma_s + \overline{\gamma}_s)X + \gamma_s\overline{\gamma}_s)$$

in $\mathbb{R}[X]$, where the quadratic factors are irreducible in $\mathbb{R}[X]$.

Exercise 3.3. A quadratic $aX^2 + bX + c \in \mathbb{R}[X]$ is irreducible if and only if its discriminant $b^2 - 4ac < 0$.

Now we have pretty much characterized irreducible polynomials in $\mathbb{R}[X]$. But what about $\mathbb{Q}[X]$?

Theorem 3.6. *Let $g = a_0 + a_1X + a_2X^2 \in \mathbb{Q}[X]$. Then*

1. *If g is irreducible over $\mathbb{R}$, then it is irreducible over $\mathbb{Q}$.*
2. *If $g = a_2(X - \beta_1)(X - \beta)$ with $\beta_1, \beta_2 \in \mathbb{R}$, then g is irreducible in $\mathbb{Q}[X]$ if and only if β_1 and β_2 are irrational.*

Proof. (1) We show the contrapositive. If g factors as

$$g = a_2(X - q_1)(X - q_2) \in \mathbb{Q}[X],$$

then g also factors in $\mathbb{R}[X]$.

(2) If β_1 and β_2 are rational, then g factors in $\mathbb{Q}[X]$ and is thus not irreducible. For the other direction, if β_1 and β_2 are irrational, then $g = a_2(X - \beta_1)(X - \beta_2)$ is the only factorization in $\mathbb{R}[X]$ since $\mathbb{R}[X]$ is a UFD, so there is no factorization in $\mathbb{Q}[X]$ into linear factors. □

Example 3.5.2. Are the following polynomials irreducible in $\mathbb{R}[X]$? In $\mathbb{Q}[X]$?

1. $X^2 + X + 1$ is irreducible over $\mathbb{R}$ and $\mathbb{Q}$ since $b^2 - 4ac = -3$.
2. $X^2 - X - 1$ has roots $(-1 \pm \sqrt{5})/2$, so it factors over $\mathbb{R}$ but is irreducible over $\mathbb{Q}$.
3. $X^2 + X - 2$ factors as $(X + 2)(X - 1)$ over $\mathbb{R}$ and $\mathbb{Q}$.

Now that we have studied irreducible polynomials in $\mathbb{R}[X]$ and $\mathbb{Q}[X]$, can a polynomial in $\mathbb{Z}[X]$ be irreducible over $\mathbb{Z}$ but not $\mathbb{Q}$? The answer is no!

Theorem 3.7 (Gauss's lemma)**.** *Let f be a polynomial in $\mathbb{Z}[X]$, irreducible over $\mathbb{Z}$. Then f is irreducible over $\mathbb{Q}$.*

Proof. For sake of contradiction, suppose $f = gh$ with $g, h \in \mathbb{Q}[X]$ and $\partial g, \partial h < \partial f$. Then there exists $n \in \mathbb{Z}_{>0}$ such that $nf = g'h'$ where $g', h' \in \mathbb{Z}[X]$. Let n be the smallest positive integer with this property. Let

$$\begin{aligned} g' &= a_0 + a_1X + \dots + a_kX^k \\ h' &= b_0 + b_1X + \dots + b_lX^l. \end{aligned}$$

If $n = 1$, then $g' = g$ and $h' = h$, a contradiction. Now $n \geq 1$, so let p be a prime factor of n.[4] Without loss of generality, assume p divides g', i.e. $g' = pg''$ where $g'' \in \mathbb{Z}[X]$. Then

$$\frac{n}{p} f = g''h',$$

contradicting the minimality of n. Hence f cannot be factored over $\mathbb{Q}$. □

[4] Lemma: Either p divides all the coefficients of g' or p divides all the coefficients of h'. Proof left as an exercise.

Example 3.5.3. Show that $g = X^3 + 2X^2 + 4X - 6$ is irreducible over $\mathbb{Q}$.

Proof. If g factors over $\mathbb{Q}$, it factors over $\mathbb{Z}$ and at least one factor must be linear, i.e.

$$g = X^3 = 2X^2 + 4X - 6 = (X - a)(X^2 + bX + c)$$

where $a, b, c \in \mathbb{Z}$. We must have $ac = 6$, so $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $g(a) = 0$. We can check this:

a	1	-1	2	-2	3	-3	-6	6
$g(a)$	1	-9	1	-10	51	-27	306	-174

Hence g is irreducible over $\mathbb{Z}$ and thus also irreducible over $\mathbb{Q}$. □

We could do this trick since the degree was 3, forcing a linear factor. What about degrees higher than 3?

Theorem 3.8 (Eisenstein's criterion)**.** *Let $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$. Suppose there exists a prime p such that*

1. $p \nmid a_n$,
2. $p | a_i$ *for* $i = 0, \ldots, n - 1$,
3. $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

Proof. By Gauss's lemma, it suffices to show that f is irreducible over $\mathbb{Z}$. Suppose for sake of contradiction that $f = gh$ for

$$g = b_0 + b_1X + \cdots + b_rX^r \quad \text{and} \quad h = c_0 + c_1X + \cdots + c_sX^s,$$

$r, s < n$, and $r + s = n$. Note that $a_0 = b_0c_0$, so $p|a_0$ from (2) implies that $p|b_0$ or $p|c_0$. Since $p^2 \nmid a_0$, it cannot be both. Without loss of generality, assume $p|b_0$ and $p \nmid c_0$. Now suppose inductively that p divides $b_0, \ldots, b_{k-1}$ where $1 \le k \le r$. Then

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

and since p divides a_k, b_0c_k, b_1c_{k-1}, $\ldots$, $b_{k-1}c_1$, it follows that $p|b_kc_0$. Since $p \nmid c_0$ by assumption, we must have $p|b_k$. Thus $p|b_r$ and since $a_n = b_rc_s$, we have $p|a_n$, contradicting (1). Hence is f is irreducible. □

Example 3.5.4. The polynomial

$$X^5 + 2X^3 + \frac{8}{7}X^2 - \frac{4}{7}X + \frac{2}{7}$$

is irreducible over $\mathbb{Q}$.

Proof. Multiply by 7 and take the integer polynomial $7X^5 + 14X^3 + 8X^2 - 4X + 2$. Taking $p = 2$ satisfies Eisenstein's criterion, so this polynomial is irreducible over $\mathbb{Z}$ and thus also irreducible over $\mathbb{Q}$. □

Example 3.5.5. If $p > 2$ is prime, then show that

$$f = 1 + X + X^2 + \cdots + X^{p-1}$$

is irreducible over $\mathbb{Q}$.

Proof. First observe that
$$f = \frac{X^p - 1}{X - 1}.$$
Let $g(X) = f(X+1)$. Then
$$\begin{aligned} g(X) &= \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{1}{X}((X+1)^p - 1) = \frac{1}{X}\sum_{i=0}^{p}\binom{p}{i}X^{p-i} - 1 \\ &= \frac{1}{X}\sum_{i=0}^{p-1}\binom{p}{i}X^{p-i} = \sum_{i=0}^{p-1}\binom{p}{i}X^{p-i-1}. \end{aligned}$$
Note that $\binom{p}{1}, \binom{p}{2}, \dots \binom{p}{p-1}$ are all divisible by p, so g is irreducible by Eisenstein's criterion. Now if f factors as $f = uv$, then $g(X) = u(X+1)v(X+1)$, which is a contradiction since g is irreducible. $\square$

Lecture 4

Jan. 22 — Field Extensions

4.1 More on Irreducibility

The following excerpt is from Howie:

> Another device for determining irreducibility over $\mathbb{Z}$ (and consequently over $\mathbb{Q}$) is to map the polynomial onto $\mathbb{Z}_p[X]$ for some suitably chosen prime p. Let $g = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and let p be a prime not dividing a_n. For each i in $\{0, 1, \ldots, n\}$, let $\overline{a}_i$ denote the residue class $a_i + \langle p \rangle$ in the field $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$, and write the polynomial $\overline{a}_0 + \overline{a}_1 X + \cdots + \overline{a}_n X^n$ as $\overline{g}$. Our choice of p ensures that $\partial \overline{g} = n$. Suppose that $g = uv$, with $\partial u, \partial v < \partial f$ and $\partial u + \partial v = \partial g$. Then $\overline{g} = \overline{u}\,\overline{v}$. If we can show that $\overline{g}$ is irreducible in $\mathbb{Z}_p[X]$, then we have a contradiction, and we deduce that g is irreducible. The advantage of transferring the problem from $\mathbb{Z}[X]$ to $\mathbb{Z}_p[X]$ is that $\mathbb{Z}_p$ is finite, and the verification of irreducibility is a matter of checking a finite number of cases.

Example 4.0.1. Show that
$$g = 7X^4 + 10X^3 - 2X^2 + 4X - 5$$
is irreducible over $\mathbb{Q}$.

Proof. Let $p = 3$ and
$$\overline{g} = X^4 + X^3 + X^2 + 1$$
This has no linear factors since
$$\overline{g}(0) = 1, \quad \overline{g}(1) = 2, \quad \overline{g}(-1) = 1.$$
So suppose
$$\overline{g} = X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$$
in $\mathbb{Z}_3[x]$. Then for some $a, b, c, d \in \mathbb{Z}_3 = \{-1, 0, 1\}$, we have
$$\begin{cases} X^3 & a + c = 1 \\ X^2 & b + ac + d = 1 \\ X & ad + bc = 1 \\ 1 & bd = 1 \end{cases}$$
The first case is if $b = d = 1$, but this implies $ac = -1$, so $a = \pm 1$ and $c = \mp 1$. But $a + c = 1$, so this cannot happen. The second case is if $b = d = -1$. This implies that $ac = 0$ and $a + c = 1$. So if $a = 0$, then $c = 1$, so $1 = ad + bc = b$, which is a contradiction with $b = -1$. If $c = 0$, then $1 = ad + bc = d$,

which is a contradiction with $d = -1$. Thus $\overline{g}$ is irreducible in $\mathbb{Z}_3[x]$, so g is irreducible in $\mathbb{Z}[x]$, and by Gauss's lemma, g is irreducible in $\mathbb{Q}[x]$. $\square$

Remark. If we had tried $p = 2$, then we have $\overline{g} = x^4 + 1 \in \mathbb{Z}_2[x]$, which is not in fact irreducible since

$$\overline{g} = x^4 + 1 = (x+1)^4 \in \mathbb{Z}_2[x].$$

4.2 Field Extensions

Definition 4.1. Let K, L be fields and $\varphi : K \to L$ an injective homomorphism. Then L is a *field extension* of K, denoted $L : K$.

