Part II - Galois Theory

Lectured by Prof. A. J. Scholl

Artur Avameri

Michaelmas 2022

Contents

0 Introduction

06 Oct 2022, Lecture 1

Galois Theory begins with polynomial equations and trying to solve them. Galois discovered certain **symmetries** of equations, which led to symmetries of fields (Steinitz, Artin).

Babylonians were able to solve the quadratic equation X^2+bX+c thousands of years ago, and so can we - write it as $(X+b/2)^2+c-b^2/4$, which leads to the quadratic formula, or use Vieta's formulas to get $x_1x_2 = c, x_1+x_2 = -b$, from which we can solve for x_1 by doing $x_1 = \frac{1}{2}\left((x_1+x_2)+(x_1-x_2)\right)$ and $(x_1-x_2)^2 = (x_1+x_2)^2-4x_1x_2$.

A lot later people figured out how to solve the cubic equation, X^3+aX^2+bX+c. We get $x_1+x_2+x_3 = -a, x_1x_2+x_2x_3+x_3x_1 = b, x_1x_2x_3 = -c$. If we replace $X \mapsto X-a/3$, we end up with a cubic equation without a quadratic term. Now

$$x_1 = \frac{1}{3}\left[(x_1+x_2+x_3)+(x_1+\omega x_2+\omega^2 x_3)+(x_1+\omega^2 x_2+\omega x_3)\right]$$

for $\omega = e^{2\pi i/3}$ a cube root of unity. Let $u = (x_1+\omega x_2+\omega^2 x_3), v = (x_1+\omega^2 x_2+\omega x_3)$.

If we cyclically permute x_1, x_2, x_3, we find $u \mapsto \omega u \mapsto \omega^2 u$ and $v \mapsto \omega v \mapsto \omega^2 v$, so u^3 and v^3 are invariant under cyclic permutations of the roots. Hence u^3+v^3 and u^3v^3 are invariant under permutations of the roots, so (as we prove in the next lecture) we can express them in terms of the coefficients of the polynomial.

In fact, they're given by $u^3+v^3 = -27c, u^3v^3 = -27b^2$, hence u^3, v^3 are roots of $Y^2+27cY-27b^2$, from which we can find u, v and hence x_1. This is **Cardano's formula**.

If we proceed similarly for quartics, we end up with a cubic equation which we can solve as above. Unfortunately, this doesn't work for quintics. The reason for this lies in group theory.

1 Polynomials

In this course, all rings will be commutative, with a one, and nonzero. For a ring R, $R[X]$ is the ring of polynomials over R, i.e. just the formal expressions $\sum_{i=0}^{n} a_i X^i$ for $a_i \in R$.

A polynomial $f \in R[X]$ determines a **function** $R \to R$. However, the polynomial $r \mapsto f(r)$ isn't in general determined by the function. For example, if $R = \mathbb{Z}/p\mathbb{Z}$ for p a prime, then $\forall a \in R, a^p = a$, so the polynomials X^p and X represent the same function, while being different polynomials.

In the case where $R = K$ is a field, we know $K[X]$ is a Euclidean domain, so it has a division algorithm: if $f, g \in K[X]$ and g is nonzero, then there exist unique q, r such that $f = gq + r$ and $\deg(r) < \deg(g)$ (note that $\deg(0) = -\infty$). If $g = X - a$ is linear, then we get $f = (X - a)q + f(a)$, the **remainder theorem**.

$K[X]$ is also a PID and UFD, so every polynomial is a product of irreducible polynomials, and there are GCDs, which we can compute using Euclid's algorithm.

Proposition 1.1. If K is a field and $f \in K[x]$ is nonzero, then f has at most $\deg(f)$ roots in K.[1]

Proof. If f has no roots, we're done. Otherwise, let $f(a) = 0$ and write $f = (X - a)g$ with $\deg(g) = \deg(f) - 1$. But if b is a root of f, then $f(b) = 0 \implies b = a$ or $g(b) = 0$, so f has at most (1 + number of roots of g) roots and the claim follows by induction. □

2 Symmetric polynomials

Let R be a ring and consider $R[X_1, \ldots, X_n]$ for some $n \geq 1$.

Definition 2.1. A polynomial $f \in R[X_1, \ldots, X_n]$ is **symmetric** if for every permutation $\sigma \in S_n$, $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f$.