Example 4.1.1. We have $\mathbb{C} : \mathbb{R}$ is a field extension.

Definition 4.2. Recall that V is a K*-vector space* if

1. V is an abelian group under $+$,
2. For $a, b \in K$ and $x, y \in V$, we have

$$\text{(i). } a(x+y) = ax + ay, \quad \text{(ii). } (a+b)x = ax + bx, \quad \text{(iii). } (ab)x = a(bx), \quad \text{(iv). } 1x = 1.$$

Remark. If $L : K$ is a field extension, then L is a a vector space over K.

Definition 4.3. A *basis* for a vector space is a linearly independent spanning set.

Example 4.3.1. The complex numbers $\mathbb{C}$ is a $\mathbb{R}$-vector space with basis $\{1, i\}$. Bases are not unique, since $\{1+i, 1-i\}$ is another basis for $\mathbb{C}$.

Example 4.3.2. If there is a vector space that we know to be a field, then it is automatically a field extension of its ground field.

Definition 4.4. The *dimension* of L is the cardinality of a basis for $L : K$.[1] The dimension is also called the *degree* of $L : K$, denoted $[L : K]$. We say that L is a *finite extension* if $[L : K]$ is finite, and an *infinite extension* otherwise.

Example 4.4.1. We have $[\mathbb{C} : \mathbb{R}] = 2$, which is finite. On the other hand, $\mathbb{R} : \mathbb{Q}$ is an infinite extension.

Theorem 4.1. *Let $L : K$ be a field extension. Then $L = K$ if and only if $[L : K] = 1$.*

Proof. ($\Rightarrow$) If $L = K$, then $\{1\}$ is a basis for $L : K$, and thus $[L : K] = 1$.

($\Leftarrow$) If $[L : K] = 1$, then $\{x\}$ is a basis for $L : K$ for some $x \in L$. Then there exists some $a \in K$ such that $1 = ax$, so $x = a^{-1} \in K$. For every $y \in L$, there exists $b \in K$ such that $y = bx$. But then

$$y = bx = b(a^{-1}) \in K,$$

so $y \in K$ as well by closure. Thus $L = K$ as desired. $\square$

Remark. Let $L : K$ and $M : L$ be field extensions with

$$K \xrightarrow{\alpha} L \xrightarrow{\beta} M$$

[1] Note that this is well-defined since any two bases of L have the same length.

Then $M : K$ is also a field extension.

Theorem 4.2. *For field extensions $L : K$ and $M : L$, we have $[M : L][L : K] = [M : K]$.*

Proof. Suppose $\{a_1, a_2, \ldots a_r\}$ is a linearly independent subset of M over L and $\{b_1, b_2, \ldots, b_s\}$ is a linearly independent subset of L over K. Now we claim that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a linearly independent subset of M over K. To see this, suppose

$$\sum_{i=1}^{r} \sum_{j=1}^{s} \lambda_{ij} a_i b_i = 0$$

for some $\lambda_{ij} \in K$. We can rewrite this as

$$\sum_{i=1}^{r} \left(\sum_{j=1}^{s} \lambda_{ij} b_j \right) a_i = 0.$$

Since the a_i are linearly independent over L, it follows that

$$\sum_{j=1}^{s} \lambda_{ij} b_j = 0$$

for each $i = 1, \ldots, r$. Since the b_j are linearly independent over K, it follows that $\lambda_{ij} = 0$ for each i, j, which proves the claim. Returning to the main proof, if $[M : L]$ or $[L : K]$ is infinite, then r or s can be made arbitrarily large, so

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

can also be made arbitrarily large, and hence $[M : K]$ is infinite. Now suppose $[M : L] = r < \infty$ and $[L : K] = s < \infty$. Let $\{a_1, a_2, \ldots, a_r\}$ be a basis for $M : L$ and $\{b_1, b_2, \ldots, b_s\}$ be a basis for $L : K$. We will show that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a basis for $M : K$. Since we already showed that $\{a_i b_j\}$ is linearly independent, it only remains to show that they span M over K. For each $z \in M$, there exist $\lambda_1, \ldots, \lambda_r \in L$ such that

$$z = \sum_{i=1}^{r} \lambda_i a_i.$$

Then for each $\lambda_i \in L$, there exist $\mu_{i1}, \ldots, \mu_{is} \in K$ such that

$$\lambda_i = \sum_{j=1}^{s} \mu_{ij} b_j.$$

Combining this yields

$$z = \sum_{i=1}^{r} \sum_{j=1}^{s} \mu_{ij} a_i b_j$$

as desired, which finishes the proof. $\square$

Example 4.4.2. Consider $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Exercise 4.1. Show that $\mathbb{Q}[\sqrt{2}]$ is a field. (Hint: $1/(a + b\sqrt{2}) = (a - b\sqrt{2})/(a^2 - 2b^2)$.)

Definition 4.5. Let K be a subfield of L and S a subset of L. The *subfield of L generated over K by S*, denoted $K(S)$, is the intersection of all subfields of L containing $K \cup S$. If $S = \{\alpha_1, \dots, \alpha_n\}$ is finite, we write $K(\alpha_1, \dots, \alpha_n)$.

Theorem 4.3. *Let E be the elements in L that can be expressed as quotients of finite K-linear combinations of finite products of elements in S. Then $K(S) = E$.*

Proof. To see that $K(S) \subseteq E$, simply check that E is a subfield of L containing $K \cup S$.

For $E \subseteq K(S)$, note that any subfield of L containing K and S must contain all finite products of elements in S, all linear combinations of such products, and all quotients of such linear combinations. This is precisely what is means to have $E \subseteq K(S)$. □

Definition 4.6. A *simple extension* of K is $K(\alpha)$, i.e. S has a single element $\alpha \notin K$.

Example 4.6.1. The previous example $\mathbb{Q}(\sqrt{2})$ is a simple extension.

Theorem 4.4. *Let L be a field, K a subfield, and $\alpha \in L$. Then either*

1. *$K(\alpha)$ is isomorphic to $K(X)$, the field of rational forms with coefficients in K,*
2. *or there exists a unique monic polynomial $m \in K[X]$ with the property that for all $f \in K[X]$,*
   (a) *$f(\alpha) = 0$ if and only if $m|f$,*
   (b) *the field $K(\alpha)$ coincides with $K[\alpha]$, the ring of all polynomials in α with coefficients in K,*
   (c) *and $[K[\alpha] : K] = \partial m$.*

Proof. Suppose there does not exist nonzero $f \in K[X]$ such that $f(\alpha) = 0$. Then there exists a map $\varphi : K(X) \to K(\alpha)$ with $f/g \mapsto f(\alpha)/g(\alpha)$, which is defined since $g(\alpha) = 0$ only if g is the zero polynomial. Note that φ is a surjective homomorphism,[2] which one can check as an exercise. Now we show that φ is also injective. To see this, suppose

$$\varphi(f/g) = \varphi(p/q),$$

which happens if and only if

$$f(\alpha)q(\alpha) - p(\alpha)g(\alpha) = 0.$$

in L. This happens if and only if $fq - pg = 0$ in $K[X]$, which happens if and only if $f/g = p/q$ in $K(X)$. This completes the first case of the theorem.

Now suppose there exists nonzero $g \in K[X]$ such that $g(\alpha) = 0$. Furthermore, suppose g is a polynomial of least degree with this property. Let a be the leading coefficient of g, and let $m = g/a$, so that m is monic and $m(\alpha) = 0$ still. The reverse implication in (2a) is clear. For the forwards implication in (2a), note that by division with remainder for polynomials over a field, we can write

$$f = qm + r,$$

where $\partial r < \partial m$. By the minimality of ∂m, we must have $r = 0$, so $m|f$. For the uniqueness of m, suppose there exists m' with the same properties. Then $m(\alpha) = m'(\alpha) = 0$, so $m|m'$ and $m'|m$, which

[2] Also check that φ is well-defined.

implies that $m = m'$ since m and m' are monic. For the irreducibility of m, suppose for the sake of contradiction that $m = pq$ with $\partial p, \partial q < \partial m$. Then $m(\alpha) = p(\alpha)q(\alpha) = 0$, so either $p(\alpha) = 0$ or $q(\alpha) = 0$, which contradicts the minimality of ∂m.

Now we show (2b), which says that $K(\alpha) = K[\alpha]$. For this, consider $p(\alpha)/q(\alpha) \in K(\alpha)$ for $q(\alpha) \neq 0$. Then $m \nmid q$, and since m is irreducible we have $\gcd(m, q) = 1$. Now by Theorem 2.15 of Howie (about gcd's in the Euclidean domain $K[X]$), there exist polynomials a, b such that $aq + bm = 1$. Setting $X = \alpha$ yields $a(\alpha)q(\alpha) = 1$, so

$$\frac{p(\alpha)}{q(\alpha)} = p(\alpha)a(\alpha) \in K[\alpha].$$

Thus $K(\alpha) \subseteq K[\alpha]$. Since we already know that $K[\alpha] \subseteq K(\alpha)$, we conclude that $K(\alpha) = K[\alpha]$.

Finally we show (2c), which claims that $[K[\alpha] : K] = \partial m$. For this, suppose $\partial m = n$ and let

$$p(\alpha) \in K[\alpha] = K(\alpha).$$

Then $p = qm + r$ where $\partial r < \partial m = n$. We have $p(\alpha) = r(\alpha)$, so if

$$r = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

for $c_i \in K$, then

$$p(\alpha) = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1}.$$

So $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a spanning set for $K[\alpha]$. To see that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is also linearly independent, suppose there exists $a_i \in K$ such that

$$a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} = 0.$$

Then $a_0 = \cdots = a_{n-1} = 0$ since otherwise we would have a polynomial

$$p = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

with $\partial p \leq n - 1$ and $p(\alpha) = 0$, which is a contradiction with the minimality of $\partial m = n$. Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis, and so $[K[\alpha] : K] = n = \partial m$. $\square$

Example 4.6.2. Continuing the same example, note that

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + a_3\sqrt{2}^3 + \cdots + a_n\sqrt{2}^n \mid a_i \in \mathbb{Q}\},$$

which falls in the second case of the previous theorem.

Remark. We also have $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/\langle X^2 - 2\rangle$.

Lecture 5

Jan. 24 — Algebraic Extensions

5.1 Minimal Polynomials

Remark. The m in the previous theorem from last class is called the *minimal polynomial* of α.

Example 5.0.1. Let
$$\mathbb{Q}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$
Here $m = X^2 + 3$, so this is a degree 2 extension.

Exercise 5.1. Write $1/(a + bi\sqrt{3})$ in the form $c + di\sqrt{3}$.

Example 5.0.2. Is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ a simple extension? In fact it is! Note that certainly
$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$
For the reverse inclusion, observe that $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$, so
$$1/(\sqrt{3} + \sqrt{2}) = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$
From this we have
$$(\sqrt{3} + \sqrt{2}) + (\sqrt{3} - \sqrt{2}) = 2\sqrt{3},$$
which implies that $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Similarly $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Now we can consider
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = (\mathbb{Q}[\sqrt{2}])[\sqrt{3}].$$
First we have $[Q[\sqrt{2}] : \mathbb{Q}] = 2$. Note that $X^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}[\sqrt{2}]$, so $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$. Hence $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$ with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.[1] To find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$, we can compute
$$\begin{aligned}(\sqrt{2} + \sqrt{3})^2 &= 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \\ (\sqrt{2} + \sqrt{3})^4 &= 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}.\end{aligned}$$
Thus $X^4 - 10X^2 + 1$ is the minimal polynomial, since $\alpha^4 - 10\alpha^2 + 1 = 0$ for $\alpha = \sqrt{2} + \sqrt{3}$.

[1] Since $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\alpha]$ where $\alpha = \sqrt{2} + \sqrt{3}$, we have $\{1, \alpha, \alpha^2, \alpha^3\}$ as another basis.

5.2 Algebraic Extensions

Definition 5.1. If α has a minimal polynomial over K, we say α is *algebraic* over K, and $K[\alpha] = K(\alpha)$ is an *algebraic extension* of K. A complex number that is algebraic over $\mathbb{Q}$ is called an *algebraic number*. Otherwise, if $K(\alpha) \cong K(X)$, then we say α is *transcendental* over K. A transcendental number α is a complex number that is transcendental over $\mathbb{Q}$.

Example 5.1.1. We have that $\mathbb{Q}(i\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are all simple algebraic extensions of $\mathbb{Q}$, whereas $\mathbb{Q}(X)$ is a simple transcendental extension of $\mathbb{Q}$.

Theorem 5.1. *Let $K(\alpha)$ be a simple transcendental extension of K. Then $[K(\alpha) : K] = \infty$.*

Proof. Observe that $1, \alpha, \alpha^2, \ldots$ are linearly independent over K, since no minimal polynomial exists. □

Definition 5.2. An extension L over K is an *algebraic extension* if any element of L is algebraic over K. Otherwise, L is a *transcendental extension*.

Theorem 5.2. *Every finite extension is algebraic.*

Proof. Let $L : K$ be a finite extension and suppose for sake of contradiction that $\alpha \in L$ is transcendental over K. Then $1, \alpha, \alpha^2, \ldots$ are linearly independent, contradicting the fact that $L : K$ is finite. □

Theorem 5.3. *Let $L : K$ be a field extension and let $\mathcal{A}(L)$ be the set of elements in L that are algebraic over K. Then $\mathcal{A}(L)$ is a subfield of L.*

Proof. See Howie. Just need to show the closure of algebraic elements under usual field operations. □

Example 5.2.1. For $L = \mathbb{C}$ and $K = \mathbb{Q}$, we have that $\mathcal{A}(\mathbb{C})$ is the field $\mathbb{A}$ of algebraic numbers.

Theorem 5.4. *The set of algebraic numbers $\mathbb{A}$ is countable.*

Proof sketch. Note that the set of monic polynomials of degree n with coefficients in $\mathbb{Q}$ is countable, and each such polynomial has at most n distinct roots in $\mathbb{C}$. Hence the number of roots of such polynomials is countable. Then $\mathbb{A}$ is the countable union of countable sets, so $\mathbb{A}$ is countable. □

Theorem 5.5. *Transcendental numbers exist.*

Proof. Since $|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0} > \aleph_0$, we must have that $\mathbb{C} \setminus \mathbb{A}$ is nonempty. □

Remark. The above proof is very nonconstructive, what about actual examples of transcendental numbers? In 1844, Liouville constructed the following example:

$$\sum_{n=1}^{\infty} 10^{-n!},$$

which was shown to be transcendental. In 1873, Hermite showed that e is transcendental, and in 1882, Lindemann showed that π is transcendental.

Theorem 5.6. *Let $L : K$ be a field extension and $\alpha_1, \ldots, \alpha_n \in L$ have minimal polynomials $m_1, \ldots, m_n$, respectively. Then $[K(\alpha_1, \ldots, \alpha_n) : K] \leq \partial m_1 \partial m_2 \ldots \partial m_n$.*

Proof. See Howie. Uses induction and the fact that $[M : L][L : K] = [M : K]$. □

Example 5.2.2. Consider

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = 2,$$

but $[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{6}] : \mathbb{Q}] = 4$. So the bound in the previous theorem cannot be made into an equality.

Proposition 5.1. *A field extension $L : K$ is finite if and only if for some n, there exist $\alpha_1, \ldots, \alpha_n$ algebraic over K such that $L = K(\alpha_1, \ldots, \alpha_n)$.*

Proof. ($\Leftarrow$) This is precisely the previous theorem.

($\Rightarrow$) Suppose $L : K$ is finite and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for L over K. Since finite extensions are algebraic, the α_i must be algebraic. □

Exercise 5.2. Show that $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[X]/\langle X^2 - 2\rangle$ defined by

$$a + b\sqrt{2} \mapsto a + bX + \langle X^2 - 2\rangle$$

is an isomorphism.

Theorem 5.7. *Let K be a field and m a monic irreducible polynomial in $K[X]$. Then $L = K[X]/\langle m\rangle$ is a simple algebraic extension $K[\alpha]$ of K, and $\alpha = X + \langle m\rangle$ has minimal polynomial m over K.*

Proof. First note that L is indeed a field since m is irreducible. Also $L : K$ is indeed a field extension since $\varphi : K \to L$ defined by $a \mapsto a + \langle m\rangle$ is an injective homomorphism. Now let $\alpha = X + \langle m\rangle$. For

$$f = a_0 + a_1 X + \cdots + a_n X^n \in K[X],$$

we have

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \cdots + a_n\alpha^n = a_0 + a_1(X + \langle m\rangle) + \cdots + a_n(X + \langle m\rangle)^n \\ &= a_0 + a_1 X + \cdots + a_n X^n + \langle m\rangle = f + \langle m\rangle. \end{aligned}$$

So $f(\alpha) = 0$ if and only if $f \in \langle m\rangle$, i.e. $m|f$. Hence m is the minimal polynomial of α. □

Lecture 6

Jan. 29 — Geometric Constructions

6.1 K-Isomorphisms

Recall from last class that $L = K[X]/\langle m\rangle$ is a simple algebraic extension of K. In fact, we can show that the field L is essentially unique, i.e. unique up to isomorphism.

Theorem 6.1. *Let K be a field and and f and an irreducible polynomial in $K[X]$. If L and L' are two extensions of K containing roots α and α' respectively of f, then there exists an isomorphism $K[\alpha] \to K[\alpha']$ which fixes every element of K.*

Proof sketch. Suppose
$$f = a_0 + a_1 X + \cdots + a_n X^n.$$
Then $K[\alpha]$ consists of polynomials of the form
$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$
This is because multiplication in $K[\alpha]$ relies on the observation that
$$\alpha^n = -\frac{1}{\alpha_n}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})$$
since α is a root of f. Define $\psi : K[\alpha] \to K[\alpha']$ by $\psi(g(a)) = g(\alpha')$ and show that ψ is an isomorphism. $\square$

Exercise 6.1. Check the following from the previous proof:

1. ψ is one-to-one and onto,
2. ψ fixes K,
3. and ψ is a homomorphism.

For the last point, the addition is mostly straightforward but the multiplication is more involved since we need to reduce when we get α^n terms in the product.

Definition 6.1. A *K-isomorphism* is an isomorphism $\varphi : L \to L'$ such that $\varphi(x) = x$ for all $x \in K$.

Example 6.1.1. For $\mathbb{C} : \mathbb{R}$, the complex conjugation map $\varphi : \mathbb{C} \to \mathbb{C}$ given by $\varphi(a + bi) = a - bi$ is a $\mathbb{R}$-isomorphism.

Example 6.1.2. For $\mathbb{Q}[X]/\langle X^2+3\rangle : \mathbb{Q}$,[1] the map $\psi : \mathbb{Q}[X]/\langle X^2+3\rangle \to \mathbb{Q}[X]/\langle X^2+3\rangle$ given by

$$\psi(a+bX+\langle X^2+3\rangle) = a-bX+\langle X^2+3\rangle$$

is a $\mathbb{Q}$-isomorphism. The analogous map $\psi : \mathbb{Q}[i\sqrt{3}] \to \mathbb{Q}[i\sqrt{3}]$ given by $\psi(a+bi\sqrt{3}) = a-bi\sqrt{3}$ also works, which we can view as a restriction of the complex conjugation map to $\mathbb{Q}[i\sqrt{3}]$.