The set of symmetric polynomials is a subring of $R[X_1, \ldots, X_n]$.

Example 2.1. $X_1 + \ldots + X_n$, or more generally, $P_k = \sum_{i=1}^{n} X_i^k$ are symmetric polynomials.

Alternative definition:

Definition 2.2. If $f \in R[X_1, \ldots, X_n]$, define $f\sigma = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. This is a (right) action on the group S_n. We say f is **symmetric** if $f\sigma = f \ \forall \sigma \in S_n$.

[1] Note that this is not true if K is a ring.

The **elementary symmetric polynomials** are

$$s_r(X_1, \ldots, X_n) = \sum_{i_1 < \ldots < i_r} X_{i_1} \ldots X_{i_r}.$$

Example 2.2. For $n = 3$, $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$, $s_3 = X_1X_2X_3$.

Theorem 2.1. (i) Every symmetric polynomial over R can be expressed as a polynomial in $\{s_r \mid 1 \leq r \leq n\}$ with coefficients in R.

(ii) There are no non-trivial relations between $s_1, \ldots, s_n$ - they're independent.

08 Oct 2022, Lecture 2

Remarks.

(a) Consider the homomorphism

$$\theta : R[Y_1, \ldots, Y_n] \to R[X_1, \ldots, X_n]$$

by $\theta(Y_r) = S_r$ (and identity on R). Then (i) says that the image of θ is the set of symmetric polynomials, and (ii) says that θ is injective.

(b) An equivalent definition of the $\{s_r\}$ is

$$\prod_{i=1}^{n}(T + x_i) = T_n + s_1T^{n-1} + \ldots + s_{n-1}T + s_n.$$

(c) If we need to specify the number of variables, we write $s_{r,n}$ instead of s_r.

Proof of Theorem 2.1. Terminology:

- A **monomial** is some $X_I = X_1^{i_1} \ldots X_n^{i_n}$ for some $I \in \mathbb{Z}^n_{\geq 0}$.
- Its **(total) degree** is $\sum i_\alpha$.
- A **term** β is some $cX_I, 0 \neq c \in R$, so a polynomial is uniquely a sum of terms.
- The total degree of f is the maximal degree of any of the terms.

Define a lexicographical ordering on monomials X_I as follows: $X_I > X_J$ if either $i_1 > j_1$ or for some $1 \leq r < n$, $i_1 = j_1, \ldots, i_r = j_r$ and $i_{r+1} > j_{r+1}$. This is a **total ordering**: for each pair $I \neq J$, exactly one of $X_I > X_J$ or $X_J > X_i$ holds.

Existence: Let d be the total degree of some symmetric polynomial f and let X_I be the lexicographically largest monomial in f with coefficient $c \in R$. As f is symmetric, we must have $i_1 \geq i_2 \geq \ldots \geq i_n$ (if not, say $i_r < i_{r+1}$, then

exchanging X_r and X_{r+1} gives a monomial occuring in f which is bigger than X_I). So

$$X_I = X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\dots(X_1\dots X_n)^{i_n}.$$

Consider $g = s_1^{i_1-i_2}s_2^{i_2-i_3}\dots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$. The leading monomial (i.e. largest in lexicographical order) of g is X_I, and g is symmetric, so $f-cg$ is also symmetric, of total degree $\leq d$, and its leading term is smaller (lexicographically) than X_I. As the set of monomials of degree $\leq d$ is finite, this process terminates.

Uniqueness: By induction on n. Say $G \in R[Y_1,\dots,Y_n]$ with

$$G(s_{n,1},\dots,s_{n,n}) = 0.$$

We want to show $G = 0$. If $n = 1$, this is trivial ($s_{1,1} = X_1$). If $G = Y_n^k H$ with $Y_n \nmid H$, then $s_{n.n}^k H(s_{n,1},\dots,s_{n,n}) = 0$. As $s_{n,n} = X_1\dots X_n$, $s_{n,n}$ is not a zero divisor in $R[X_1,\dots,X_n]$, hence $H(s_{1,n},\dots,s_{n,n}) = 0$. So we may assume WLOG that G is not divisible by Y_n.