6.2 Applications to Geometric Constructions

Consider the straightedge and compass Constructions from geometry. Let B_0 be a set of points. Then we have the following operations:

1. (straightedge) Draw a straight line through any two points in B_0.
2. (compass) Draw a circle whose center is a point in B_0 passing through another point in B_0.

Let $C(B_0)$ be the set of points which are intersections of lines or circles obtained form B_0 by (1) and (2). Let $B_1 = B_0 \cup C(B_0)$, and proceed inductively to get $B_n = B_{n-1} \cup C(B_{n-1})$.

Definition 6.2. A point is *constructible from* B_0 if it belongs to B_n for some n. A point is *constructible* if it is constructible from $\{O, I\}$ where $O = (0,0)$ and $I = (1,0)$.

Example 6.2.1. To find the midpoint of the line segment OI from $B_0 = \{O, I\}$, we can do the following:

1. Draw a circle with center O passing through I.
2. Draw a circle with center I passing through O.
3. Mark points P and Q where these circles intersect. So $B_1 \supseteq \{O, I, P, Q\}$.
4. Draw a line connecting P and Q.
5. Draw a line connecting O and I.
6. Mark the point M where PQ and OI meet. So $B_2 \supseteq \{O, I, P, Q, M\}$.

Thus M is constructible from $\{O, I\}$.

The algebraic perspective is the following: Associate to B_i the subfield of $\mathbb{R}$ generated by coordinates of points in B_i, i.e. view each coordinate of each point as an element and take the subfield generated.

Example 6.2.2. For $B_0 = \{(0,0),(1,0)\}$, we have $\{0,0,1,0\} \subseteq K_0 = \mathbb{Q}$ is the subfield of $\mathbb{R}$ generated by the coordinates of B_0. Next take[2]

$$B_1 = \{O, I, P, Q\} = \{(0,0),(1,0),(1/2, \pm\sqrt{3}/2)\},$$

so that $K_1 = \mathbb{Q}[\sqrt{3}]$ is the field generated by B_1. Then

$$B_2 = \{O, I, P, Q, M\} = \{(0,0),(1,0),(1/2, \pm\sqrt{3}/2),(1/2,0)\},$$

and the field generated by B_2 is still $K_2 = \mathbb{Q}[\sqrt{3}]$.

[1] Note that $\mathbb{Q}[X]/\langle X^2+3\rangle \cong \mathbb{Q}[i\sqrt{3}]$. The isomorphism is given by $a+bX+\langle X^3+3\rangle \mapsto a+bi\sqrt{3}$.

[2] There is some abuse of notation here since we take B_i to be only some subset of all the actual possible points.

Theorem 6.2. *Let P be a constructible point belonging to B_n, where $B_0 = \{(0,0),(1,0)\}$, and let K_n be the field generated over $\mathbb{Q}$ by B_n. Then $[K_n : \mathbb{Q}]$ is a power of 2.*

Proof sketch. We proceed by induction. The base case is $K_0 = \mathbb{Q}$, so $[K_0 : \mathbb{Q}] = 1 = 2^0$. Now suppose $[K_{n-1} : \mathbb{Q}] = 2^k$ for some $k \geq 0$, and we want to show that $[K_n : K_{n-1}]$ is a power of 2. Observe that new points in B_n can be obtained by

1. intersection of two lines,
2. intersection of a line and a circle,
3. or intersection of two circles.

In case (1), the intersection of two lines is given by solving a system of two linear equations, which only involves rational operations[3]. In other words, this case takes place entirely in K_{n-1}.

In case (2), the intersection of a line and a circle is given by solving of a system of one linear equation and one quadratic equation. Solving the linear equation for one of the variables and substituting into the quadratic equation reduces the system down to a single quadratic equation in a single variable. The solution involves $\sqrt{\Delta}$, where Δ is the discriminant. Then the new points are in $K_{n-1}[\sqrt{\Delta}]$.

In case (3), the intersection of two circles is given by solving a system of two quadratic equations. Subtracting the two quadratic equations yields a linear equation, which reduces back to case (2).

Thus the elements in K_n are either in K_{n-1} or $K_{n-1}[\sqrt{\Delta}]$ for some $\Delta \in K_{n-1}$.[4] Hence $[K_n : K_{n-1}]$ is either 1 or 2, so by induction $[K_n : \mathbb{Q}]$ is a power of 2. □

6.3 Classic Problems

6.3.1 Duplicating the Cube

Consider the problem of taking a cube of volume 1, and constructing a cube of volume 2. We need α such that $\alpha^3 = 2$. But $X^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$. This is not a power of 2, so α is not constructible and thus we cannot duplicate the cube.

6.3.2 Trisecting the Angle

Recall the triple angle formula:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Suppose $\cos 3\theta = c$. So to find $\cos\theta$, we want a root of $4X^3 - 3X - c = 0$. This depends on c.

Example 6.2.3. If $3\theta = \pi/2$, then $c = 0$ and the polynomial factors into

$$4X^3 - 3X = 4X(4X^2 - 3),$$

so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$. So in fact we can trisect $\pi/2 = 90°$.

[3]By rational operations we mean addition, subtraction, multiplication, division.

[4]We can set it up so that we only gain one extra intersection, i.e. only one Δ, at each step.

Example 6.2.4. If $3\theta = \pi/3$, then $c = 1/2$ and we have $4X^3 - 3X - 1/2$. Let

$$f(X) = 8X^3 - 6X - 1,$$

so that $g(X) = g(X/2) = X^3 - 3X - 1$. Note that g does not factor over $\mathbb{Z}$ since that requires a linear factor of $X \pm 1$ but $g(\pm 1) \neq 0$. So g is irreducible over $\mathbb{Z}$ and by Gauss's lemma, g is irreducible over $\mathbb{Q}$. Thus f is irreducible. Hence $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, so we cannot trisect $\pi/3$ with a straightedge and compass.

Lecture 7

Jan. 31 — Splitting Fields

7.1 Review of Notation

Recall that

$$\mathbb{Q}[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in \mathbb{Q}\}$$
$$\mathbb{Q}(X) = \{f/g : f, g \in \mathbb{Q}[X], g \neq 0\}/\sim,$$

where $\sim$ is the usual relation on fractions, e.g. $2f/2g = f/g$. Next, recall that

$$\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} + \cdots + a_n\sqrt{2}^n : a_i \in \mathbb{Q}\} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

since $\sqrt{2}^2 = 2$. Also $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q} \cup \{\sqrt{2}\}$. In this case, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ since

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

Next, we have

$$\begin{aligned}\mathbb{Q}[X]/\langle X^2 - 2\rangle &= \{a_0 + a_1X + \cdots + a_nX^n + \langle X^2 - 2\rangle : a_i \in \mathbb{Q}\}\\ &= \{a + bX + \langle X^2 - 2\rangle : a, b \in \mathbb{Q}\}\end{aligned}$$

since $X^2 + \langle X^2 - 2\rangle = 2 + \langle X^2 - 2\rangle$. In fact, $\mathbb{Q}[X]/\langle X^2 - 2\rangle \cong \mathbb{Q}[\sqrt{2}]$.[1]

7.2 Splitting Fields

The motivating question here is: When can we factor a polynomial into linear factors?

Definition 7.1. A polynomial *splits completely* over K if it can be factored into linear factors over K.

Example 7.1.1. The polynomial X^2+2 splits completely over $\mathbb{Q}[i\sqrt{2}]$ since $X^2+2 = (X-i\sqrt{2})(X+i\sqrt{2})$.

Example 7.1.2. The polynomial $X^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. However, it factors as

$$X^3 - 2 = (X - \alpha)(X^2 + \alpha X + \alpha^2)$$

in $\mathbb{Q}[\alpha]$, where $\alpha = \sqrt[3]{2}$. Also $X^2 + \alpha X + \alpha^2$ is irreducible over $\mathbb{Q}[\alpha]$, since its discriminant shows that it is irreducible even over $\mathbb{R}$. But in $\mathbb{C}$, we can factor it as

$$X^3 - 2 = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{4\pi i/3}).$$

A smaller field that $X^3 - 2$ splits completely over is $\mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$.

[1] Here the isomorphism $\mathbb{Q}[X]/\langle X^2 - 2\rangle \to \mathbb{Q}[\sqrt{2}]$ is given by $a + bX + \langle X^2 - 2\rangle \mapsto a + b\sqrt{2}$.

Definition 7.2. Let K be a field and $f \in K[X]$. An extension L of K is a *splitting field* for f over K if

1. f splits completely over L,
2. and f does not split completely over any subfield E with $K < E < L$.

Example 7.2.1. From the last two examples, $\mathbb{Q}[i\sqrt{2}]$ is a splitting field over $\mathbb{Q}$ for X^2+2, and $\mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$ is a splitting field for $X^3 - 2$ over $\mathbb{Q}$.

Theorem 7.1. *Let K be a field and $f \in K[X]$ with $\partial f = n$. Then there exists a splitting field L for f over K and $[L : K] \leq n!$.*

Proof. The proof is essentially the process we perform in the following example. At each step, construct an extension in which we can split off a linear factor from f. For more details, see Howie. □

Example 7.2.2. Let us find a splitting field for

$$f = X^5 + X^4 - X^3 - 3X^2 - 3X + 3$$

over $\mathbb{Q}$. Note that $\partial f = n$. Stare hard enough and we can see that

$$f = (X^3 - 3)(X^2 + X - 1),$$

where the first factor is irreducible by Eisenstein's criterion and the second factor is irreducible by checking the discriminant. Now add a root, say $\alpha = \sqrt[3]{3}$, and let $E_1 = \mathbb{Q}(\alpha)$. Then

$$f = (X - \alpha)(X^2 + \alpha X + \alpha^2)(X^2 + X - 1).$$

Note that $[E_1 : K] \leq n = \partial f$. Now let $E_2 = E_1(\alpha e^{2\pi i/3})$, so that

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1).$$

Note that $[E_2 : \mathbb{Q}] \leq n(n-1)$. Next $E_3 = E_2(\alpha e^{-2\pi i/3})$ with

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1).$$

Note that $[E_3 : K] \leq n(n-1)(n-2)$. Now let

$$\gamma = \frac{-1 + \sqrt{5}}{2}, \quad \delta = \frac{-1 - \sqrt{5}}{2}.$$

Let $E_4 = E_3(\gamma)$,

$$f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X - \gamma)(X - \delta).$$

Finally $E_5 = E_4(\delta)$ is the splitting field for f over $\mathbb{Q}$. Note that we did much better than $n!$ here, since

$$[E_1 : \mathbb{Q}] = 3, \quad [E_2 : E_1] = 2, \quad [E_3 : E_2] = 1, \quad [E_4 : E_3] = 2, \quad [E_5 : E_4] = 1,$$

so $[E_5 : \mathbb{Q}] = 12 \leq 120$.

Remark. Splitting fields are unique (up to isomorphism).

Theorem 7.2. *Let L and L' be splitting fields of f over K. Then there exists an isomorphism $\varphi : L \to L'$ fixing K.*

Proof sketch. Induct on the number of roots of f that are not in K. The induction step uses Theorem 6.1 from last class giving an isomorphism $K[\alpha] \to K[\alpha']$ for α, α' roots of an irreducible polynomial. $\square$

Example 7.2.3. Let us find the splitting field of $f = X^4 - 2$ over $\mathbb{Q}$ and its degree. Note that $X^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Note that

$$X^4 - 2 = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha)$$

where $\alpha = \sqrt[4]{2}$. So the splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. For the degree, note that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ since the minimal polynomial of $\sqrt[4]{2}$ is $X^4 - 2$. A basis for this extension is $\{1, \sqrt[4]{2}, \sqrt[4]{2}^2, \sqrt[4]{2}^3\}$. Since $i \notin \mathbb{Q}(\sqrt[4]{2})$, we have $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ since the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$ is $X^2 + 1$. Thus we see that the degree of the splitting field is $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$.

Example 7.2.4. Let us look at monic quadratic polynomials over $\mathbb{Z}_3 = \{-1, 0, 1\}$.[2] These are

$$\begin{array}{ccc} X^2 & X^2+1 & X^2-1 \\ X^2+X & X^2+X+1 & X^2+X-1 \\ X^2-X & X^2-X+1 & X^2-X-1. \end{array}$$

We have 0 is a root of the polynomials in the first column, 1 is a root of $X^2 - 1$ and $X^2 + X + 1$, and -1 is a root of $X^2 - X + 1$. So the irreducible polynomials over $\mathbb{Z}_3$ are

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1.$$

Let $L = \mathbb{Z}_3[X]/\langle X^2 + 1\rangle$. Observe that $\alpha = X + \langle X^2 + 1\rangle$ satisfies

$$\alpha^2 = X^2 + \langle X^2 + 1\rangle = -1 + \langle X^2 + 1\rangle.$$

Hence L is a splitting field for $X^2 + 1$ since $(X - \alpha)(X + \alpha) = X^2 + 1$. Similarly, $\mathbb{Z}_3[X]/\langle X^2 + X - 1\rangle$ is a splitting field for $X^2 + X - 1$ and $\mathbb{Z}_3[X]/\langle X^2 - X - 1\rangle$ is a splitting field for $X^2 - X - 1$. Note that each of these fields have $9 = 3^2$ elements since they are degree 2 extensions of $\mathbb{Z}_3$.

Remark. In L, we had $\alpha \in L$ such that $\alpha^2 = -1$ and addition is performed modulo 3. Now observe

$$(\alpha + 1)^2 + (\alpha + 1) - 1 = (\alpha^2 - \alpha + 1) + (\alpha + 1) - 1 = \alpha^2 - \alpha + \alpha + 1 + 1 - 1 = 0$$

since $\alpha^2 = -1$. So $\alpha + 1$ is a root of $X^2 + X - 1$ in L. By a similar computation, we see that $-\alpha + 1$ is a root of $X^2 + X - 1$, so L is also a splitting field for $X^2 + X - 1$. Additionally, $\alpha - 1$ and $-\alpha - 1$ are roots of $X^2 - X - 1$, so L is also a splitting field for $X^2 - X - 1$. So by uniqueness of splitting fields,

$$\mathbb{Z}_3[X]/\langle X^2 + 1\rangle \cong \mathbb{Z}_3[X]/\langle X^2 + X - 1\rangle \cong \mathbb{Z}_3[X]/\langle X^2 - X - 1\rangle.$$

Exercise 7.1. Find explicit isomorphisms between these fields.

7.3 Finite Fields

Definition 7.3. Let $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$. Then the *formal derivative* of f is

$$Df = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Exercise 7.2. The usual formulas for derivatives

$$D(kf) = kDf, \quad D(f + g) = Df + Dg, \quad D(fg) = (Df)g + f(Dg)$$

all still hold for $f, g \in K[X]$ and $k \in K$.

[2] Note that as opposite to $\mathbb{Q}$, this field has finite characteristic.

Lecture 8

Feb. 5 — Finite Fields

8.1 Last Time

Example 8.0.1. The splitting field of $X^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[4]{2}])$ since

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}).$$

Example 8.0.2. The splitting field of $Y^2 + 1$ over $\mathbb{Z}_3$ is $\mathbb{Z}_3[X]/\langle X^2 + 1\rangle$. If $\alpha = X + \langle X^2 + 1\rangle$, then

$$Y^2 + 1 = (Y - \alpha)(Y + \alpha).$$

Also the degree of this extension is $[Z_3[X]/\langle X^2 + 1\rangle : \mathbb{Z}_3] = 2$, and a basis for the extension is $\{1, X\}$.

8.2 Finite Fields

Lemma 8.1. *Let $f \in K[X]$, K a field, and L be a splitting field for f over K. Then the roots of f are distinct if and only if f and Df have no nonconstant common factor.*

Proof. ($\Leftarrow$) We show the contrapositive. Suppose f has a repeated root α in L. Then

$$f = (X - \alpha)^r g$$

for some $r \geq 2$. Then

$$Df = (X - \alpha)^r Dg + r(X - \alpha)^{r-1} g,$$

so Df and f both have $X - \alpha$ as a factor.

($\Rightarrow$) Suppose the roots of f are all distinct. Then for each root α of f in L, we have

$$f = (X - \alpha)g,$$

where $g(\alpha) \neq 0$. Then

$$Df = (X - \alpha)Dg + g,$$

so that

$$(Df)(\alpha) = g(\alpha) \neq 0,$$

i.e. $X - \alpha \nmid Df$. This holds for factor of f in $L[X]$, so f and Df have no common proper factors. ☐

Theorem 8.1. *Finite fields exist and are unique up to isomorphism. In particular,*

1. *Let K be a finite field. Then $|K| = p^n$ for some prime p and integer $n \geq 1$. Every element of K is a root of $X^{p^n} - X$ and K is a splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$.*

2. *Let p be a prime and $n \in \mathbb{Z}$, $n \geq 1$. Then there exists a unique field of order p^n up to isomorphism.*

Proof. (1) Let $\operatorname{char} K = p$. Then K is a finite extension of $\mathbb{Z}_p$. Let $n = [K : \mathbb{Z}_p]$. If $\{\delta_1, \dots, \delta_n\}$ is a basis for K over $\mathbb{Z}_p$, then every element in K can be uniquely written as

$$a_1\delta_1 + \cdots + a_n\delta_n$$

for some $a_i \in \mathbb{Z}_p$. There are p^n such elements, so $|K| = p^n$. Then $|K^*| = p^n - 1$.[1] For any $\alpha \in K^*$, the order of α divides $p^n - 1$. So $\alpha^{p^n-1} = 1$, and hence $\alpha^{p^n} - \alpha = 0$. We also have $0^{p^n} - 0 = 0$ so every element in K is a root of $X^{p^n} - X$. Hence $X^{p^n} - X$ splits completely over K. Since $X - \alpha$ is a factor of $X^{p^n} - X$ for each of the p^n elements of K, $X^{p^n} - X$ does not split over any proper subfield of K. Thus we conclude that K is a splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$.

(2) Given a prime p and an integer $n \geq 1$, let L be the splitting field of $X^{p^n} - X$ over $\mathbb{Z}_p$. Note that

$$Df = p^n X^{p^n-1} - 1 = -1$$

since $\operatorname{char} \mathbb{Z}_p = p$. Then Df and f have no nonconstant common factors, so by Lemma 8.1, we see that $X^{p^n} - X$ has p^n distinct roots in L. Let K be the set of p^n distinct roots, and we claim that K is a subfield of L. To check this, let $a, b \in K$. Then by an extension of Theorem 2.4,

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$$

in $\mathbb{Z}_p$, $a - b \in K$. Also

$$(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1},$$

so $ab^{-1} \in K$. Hence K is a field of order p^n. In fact, $K = L$ since K contains all the roots of $X^{p^n} - X$ and no proper subfield does. By uniqueness of splitting fields, K is unique up to isomorphism. $\square$

Definition 8.1. We call the field of order p^n the *Galois field* of order p^n, denoted $\mathrm{GF}(p^n)$.

Example 8.1.1. We have $\mathrm{GF}(3^2) = \mathbb{Z}_3[X]/\langle X^2+1\rangle \cong \mathbb{Z}_3[X]/\langle X^2+X-1\rangle \cong \mathbb{Z}_3[X]/\langle X^2-X-1\rangle$.

Remark. Recall that for a finite group G and $a \in G$, the *order* of a is

$$\operatorname{ord}(a) = \min\{k \in \mathbb{N} : a^k = 1\}.$$

The *exponent* of G is

$$\exp(G) = \min\{k \in \mathbb{N} : a^k = 1 \text{ for all } a \in G\}.$$

Also recall that $\operatorname{ord}(a)$ divides $|G|$ for all $a \in G$, and thus $\exp(G)$ divides $|G|$.

Exercise 8.1. Show that $\exp(G) = \operatorname{lcm}\{\operatorname{ord}(a) : a \in G\}$.

Example 8.1.2. For $S_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\}$, the order of the transpositions is 2 and the order of 3-cycles is 3. So we see that $\exp(S_3) = 6$.

Proposition 8.1. *If G is a finite abelian group, then there exists $a \in G$ such that* $\operatorname{ord}(a) = \exp(G)$.