Replace X_n by 0. Then

$$s_{n,r}(X_1,\dots,X_{n-1},0) = \begin{cases} s_{n-1,r}(X_1,\dots,X_{n-1}) & \text{if } r < n \\ 0 & \text{if } r = n \end{cases}$$

and so $G(s_{n-1,1},\dots,s_{n-1,n-1},0) = 0$. So by induction, $G(Y_1,\dots,Y_{n-1},0) = 0$, so $Y_n \mid G$, contradiction and we're done. □

Example 2.3. Say $f = \sum_{i\neq j} X_i^2X_j$ for some $n \geq 3$. Its leading term is $X_1^2X_2 = X_1(X_1X_2)$. Then

$$s_1s_2 = \sum_i \sum_{j<k} X_iX_jX_k = \sum_{i\neq j} X_i^2X_j + 3\sum_{i<j<k} X_iX_jX_k.$$

So $f = s_1s_2 - 3s_3$.

Computing, say $\sum X_i^5$ by hand is tedious. But there are formulae for this! Recall $p_k = \sum_{i=1}^n X_i^k$.

Theorem 2.2 (Newton's formulae)**.** Let $n \geq 1$. Then $\forall k \geq 1$,

$$p_k - s_1p_{k-1} + \dots + (-1)^{k-1}s_{k-1}p_1 + (-1)^k k s_k = 0.$$

(By convention, $s_0 = 1$ and $s_r = 0$ if $r > n$).

Proof. We may assume $R = \mathbb{Z}$. Consider the generating function

$$F(T) = \prod_{i=1}^n (1 - X_iT) = \sum_{r=0}^n (-1)^r s_r T^r.$$

Take the logarithmic derivative w.r.t T, i.e.

$$\frac{F'(T)}{F(T)} = \sum_{i=1}^{n} \frac{-X_i}{1 - X_i T} = -\frac{1}{T} \sum_{i=1}^{n} \sum_{r=1}^{\infty} X_i^r T^r = -\frac{1}{T} \sum_{r=1}^{\infty} p_r T^r.$$

Thus $-TF'(T) = s_1 T - 2s_2 T^2 + \ldots + (-1)^{n-1} n s_n T^n$ from our generating function above, but we also have (from the previous line) that

$$-TF'(T) = F(T) \sum_{r=1}^{\infty} p_r T^r = (s_0 - s_1 T + \ldots + (-1)^n s_n T^n)(p_1 T + p_2 T^2 + \ldots).$$

Comparing coefficients of T^k gives the identity. □

The **discriminant** polynomial is $D(X_1, \ldots, X_n) = \Delta(X_1, \ldots, X_n)^2$ where $\Delta = \prod_{i<j}(X_i - X_j)$. (Recall from IA Groups that applying $\sigma \in S_n$ to Δ multiplies Δ by $\mathrm{sgn}(\sigma)$). So D is symmetric. So $D(X_1, \ldots, X_n) = d(s_1, \ldots, s_n)$ for some polynomial d (with coefficients in $\mathbb{Z}$).

Example 2.4. If $n = 2$, then $D = (X_1 - X_2)^2 = s_1^2 - 4s_2$.

Definition 2.3. Let $f = T^n + \sum_{i=0}^{n-1} a_{n-i} T^i \in R[T]$ be monic. Then its **discriminant** is $\mathrm{Disc}(f) = d(-a_1, a_2, -a_3, \ldots, (-1)^n a_n) \in R$.

Observe that if $f = \prod_{i=1}^{n}(T - x_i), x_i \in R$, then $a_r = (-1)^r s_r(x_1, \ldots, x_n)$, so $\mathrm{Disc}(f) = \prod_{i<j}(x_i - x_j)^2 = D(x_1, \ldots, x_n)$. If moreover $R = K$ is a field, then $\mathrm{Disc}(f) = 0$ if and only if f has a repeated root (i.e. $x_i = x_j$ for some $i \neq j$).

Example 2.5. $\mathrm{Disc}(T^2 + bT + c) = b^2 - 4c$.

11 Oct 2022, Lecture 3

3 Fields

Recall that a **field** is a ring K (commutative, nonzero, with a 1) in which every nonzero element has a multiplicative inverse. The set of nonzero elements of K is then a **group** K^* (or $K^\times$), called the multiplicative group of K.

The **characteristic** of K is the least positive integer p (if it exists) such that $p \cdot 1_K = 0_K$, or 0 if no such p exists. For example, $\mathbb{Q}$ has characteristic 0, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p.

The characteristic $\mathrm{char}(K)$ of K is always either 0 or prime. Inside K, there is a smallest subfield, called the **prime subfield** of K, which is either isomorphic to $\mathbb{Q}$ (if $\mathrm{char}(K) = 0$) or to $\mathbb{F}_p$ (if $\mathrm{char}(K) = p$).

Proposition 3.1. Let $\phi : K \to L$ be a homomorphism of fields. Then ϕ is an injection.

Proof. $\phi(1_K) = 1_L \neq 0_L$, so $\ker(\phi) \subset K$ is a proper ideal of K, so $\ker(\phi) = (0)$. □

Definition 3.1. Let $K \subset L$ be fields (where the field operations on K are the same as those in L). We say K is a **subfield** of L, and L is an **extension** of K, denoted L/K, "L over K".

Remarks. (i) This has nothing to do with quotients.

(ii): It is useful to be more general - if $i : K \to L$ is a homomorphism of fields, then by Prop 3.1 i is an isomorphism of K and the subfield $i(K) \subset L$. In this situation, we also say that "L is an extension of K".

Example 3.1. We have extensions $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}/\mathbb{Q}$.

Notation/definition. Suppose we have two field $K \subset L$ and $x \in L$. Define $K[x] = \{p(x) \mid p \in K[T]\}$, the set of polynomials in x. This is a **subring** of L.

We also define $K(x) = \{\frac{p(x)}{q(x)} \mid p, q \in K[T], q(x) \neq 0\}$. This is a **subfield** of L (read "K adjoin x").

For $x_1, \ldots, x_n \in L$, similarly define

$$K(x_1, \ldots, x_n) = \left\{ \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \mid p, q \in K[T_1, \ldots, T_n, q(x) \neq 0 \right\}.$$

We can check that $K(x_1, \ldots, x_{n-1})(x_n) = K(x_1, \ldots, x_n)$, and likewise for $K[x_1, \ldots, x_n]$.

If we have L/K a field extension, then L is naturally a vector space over its subfield K (just forget multiplication by elements of L). We can ask whether this is a **finite-dimensional** vector space.

- If so, we say L/K is a **finite extension** and write $[L : K] = \dim_K(L)$ for the dimension. We call this the **degree** of the extension.
- If not, write $[L : K] = \infty$.

$\dim_K$ is the dimension as a K-vector space. Since L is a vector space over L, we have $\dim_L(L) = 1$. As a K-vecor space, $L \cong K^{[L:K]}$.

Example 3.2. (i) $\mathbb{C}/\mathbb{R}$ is a finite extension with $[\mathbb{C} : \mathbb{R}] = 2$.

(ii) Let K be any field, $K(X)$ the field of rational functions in X, i.e. the field of fractions of the polynomial ring $K[X]$. Then $[K(X) : K] = \infty$ since $1, x, x^2, \ldots$ are linearly independent.

(iii) $[\mathbb{R} : \mathbb{Q}] = \infty$ (use countability: every finite dimensional $\mathbb{Q}$-vector space is countable).

This course is largely about preperties (and symmetries) of **finite** field extensions.

Definition 3.2. We say an extension L/K is **quadratic** if $[L : K] = 2$. Similarly for **cubic**, etc.

Proposition 3.2. Suppose K is a **finite** field (necessarily of characteristic $p > 0$). Then the number of elements of K is a power of p.

Proof. Certainly $K/\mathbb{F}_p$ is finite, so $K \cong (\mathbb{F}_p)^n$ for $n = [K : \mathbb{F}_p]$, so $|K| = p^n$. □

Later we will show that for any prime power $q = p^n$ there exists a finite field $\mathbb{F}_q$ with q elements. We have $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, but $\mathbb{F}_{p^n} \neq \mathbb{Z}/p^n\mathbb{Z}$ if $n > 1$.

A simple, yet powerful fact:

Theorem 3.3 (Tower law)**.** Suppose we have two field extensions M/L and L/K. Then M/K is a finite extension if and only if both M/L and L/K are finite, and if so, then

$$[M : K] = [M : L][L : K].$$

In fact, a slightly more general statement by taking $V = M$ in the above:

Theorem 3.4. Let L/K be a field extension, V a L-vector space. Then

$$\dim_K V = [L : K] \cdot \dim_L V$$

(with the obvious meaning if any of these are infinite).