[1] Recall that K^* is the set of nonzero elements of K, which forms a group under multiplication. We also call K^* the group of units of K.

Proof. Suppose that
$$\exp(G) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$
where the p_i are distinct primes and $\alpha_i \geq 1$ for all i. Since
$$\exp(G) = \operatorname{lcm}\{\operatorname{ord}(a) : a \in G\},$$
there exists $h_1 \in G$ such that $p_1^{\alpha_1} | \operatorname{ord}(h_1)$. So $\operatorname{ord}(h_1) = p_1^{\alpha_1} q_1$ where $q_1 | p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Let $g_1 = h_1^{q_1}$. For each $m \geq 1$, we have $g_1^m = h_1^{mq_1}$, and
$$h_1^{mq_1} = 1 \iff p_1^{\alpha_1} q_1 | m q_1 \iff p_1^{\alpha_1} | m.$$
Hence $\operatorname{ord}(g_1) = p_1^{\alpha_1}$. Similarly for $i = 2, \dots, k$, we can find elements g_i of order $p_i^{\alpha_i}$. Let
$$a = g_1 g_2 \dots g_k$$
and $n = \operatorname{ord}(a)$. Now check as an exercise that $\operatorname{ord}(a) = \exp(G)$. This relies on
$$a^n = g_1^n g_2^n \dots g_k^n = 1,$$
which uses the assumption that G is abelian. □

Remark. The previous example shows that the abelian condition in this theorem is necessary.

Corollary 8.1.1. *If G is a finite abelian group with $\exp(G) = |G|$, then G is cyclic.*

Theorem 8.2. *The group of units $\mathrm{GF}(p^n)^*$ of a Galois field is cyclic.*

Proof. Let $e = \exp(\mathrm{GF}(p^n)^*)$. Then $a^e = 1$ for all $a \in \mathrm{GF}(p^n)^*$, so every element $a \in \mathrm{GF}(p^n)^*$ is a root of $X^e - 1$. Since $X^e - 1$ has at most e roots, we see that $|\mathrm{GF}(p^n)^*| \leq e$. But $e \leq |\mathrm{GF}(p^n)^*|$ since $\exp(\mathrm{GF}(p^n)^*)$ divides $|\mathrm{GF}(p^n)^*|$. Hence $|\mathrm{GF}(p^n)^*| = e$, so by Corollary 8.1.1, $\mathrm{GF}(p^n)^*$ is cyclic. □

8.3 Automorphisms of Fields

Example 8.1.3. The complex conjugation $f : \mathbb{C} \to \mathbb{C}$ given by $f(a + bi) = a - bi$ is an automorphism of $\mathbb{C}$. Observe that $f(c) = c$ if and only if $c \in \mathbb{R}$.

Theorem 8.3. *Let K be a field. The set $\operatorname{Aut} K$ of automorphisms of K forms a group under composition.*

Proof. First observe that composition is associative. The identity element in $\operatorname{Aut} K$ is the identity map id_K. For inverses, let $\alpha \in \operatorname{Aut} K$. Since α is a bijection, there exists an inverse map $\alpha^{-1} : K \to K$, where $\alpha^{-1}(x)$ is the unique element s such that $\alpha(s) = x$. Now we check that α^{-1} is also a homomorphism. For this, let $x, y \in K$ and suppose that $\alpha^{-1}(x) = s$ and $\alpha^{-1}(y) = t$. Then $\alpha(s) = x$ and $\alpha(t) = y$, so
$$\alpha(s + t) = \alpha(s) + \alpha(t) = x + y$$
since α is a homomorphism. Then we see that
$$\alpha^{-1}(x + y) = s + t = \alpha^{-1}(x) + \alpha^{-1}(y).$$
Similarly, $\alpha(st) = xy$, so
$$\alpha^{-1}(xy) = st = \alpha^{-1}(x)\alpha^{-1}(y).$$
Hence $\alpha^{-1} \in \operatorname{Aut} K$ and $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \mathrm{id}_K$, so $\operatorname{Aut} K$ is indeed a group. □

Definition 8.2. We call $\operatorname{Aut} K$ the *group of automorphisms* of K.

Definition 8.3. Let L be a field extension of K. A *K-automorphism* is an automorphism $\alpha : L \to L$ such that $\alpha(x) = x$ for all $x \in K$. The *Galois group* of L over K, denoted $\operatorname{Gal}(L : K)$, is the set of K-automorphisms of L. The *Galois group* $\operatorname{Gal}(f)$ of a polynomial $f \in K[X]$ is $\operatorname{Gal}(L : K)$ where L is a splitting field of f over K.

Theorem 8.4. *The Galois group* $\operatorname{Gal}(L : K)$ *is a subgroup of* $\operatorname{Aut} L$.

Proof. Clearly $\mathrm{id}_L \in \operatorname{Gal}(L : K)$ since it fixes all elements of L. Now let $\alpha, \beta \in \operatorname{Gal}(L : K)$. Then we have $\alpha(x) = x$ and $\beta(x) = x$ for all $x \in K$. Then $\beta^{-1}(x) = x$, which gives

$$\alpha\beta^{-1}(x) = \alpha(x) = x,$$

so $\alpha\beta^{-1} \in \operatorname{Gal}(L : K)$. Thus $\operatorname{Gal}(L : K)$ is a subgroup of $\operatorname{Aut} L$. $\square$

Remark. The big idea here is that there is a correspondence between subfields E with $K \subseteq E \subseteq L$ and subgroups H of $\operatorname{Gal}(L : K)$.

Exercise 8.2. From a past homework, we identified the subfields of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ as:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{3}, \sqrt{5}) & \\
\mathbb{Q}(\sqrt{3}) \arrow[ur] & \mathbb{Q}(\sqrt{5}) \arrow[u] & \mathbb{Q}(\sqrt{15}) \arrow[ul] \\
& \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Compare the subgroups of $\operatorname{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q})$ to the subfields of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ containing $\mathbb{Q}$.

Lecture 9

Feb. 7 — The Galois Correspondence

9.1 Automorphisms of Fields

Example 9.0.1. The complex conjugation $\beta : \mathbb{C} \to \mathbb{C}$ given by $\beta(a+bi) = a - bi$ is a nontrivial element of the Galois group of $\mathbb{C} : \mathbb{R}$. In fact, $\mathrm{Gal}(\mathbb{C} : \mathbb{R}) = \{\mathrm{id}, \beta\}$. Note that β fixes $\mathbb{R}$, id fixes $\mathbb{C}$, and

$$\begin{array}{c} \mathbb{C} \\ \uparrow \\ \mathbb{R} \end{array}$$

9.2 The Galois Correspondence

Definition 9.1. Define

$$\begin{aligned} \Gamma(E) &= \{\alpha \in \mathrm{Aut}\, L : \alpha(z) = z \text{ for all } z \in E\}, \\ \Phi(H) &= \{x \in L : \alpha(x) = x \text{ for all } \alpha \in H\}, \end{aligned}$$

where E is a subfield of L and H is a subgroup of $\mathrm{Gal}(L : K)$. This is called the *Galois correspondence*.

Example 9.1.1. In the previous example of $\mathbb{C} : \mathbb{R}$, we have $\Gamma(\mathbb{C}) = \{\mathrm{id}\}$ and $\Gamma(\mathbb{R}) = \{\mathrm{id}, \beta\}$. We also have $\Phi(\{\mathrm{id}, \beta\}) = \mathbb{R}$ and $\Phi(\{\mathrm{id}\}) = \mathbb{C}$.

Remark. The goal is to determine: When are Γ and Φ inverses of one another?

Theorem 9.1. *We have the following:*

1. *For every subfield E of L containing K, $\Gamma(E)$ is a subgroup of $\mathrm{Gal}(L : K)$.*
2. *Conversely, for every subgroup H of $\mathrm{Gal}(L : K)$, $\Phi(H)$ is a subfield of L containing K.*

Proof. See Howie. □

Theorem 9.2. *Let $z \in L \setminus K$. If z is a root of $f \in K[X]$ and $\alpha \in \mathrm{Gal}(L : K)$, then $\alpha(z)$ is also a root of f.*

Proof. Let $f = a_0 + a_1 X + \cdots + a_n X^n$, where $a_i \in K$. Then since α fixes each $a_i \in K$, we have

$$\begin{aligned} f(\alpha(z)) = a_0 + a_1\alpha(z) + \cdots + a_n(\alpha(z))^n &= \alpha(a_0) + \alpha(a_1)\alpha(z) + \cdots + \alpha(a_n)(\alpha(z))^n \\ &= \alpha(a_0 + a_1 z + \cdots + a_n z^n) = \alpha(0) = 0, \end{aligned}$$

which completes the proof. □

Example 9.1.2. Recall this example from homework:

$$\begin{tikzcd}
 & L = \mathbb{Q}(\sqrt{3}, \sqrt{5}) & \\
\mathbb{Q}(\sqrt{3}) \arrow[ur] & \mathbb{Q}(\sqrt{5}) \arrow[u] & \mathbb{Q}(\sqrt{15}) \arrow[ul] \\
 & K = \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

A basis for L over K is $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$. Since $\sqrt{3}$ is a root of $X^2 - 3$, by the previous theorem, any element in $\mathrm{Gal}(L : K)$ must send $\sqrt{3} \mapsto \pm\sqrt{3}$. Similarly, any element must send $\sqrt{5} \mapsto \pm\sqrt{5}$. So the $\mathbb{Q}$-isomorphisms of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ are

$$\begin{aligned}
\alpha(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}, \\
\beta(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a + b\sqrt{3} - c\sqrt{5} - d\sqrt{15}, \\
\gamma(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}, \\
\mathrm{id}(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) &= a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}.
\end{aligned}$$

We can write the multiplication table for this group as:

$\times$	id	α	β	γ
id	id	α	β	γ
α	α	id	γ	β
β	β	γ	id	α
γ	γ	β	α	id

The proper subgroups are $H_1 = \{\mathrm{id}, \alpha\}$, $H_2 = \{\mathrm{id}, \beta\}$, and $H_3 = \{\mathrm{id}, \gamma\}$. Also $\{\mathrm{id}\}$ and $G = \{\mathrm{id}, \alpha, \beta, \gamma\}$ are subgroups. Then

$$\Phi(H_1) = \mathbb{Q}(\sqrt{5}), \quad \Phi(H_2) = \mathbb{Q}(\sqrt{3}), \quad \Phi(H_3) = \mathbb{Q}(\sqrt{15}),$$
$$\Phi(\{\mathrm{id}\}) = \mathbb{Q}(\sqrt{3}, \sqrt{5}), \quad \Phi(G) = \mathbb{Q}.$$

Under Φ, this gives the diagram:

$$\begin{tikzcd}
 & G & \\
H_2 \arrow[ur] & H_1 \arrow[u] & H_3 \arrow[ul] \\
 & \{\mathrm{id}\} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}
\longrightarrow
\begin{tikzcd}
 & \Phi(G) = \mathbb{Q} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr] & \mathbb{Q}(\sqrt{5}) \arrow[d] & \mathbb{Q}(\sqrt{15}) \arrow[dl] \\
 & \Phi(\{\mathrm{id}\}) = \mathbb{Q}(\sqrt{3}, \sqrt{5}) &
\end{tikzcd}$$

Also note that $\Gamma(\mathbb{Q}(\sqrt{3})) = \{\mathrm{id}, \alpha\}$ since

$$\alpha(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}.$$

Exercise 9.1. Show that Γ is the inverse of Φ in the previous example.