Example 3.3. $V = \mathbb{C}^n = \mathbb{R}^{2n}$.

Proof. Let $\dim_L V = d < \infty$. Then $V \cong L \oplus \ldots \oplus L = L^d$ as a L-vector space, so also certainly as a K-vector space. If $[L : K] = n < \infty$, then $L \cong K^n$ as a K-vector space, so $V = K^n \oplus \ldots \oplus K^n = K^{nd}$, so $\dim_K V = [L : K] \cdot \dim_L V$.

If V is finite-dimensional over K, then a K-basis for V certainly spans V over L. So if $\dim_L V = \infty$, then $\dim_K V = \infty$. Likewise, if $[L : K] = \infty$ and $V \neq \emptyset$, then V has a infinite linearly independent subst, so $\dim_K V = \infty$. □

Another important fact:

Proposition 3.5. (i) Let K be a field and $G \subset K^\times$ a **finite** subgroup. Then G is **cyclic**.

(ii) If K is finite, then $K^\times$ is cyclic.

Proof. (i): Write $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ as a product of cyclic groups such that $1 < m_1 \mid m_2 \mid \ldots \mid m_k = m$ (by GRM). So $\forall x \in G, x^m = 1$. As K is a field, the polynomial $T^m - 1$ has at most m roots. So $|G| \leq m$, so $k = 1$, and hence G is cyclic.

(ii) is now obvious. □

Remark. If $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the above says $\exists a \in \{1, \dots, p-1\}$ such that $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup \{a, a^2, \dots, a^{p-1} \pmod p\}$. This a is called a **primitive root** mod p.

13 Oct 2022, Lecture 4

Proposition 3.6. Let R be a ring and p a prime such that $p1_R = 0_R$ (e.g. R is a field of characteristic p). Then the map

$$\phi_p : R \to R \text{ by } \phi_p(x) = x^p$$

is a **homomorphism** from R to itself, called the **Frobenius endomorphism** of R.

Proof. We have to show that $\phi_q(1) = 1, \phi_p(xy) = \phi_p(x)\phi_p(y)$ and $\phi_p(x+y) = \phi_p(x) + \phi_p(y)$. But the first two are obvious, and for the last one we get

$$\phi_p(x+y) = (x+y)^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p = x^p + y^p,$$

where all the terms $\binom{p}{i}$ are divisible by p as p is a prime. □

Remark. This is a very important map. For example, this gives another proof of Fermat's little theorem $x^p \equiv x \pmod p$: induction on x and $(x+1)^p \equiv x^p + 1 \pmod p$.

4 Algebraic elements and extensions

Let L/K be an extension and $x \in L$.

Definition 4.1. x is **algebraic** over K if $\exists$ a nonzero polynomial $f \in K[T]$ such that $f(x) = 0$. If x is not algebraic, we say it is **transcendental over** K.

Suppose $f \in K[T]$ with evaluation $f(x) \in L$. This gives a map

$$\mathrm{ev}_x : K[T] \to L, f \mapsto f(x),$$

which is obviously a homomorphism of rings.

$I = \ker(\mathrm{ev}_x) \subset K[T]$ is an ideal ($= \{f \mid f(x) = 0\}$). As $\mathrm{Im}(\mathrm{ev}_x)$ is a subring of L, it is an integral domain. So I is a **prime** ideal, so there are two possibilities:

(i) $I = \{0\} \implies$ the only f with $f(x) = 0$ is $f = 0$, so x is transcendental over K.

(ii) $I \neq \{0\}$. AS $K[T]$ is a PID, there exists a unique monic irreducible $g \in K[T]$ such that $I = (g)$. So $f(x) = 0 \iff f$ is a multiple of g.

So x is algebraic over K and we call g the **minimal polynomial** of x over K, which we might write as $m_{x,K}$. It is the unique irreducible monic polynomial with x as a root (and is the monic polynomial of least degree with x as a root - this depends on K as well as x).