Theorem 9.3. *Let $L : K$ be a field extension. Then*

1. *If E_1, E_2 are two subfields of L containing K, then $E_1 \subseteq E_2$ implies $\Gamma(E_1) \supseteq \Gamma(E_2)$.*
2. *If H_1, H_2 are subgroups of $\mathrm{Gal}(L : K)$, then $H_1 \subseteq H_2$ implies $\Phi(H_1) \supseteq \Phi(H_2)$.*

Proof. (1) Suppose $E_1 \subseteq E_2$ and $\alpha \in \Gamma(E_2)$. Then α fixes every element in E_2, so since $E_1 \subseteq E_2$, α also fixes every element in E_1. Hence $\alpha \in \Gamma(E_1)$ by definition.

(2) Suppose $H_1 \subseteq H_2$ and let $z \in \Phi(H_2)$. Then $\alpha(z) = z$ for every $\alpha \in H_2$, and since $H_1 \subseteq H_2$, $\alpha(z) = z$ for every $\alpha \in H_1$ as well. Hence $z \in \Phi(H_1)$ by definition. □

Remark. Note that Γ and Φ are not always inverses of one another.

Example 9.1.3. Consider the extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. If $\alpha \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$, then

$$\alpha(\sqrt[3]{2})^3 = \alpha(2) = 2.$$

Since there is only one cube root of 2 in this field, we must have $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$. So $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{\mathrm{id}\}$. So Γ cannot be the inverse of Φ here since there are two subfields, namely $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}$. In particular,

$$\Gamma(\mathbb{Q}(\sqrt[3]{2})) = \Gamma(\mathbb{Q}) = \{\mathrm{id}\} \quad \text{and} \quad \Phi(\{\mathrm{id}\}) = \mathbb{Q}(\sqrt[3]{2}).$$

Theorem 9.4. *For any subfield E of L and subgroup H of $\mathrm{Gal}(L : K)$, we have*

1. *$E \subseteq \Phi(\Gamma(E))$*
2. *and $H \subseteq \Gamma(\Phi(H))$.*

Proof. (1) Let $z \in E$. Then $\Gamma(E)$ is the set of all automorphisms fixing every element of E, and so z is fixed by every element of $\Gamma(E)$. Hence $z \in \Phi(\Gamma(E))$.

(2) Let $\alpha \in H$. Then $\Phi(H)$ is the set of elements of L fixed by every element of H, and so α fixes every element of $\Phi(H)$. Hence $\alpha \in \Gamma(\Phi(H))$. □

Remark. Now the goal will be to find sufficient conditions for Γ and Φ to be inverses of one another.

9.3 Normal Extensions

Definition 9.2. A field extension $L : K$ is *normal* if every irreducible polynomial in $K[X]$ having at least one root in L splits completely over L.

Example 9.2.1. An nonexample is $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. This is not a normal extension since $X^3 - 2$ is irreducible and has a root in $\mathbb{Q}(\sqrt[3]{2})$, but does not split completely over $\mathbb{Q}(\sqrt[3]{2})$.

Remark. Is $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ normal?

Theorem 9.5. *A finite extension $L : K$ is normal if and only if it is a splitting field for some polynomial in $K[X]$.*

Proof. ($\Rightarrow$) Let L be a finite normal extension and $\{z_1, \ldots, z_n\}$ be a basis for $L : K$. let m_i be the minimal polynomial for z_i, and let

$$m = m_1 m_2 \ldots m_n.$$

Each m_i has at least one root z_i in L, hence m splits completely over L since L is normal. Since L is generated by $z_1, \ldots, z_n$, it is not possible for m to split over a proper subfield of L, hence L is a splitting field for m over K.

($\Leftarrow$) See Howie. Relies on the isomorphism $K(\alpha) \to K(\beta)$ for α, β roots of an irreducible polynomial f. We also need properties of degrees of field extensions. □

Corollary 9.5.1. *Let L be a normal extension of K and E a subfield of L containing K. Then every injective K-homomorphism $\varphi : E \to L$ can be extended to a K-automorphism φ^* of L.*

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, hook, "i"'] & L \\ L \arrow[ur, dashed, "\varphi^*"'] & \end{tikzcd}$$

Proof. By the theorem, there exists $f \in K[X]$ such that L is a splitting field for f over K. But L is also a splitting field for f over E and $\varphi(E)$. From here, a slight generalization of the proof of uniqueness of splitting fields gives the desired K-automorphism of L extending φ. □

Example 9.2.2. Let $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $K = \mathbb{Q}$, and $E = \mathbb{Q}(\sqrt{3})$. Define $\varphi : E \to L$ by

$$\varphi(a + b\sqrt{3}) = a - b\sqrt{3},$$

which is an injective K-homomorphism. We have the following diagram:

$$\begin{tikzcd} \mathbb{Q}(\sqrt{3}) \arrow[r, "\varphi"] \arrow[d, hook, "i"'] & \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\ \mathbb{Q}(\sqrt{3}, \sqrt{5}) \arrow[ur, dashed, "\varphi^*"'] & \end{tikzcd}$$

Then we can define

$$\varphi^*(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}$$

as an extension of φ. Note that we could have also defined

$$\varphi^*(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}) = a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}.$$

Remark. From the previous example we see that φ^* is not unique.

Lecture 10

Feb. 12 — Normal Closures

10.1 Normal Closures

Recall this theorem from last time:

> **Theorem 9.5.** A finite extension $L : K$ is normal if and only if it is a splitting field for some polynomial in $K[X]$.

A natural question to ask is: Can we always extend a finite extension to make it normal?

Definition 10.1. Let $L : K$ be a finite extension. A field N containing L is a *normal closure* of $L : K$ if

1. N is a normal extension of K,
2. and if E is a proper subfield of N containing L, then E is not a normal extension of K.

Theorem 10.1. *Let $L : K$ be a finite extension. Then*

1. *there exists a normal closure N of L over K,*
2. *and N is unique up to isomorphism.*

Proof. Let $\{z_1, \ldots, z_n\}$ be a basis for $L : K$. Since $L : K$ is finite, each z_i is algebraic over K, with say minimal polynomial $m_i \in K[X]$. Let

$$m = m_1 \ldots m_n,$$

and let N be the splitting field of m over L. Then N is also a splitting field of m over K, since L is generated over K by some of the roots of m in N. Hence N is a normal extension of K containing L.

To see that N is the smallest such field, suppose E is a subfield of N containing L, and suppose E is normal. For each m_i, E contains a root z_i, so the normality of E implies that E contains all the roots of m, so $E = N$. For uniqueness, see Howie. The proof relies on the uniqueness of splitting fields. $\square$

Definition 10.2. Let $K_1, \ldots, K_n$ be subfields of L. The *join* of $K_1, \ldots, K_n$, denoted

$$K_1 \vee K_2 \vee \cdots \vee K_n,$$

is the smallest subfield of L containing $K_1 \cup K_2 \cup \cdots \cup K_n$.

Remark. The smallest subfield of L containing $K_1 \cup K_2$ is $K_1 \vee K_2 = K_1(K_2) = K_2(K_1)$, similar to how the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q} \cup \{\sqrt{3}\}$ is $\mathbb{Q}(\sqrt{3})$.

Example 10.2.1. Let $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(e^{2\pi i/3}\cdot\sqrt[3]{2}) \subseteq \mathbb{C}$. Then $\mathbb{Q}(\sqrt[3]{2}) \vee \mathbb{Q}(e^{2\pi i/3}\cdot\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, since

$$e^{2\pi i/3}\cdot\sqrt[3]{2} = -\frac{\sqrt[3]{2}}{2} + \frac{i\sqrt{3}}{2}\sqrt[3]{2}.$$

Remark. In the above example, we have $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(e^{2\pi i/3}\cdot\sqrt[3]{2}) \cong \mathbb{Q}[X]/\langle X^3-2\rangle$.

Corollary 10.1.1. *Let $L : K$ be a finite extension, and N the normal closure of $L : K$. Then*

$$N = L_1 \vee L_2 \vee \cdots \vee L_k,$$

where $L_1, L_2, \ldots, L_k$ are subfields of N containing K isomorphic to L.

Proof. As in the previous proof, suppose $\{z_1, \ldots, z_n\}$ is a basis for $L : K$, so $L = K(z_1, \ldots, z_n)$, and m_i is a minimal polynomial for z_i, and N a splitting field for $m = m_1 \ldots m_n$ over K. Let z_i' be an arbitrary root of m_i. Since z_i and z_i' are both roots of m_i, there exists a K-isomorphism $\varphi : K(z_i) \to K(z_i')$, which by Corollary 9.5.1 implies there exists a K-automorphism $\varphi^* : N \to N$. We have that

$$z_i' \in \varphi^*(L) \cong L,$$

so every root of m_i is contained in a subfield $L' = \varphi^*(L)$ of N that contains K and is isomorphic to L, since φ^* is a K-automorphism. Since N is generated over K by the roots of m, it is generated by finitely many subfields containing K and isomorphic to L. □

Example 10.2.2. Find the normal closure of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Following the proof of the theorem,

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

is a basis of $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. The minimal polynomials of $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ are $X-1, X^3-2, X^3-4$, respectively. The splitting field of

$$(X-1)(X^3-2)(X^3-4)$$

over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, since

$$X^3-2 = (X-\sqrt[3]{2})(X-e^{2\pi i/3}\sqrt[3]{2})(X-e^{-2\pi i/3}\sqrt[3]{2})$$

and

$$X^3-4 = (X-\sqrt[3]{2}^2)(X-e^{2\pi i/3}\sqrt[3]{2}^2)(X-e^{-2\pi i/3}\sqrt[3]{2}^2).$$

So $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = L_1 \vee L_2 \vee L_3$, where $L_1 = \mathbb{Q}(\sqrt[3]{2})$, $L_2 = \mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, and $L_3 = \mathbb{Q}(e^{-2\pi i/3}\sqrt[3]{2})$, and

$$L_1 \cong L_2 \cong L_3 \cong \mathbb{Q}[X]/\langle X^3-2\rangle.$$

Theorem 10.2. *Let $L : K$ be a finite normal extension and E a subfield of L containing K. Then E is a normal extension of K if and only if every K-monomorphism of E into L is a K-automorphism of E.*

Proof. See Howie. □

Example 10.2.3. Consider $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$, which is not normal. The $\mathbb{Q}$-monomorphism $\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ given by

$$\varphi(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + be^{2\pi i/3}\sqrt[3]{2} + ce^{-2\pi i/3}\sqrt[3]{2}^2$$

is not an automorphism of $\mathbb{Q}(\sqrt[3]{2})$.

Example 10.2.4. Consider $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$, which is normal. The $\mathbb{Q}$-monomorphisms are id and

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

which are both $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2})$.

10.2 Separable Extensions

Definition 10.3. An irreducible polynomial $f \in K[X]$ is *separable* over K if it has no repeated roots over a splitting field. A polynomial $g \in K[X]$ is *separable* over K if its irreducible factors are separable over K. An algebraic element in $L : K$ is *separable* over K if its minimal polynomial is separable over K. An algebraic extension $L : K$ is *separable* if every $\alpha \in L$ is separable over K.

Remark. A polynomial like $(X-2)^2$ actually *is* separable over $\mathbb{Q}$ since its irreducible factors are $X - 2$ and $X - 2$, which are each separable.

Definition 10.4. A field K is *perfect* if every polynomial in $K[X]$ is separable over K.

Theorem 10.3. *We have the following:*

1. *Every field of characteristic* 0 *is perfect.*
2. *Every finite field is perfect.*

Proof. (1) It suffices to show that if $\operatorname{char} K = 0$, then any irreducible polynomial f is separable. Let

$$f = a_0 + a_1 X + \cdots + a_n X^n$$

for $n \geq 1$ and suppose f is not separable. Then f and Df have a non-constant common factor d. Since f is irreducible, d must be a constant multiple of f, and thus d cannot divide Df unless

$$Df = a_1 + 2a_2 X + \cdots + na_n X^{n-1}$$

is the zero polynomial, by comparing degrees. Then

$$a_1 = 2a_2 = \cdots = na_n = 0.$$

Since $\operatorname{char} K = 0$, this implies

$$a_1 = a_2 = \cdots = a_n = 0,$$

and so $f = a_0$, a constant polynomial.[1] Contradiction. Hence f is separable.

(2) The same argument as above implies the only possible inseparable irreducible polynomials are of the form[2]

$$f(X) = b_0 + b_1 X^p + b_2 X^{2p} \cdots + b_m X^{mp}.$$

Now Theorem 7.24 of Howie implies that if K is finite, such a polynomial is reducible. Hence every irreducible polynomial is separable, so K is perfect. See Howie for details. □

Remark. Recall that $\mathbb{Z}_p(X)$ is an example of an infinite field with characteristic p.

[1] Recall that an irreducible polynomial is by definition a non-unit.

[2] We can still conclude $ka_k = 0$ implies $a_k = 0$ when k is not a multiple of p.

Lecture 11

Feb. 21 — Galois Extensions

11.1 Example of an Inseparable Extension

Example 11.0.1. The field $K = \mathbb{Z}_p(X)$ is not perfect. Consider the polynomial

$$f = Y^p - X \in \mathbb{Z}_p(X)[Y],$$

which is irreducible. Now let L be a splitting field of f over K and α a root of f, i.e. $\alpha^p - X = 0$. Then

$$(Y - \alpha)^p = Y^p - \alpha^p = Y^p - X$$

by freshman exponentiation. In particular, α is a repeated root of f in L.

11.2 Galois Extensions

Definition 11.1. A *Galois extension* of K is a finite extension that is both normal and separable.

Remark. The main goal here is: For a Galois extension, Γ and Φ are inverses of one another.

Theorem 11.1. *Let $L : K$ be a separable extension of degree n. Then there are exactly n distinct K-monomorphisms of L into a normal closure N of L over K.*

Proof. Use strong induction on the degree of $L : K$. See Howie for details. □

Corollary 11.1.1. *If $L : K$ is Galois, then $|\mathrm{Gal}(L : K)| = [L : K]$.*

Proof. If $L : K$ is Galois, then $L : K$ is normal and separable. So the previous theorem applies, where L is its own normal closure. So we get exactly $[L : K]$ distinct K-monomorphisms of L into L, which are precisely the K-automorphisms of L and thus the elements of the Galois group. □

Example 11.1.1. The extension $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}$ is Galois with $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$. We could have

$$\sqrt[3]{2} \mapsto \sqrt[3]{2} \text{ or } e^{2\pi i/3}\sqrt[3]{2} \text{ or } e^{-2\pi i/3}\sqrt[3]{2} \quad \text{and} \quad i\sqrt{3} \mapsto i\sqrt{3} \text{ or } -i\sqrt{3}.$$

Combinining these options gives us 6 distinct maps, so these must in fact all be $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, since we know the Galois group has size 6. In fact, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}) \cong S_3 \cong D_3$.

Remark. The proper nontrivial subfields of $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ are $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, $\mathbb{Q}(e^{-2\pi i/3}\sqrt[3]{2})$, and $\mathbb{Q}(i\sqrt{3})$. Maybe draw a pretty diagram with this showing the Galois correspondence.

Exercise 11.1. Show that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Exercise 11.2. Show that $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Theorem 11.2. *Let $L : K$ be a finite extension. Then $\Phi(\mathrm{Gal}(L : K)) = K$ if and only if $L : K$ is normal and separable.*

Proof. ($\Leftarrow$) Let $[L : K] = n$. By Corollary 11.1.1, we have $|\mathrm{Gal}(L : K)| = n$. Let $K' = \Phi(\mathrm{Gal}(L : K))$. By definition, $K \subseteq K'$. By Theorem 7.12 of Howie, we find that

$$[L : K'] = |\mathrm{Gal}(L : K)|.$$

Hence $[L : K'] = [L : K]$ and thus we conclude that $K = K'$.

($\Rightarrow$) See Howie. □

Exercise 11.3. Show that if $K \subseteq K'$ and $[L : K'] = [L : K]$, then $K = K'$.

Theorem 11.3. *Let $L : K$ be Galois and E a subfield of L containing K. If $\delta \in \mathrm{Gal}(L : K)$, then*

$$\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}.$$

Proof. Next class, see Howie for now. □

Example 11.1.2. Consider $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}$. Define the elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q})$ by

$$\mu_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2},\ i\sqrt{3} \mapsto -i\sqrt{3}, \quad \mu_2 : \sqrt[3]{2} \mapsto e^{2\pi i/3}\sqrt[3]{2},\ i\sqrt{3} \mapsto -i\sqrt{3},$$
$$\mu_3 : \sqrt[3]{2} \mapsto e^{-2\pi i/3}\sqrt[3]{2},\ i\sqrt{3} \mapsto -i\sqrt{3},$$
$$\rho_1 : \sqrt[3]{2} \mapsto e^{2\pi i/3}\sqrt[3]{2},\ i\sqrt{3} \mapsto i\sqrt{3}, \quad \rho_2 : \sqrt[3]{2} \mapsto e^{-2\pi i/3}\sqrt[3]{2},\ i\sqrt{3} \mapsto i\sqrt{3}.$$

Let $\delta = \mu_3$ and $E = \mathbb{Q}(\sqrt[3]{2})$. Then $\delta(E) = \mathbb{Q}(e^{-2\pi i/3}\sqrt[3]{2})$ since $\mu_3(\sqrt[3]{2}) = e^{-2\pi i/3}\sqrt[3]{2}$. Now

$$\begin{aligned}\mu_2(e^{-2\pi i/3}\sqrt[3]{2}) &= \mu_2(e^{-2\pi i/3})\mu_2(\sqrt[3]{2}) = \mu_2(-\frac{1}{2} - i\frac{\sqrt{3}}{2})\mu_2(\sqrt[3]{2}) \\ &= (-\frac{1}{2} + i\frac{\sqrt{3}}{2})(e^{2\pi i/3}\sqrt[3]{2}) = e^{2\pi i/3}e^{2\pi i/3}\sqrt[3]{2} = e^{-2\pi i/3}\sqrt[3]{2},\end{aligned}$$

so $\Gamma(\delta(E)) = \{\mathrm{id}, \mu_2\}$. Also $\Gamma(E) = \{\mathrm{id}, \mu_1\}$, and we find that

$$\delta\Gamma(E)\delta^{-1} = \{\delta\mathrm{id}\delta^{-1}, \delta\mu_1\delta^{-1}\} = \{\mathrm{id}, \mu_3\mu_1\mu_3^{-1}\} = \{\mathrm{id}, \mu_2\},$$

so indeed we have $\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$ in this case.