Some examples:

- $x \in K$, $m_{x,K} = T - x$.
- p a prime, $d \geq 1$. Then $T^d - p \in \mathbb{Q}[T]$ is irreducible by Eisenstein's criterion, so it is the min. poly. of $\sqrt[d]{p} = x$ over $\mathbb{Q}$.
- $z = e^{2\pi i/p}$ for p a prime is a root of $T^p - 1$ and

$$\frac{T^p - 1}{T - 1} = g(T) = T^{p-1} + \ldots + T + 1 \in \mathbb{Q}[T].$$

  As $g(T+1) = \frac{(T+1)^p - 1}{T} = T^{p-1} + \binom{p}{1}T^{p-2} + \ldots + pT + p$, this is also irreducible by Eisenstein and hence g is the min. poly. of z over $\mathbb{Q}$.

Terminology. We say **the degree of x over K** (where x is algebraic over K) is the degree of $m_{x,K}$, written $\deg_K(x)$ or $\deg(x/K)$.

A ring/field-theoretic characterization of the notion of being algebraic:

Proposition 4.1. Let $L/K, x \in L$. The following are equivalent:

(i) x is algebraic over K.

(ii) $[K(x) : K] < \infty$.

(iii) $\dim_K K[x] < \infty$.

(iv) $K[x] = K(x)$.

(v) $K[x]$ is a field.

If these hold, then $\deg_K(x) = [K(x) : K]$.

Recall $K[X] = \{p(x)\}$ and $K(x) = \{\frac{p(x)}{q(x)} \mid q(x) \neq 0\}$ for $p, q \in K[T]$. The most important results here are (i) $\iff$ (ii) and the degree formula. (This is a part of a series of results relating properties of x and $K(x)$).

Proof. (ii) $\implies$ (iii) and (iv) $\iff$ (v) are trivial.

(iii) $\implies$ (iv) and (ii): Let $0 \neq y = g(x) \in K[x]$. Consider $K[x] \to K[x]$ by $z \mapsto yz$. It is a K-linear transformation, it is injective as $y \neq 0$. As $\dim_K K[X] < \infty$, it is bijective. So $\exists$ s.t. $yz = 1$. So $K[x]$ is a field, equal to $K(x)$, and $[K(x) : K]$ is finite-dimensional.

(v) $\implies$ (i): WLOG $x \neq 0$, then $x^{-1} = a_0 + a_1 x + \ldots + a_n x^n \in K[X]$ for a_i not all equal to 0, so $a_n x^{n+1} + \ldots + a_0 x - 1 = 0$, so x is algebraic over K.

(i) $\implies$ (iii) and the degree formula: The image of $\mathrm{ev}_x : K[T] \to L$ is $K[X] \subset L$. x is algebraic over $K \implies \ker(\mathrm{ev}_x) = (m_{x,K})$ is a maximal ideal (GRM, because m is irreducible), so by the first isomorphism theorem, $K[T]/(m_{x,K}) \cong K[x]$. The LHS is a field, so $K[X]$ is a field. $m_{x,K}$ is monic of degree $d = \deg_K(x)$, so $K[T]/(m_{x,K})$ has a K-basis $1, T, \ldots, T^{d-1}$. Hence $\dim_K K[x] = d < \infty$ (this gives (iii)) and so $[K(x) : K] = d$ as well. □

Corollary 4.2. (i) The elements $x_1, \ldots, x_n$ are all algebraic over K if and only if $L = K(x_1, \ldots, x_n)$ is a finite extension of K. If so, then **every** element of L is algebraic over K.

(ii) If x, y are algebraic over K, then so are $x + y$, xy, and $1/x$ (if $x \neq 0$).

(iii) Let L/K be any extension. Then $\{x \in L \mid x \text{ algebraic over } K\}$ is a subfield of L.

Proof. (i) If x_n is algebraic over K, it is certainly algebraic over $K(x_1, \ldots, x_{n-1})$, so $[L : K(x_1, \ldots, x_{n-1})] < \infty$. So by tower law and induction on n, $[L : K] < \infty$. Conversely, if $[L : K] < \infty$, then the subfield $K(y)$ is finite over K for all y in L. So y is algebraic over K by the previous proposition.

(ii) $x \pm y, xy, \frac{1}{x} \in K(x, y)$, so by (i), every element of this field is algebraic.

(iii) This clearly follows from (ii).

□

Remark. The key ingredient here is the tower law.

15 Oct 2022, Lecture 5

Example 4.1. We saw earlier that $z = e^{2\pi i/p}$ for p an odd prime has min. poly. of degree $p - 1$.

Consider now $x = 2\cos\frac{2\pi}{p} = z + z^{-1} \in \mathbb{Q}(z)$ (so x is algebraic over $\mathbb{Q}$).

We have $\mathbb{Q}(z) \supset \mathbb{Q}(x) \supset \mathbb{Q}$, and $z^2 - xz + 1 = 0$. So $\deg_{\mathbb{Q}(x)}(z) \leq 2$, and we know $[\mathbb{Q}(z) : \mathbb{Q}] = p - 1$, so $[\mathbb{Q}(z) : \mathbb{Q}(x)]$ is either 1 or 2.

But $z \notin \mathbb{Q}(x) \subset \mathbb{R}$, so $[\mathbb{Q}(z) : \mathbb{Q}(x)] = 2$ and hence $\deg_{\mathbb{Q}}(x) = \frac{p-1}{2}$.

To actually find this polynomial, write

$$z^{\frac{p-1}{2}} + z^{\frac{p-3}{2}} + \ldots + z^{\frac{-(p-1)}{2}} = 0,$$

which remains unchanged under $z \mapsto \frac{1}{z}$, and hence we can express the above polynomial in terms of $z + \frac{1}{z} = x$ as a polynomial of degree $\frac{p-1}{2}$.

Example 4.2. $x = \sqrt{m} + \sqrt{n}$ for $m, n \in \mathbb{Z}$, m, n, mn not squares. We have

$$n = (x - \sqrt{m})^2 \overset{\star}{=} x^2 - 2\sqrt{m}x + m,$$

so $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{m})] \leq 2$. Similarly, $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{n})] \leq 2$. Also note that $\star$ implies that $\sqrt{m} \in \mathbb{Q}(x)$.

So (by the tower law), either $[\mathbb{Q}(x) : \mathbb{Q}] = 4$, or $[\mathbb{Q}(x) : \mathbb{Q}] = 2$ and $\mathbb{Q}(x) = \mathbb{Q}(m) = \mathbb{Q}(n)$ (since m, n not squares implies $[\mathbb{Q}(m) : \mathbb{Q}] = [\mathbb{Q}(n) : \mathbb{Q}] = 2$). But then $\mathbb{Q}(m) = \mathbb{Q}(n) \implies \sqrt{m} = a + b\sqrt{n}$ for $a, b \in \mathbb{Q} \implies m = a^2 + b^2 n + 2ab\sqrt{n}$. So $ab = 0$, whence either $b = 0$, so $m = a^2$ is a square, or $a = 0$, so $mn = b^2 n^2$ is a square. This forces $[\mathbb{Q}(x) : \mathbb{Q}] = 4$.

Definition 4.2. An extension $[L : K]$ is **algebraic** if every $x \in L$ is algebraic over K.

Proposition 4.3. (i) Finite extensions are algebraic.

(ii) $K(x)$ is algebraic over K if and only if x is algebraic over K.

(iii) If $M/L/K$, then M/K is algebraic if and only if both M/L and L/K are algebraic.

Proof. (i) $[L : K] < \infty \implies \forall x \in L, [K(x) : K] < \infty \implies x$ is algebraic over K.

(ii) $\implies$ follows by definition, $\impliedby$ follows by (i).

(iii) Assume M/K is algebraic. Then $\forall x \in M$, x is algebraic over K, so it is certainly algebraic over L. So M/L is algebraic. As $L \subset M$, L is algebraic over K.

The other direction follows from the following lemma:

Lemma 4.4. Suppose we have $M/L/K$ with L/K algebraic. Let $x \in M$, and suppose X is algebraic over L. Then x is algebraic over K.

Proof. $\exists f = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \in L[T]$ with $f \neq 0$ and $f(x) = 0$. Let $L_0 = K(a_0, \ldots, a_{n-1})$. As each a_i is algebraic over K, by Corollary 4.2, $[L_0 : K]$ is finite. As $f \in L_0[T]$, x is algebraic over L_0. So $[L_0(x) : L_0] < \infty$, so $[L_0(x) : K] < \infty$ by the tower law, so $[K(x) : K] < \infty$ and we're done. □

□

Example 4.3. Say $K = \mathbb{Q}, L = \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\}$, usually written $\overline{\mathbb{Q}}$. Obviously $L/\mathbb{Q}$ is algebraic, but it is not finite - for every $n \geq 1$, $\sqrt[n]{2} \in L$, and so $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ (as $T^n - 2$ is irreducible over $\mathbb{Q}$). So as this holds for all n, L cannot be finite over $\mathbb{Q}$.

We will see other fields like $\overline{\mathbb{Q}}$ later on. They are called **algebraically closed fields**.

5 Algebraic numbers in $\mathbb{R}$ and $\mathbb{C}$

Traditionally, we say that $x \in \mathbb{C}$ is **algebraic** if it is algebraic over $\mathbb{Q}$. Otherwise, we say it's transcendental. $\overline{\mathbb{Q}} = \{\text{algebraic } x\}$ is a subfield of $\mathbb{C}$. It is easy to see that $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$, as $\mathbb{Q}[T]$ and hence $\overline{\mathbb{Q}}$ are countable, while $\mathbb{C}$ is uncountable. So in a sense, basically all complex numbers are transcendental. However, it is a lot harder to write one down explicitly, or to show that some given number is transcendental.

Aside: some history. Liouville showed that $\sum_{n\geq 1} \frac{1}{10^{n!}}$ is transcendental ("algebraic numbers can't be very well approximated by rationals").

Hermite, Lindemann: e and π are transcendental.

Gelfond-Schneider (20^{th} century): if x, y are algebraic ($x \neq 0, 1$), then x^y is algebraic if and only if y is rational (e.g. $\sqrt{2}^{\sqrt{3}}$ is transcendental, and $e^{\pi} = (-1)^{-i/2}$ is transcendental). End of aside.

18 Oct 2022, Lecture 6

5.1 Ruler and compass constructions

We have three basic geometric operations.

(A) Given $P_1, P_2, Q_1, Q_2 \in \mathbb{R}^2$ with $P_i \neq Q_i$, we can construct the intersection of the lines P_1Q_1 and P_2Q_2 (assuming they intersect properly).

(B) Given P_1, P_2, Q_1, Q_2 with $P_i \neq Q_i$, we can construct the intersection points of the circles with centers P_i passing through Q_i (assuming they intersect properly).

(C) Similarly, we can construct line $\cap$ circle.

We say that a point $(x, y) \in \mathbb{R}^2$ is **constructible from** $(x_1, y_1), \ldots, (x_n, y_n)$ if it can be obtained by a finite sequence of the above operations A, B, C, each using only $\{(x_i, y_i)\}$ and any points produced in previous steps.

We say a real number $x \in \mathbb{R}$ is constructible if $(x, 0)$ is constructible from $\{(0, 0), (1, 0)\}$. For example, every $x \in \mathbb{Q}$ is constructible, as is $\sqrt{2}$.

Now a purely algebraic notion:

Definition 5.1. Suppose $K \subset \mathbb{R}$ is a subfield. Say K is **constructible** if $\exists n \geq 0$ and a sequence of fields $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \mathbb{R}$ and $a_i \in F_i$ such that

(i) $K \subset F_n$

(ii) $F_i = F_{i-1}(a_i)$

(iii) $a_i^2 \in F_{i-1}$.

Note. (ii) and (iii) tell us that $[F_i : F_{i-1}] \leq 2$. So by tower law, $[K : \mathbb{Q}]$ is finite, and it is a power of two.

Theorem 5.1. If $x \in \mathbb{R}$ is constructible, then $K = \mathbb{Q}(x)$ is constructible.

Corollary 5.2. If $x \in \mathbb{R}$ is constructible, then x is algebraic over $\mathbb{Q}$ and $\deg_{\mathbb{Q}}(x)$ is a power of two (this follows from the note above).

Proof. Induction on $k \geq 1$: we prove that if $(x, y) \in \mathbb{R}^2$ can be constructed with k ruler and compass constructions, then $\mathbb{Q}(x, y)$ is a constructible extension of $\mathbb{Q}$.

So assume we have $\mathbb{Q} = F_0 \subset \ldots \subset F_n$ satisfying (ii) and (iii) and such that the coordinates of all points obtained after $k-1$ constructions lie in F_n. But elementary analytic geometry tells us that the intersection point of two lines has coordinates that are rational functions of the coordinates of (P_i, Q_i) with rational coefficients. So if the k^{th} construction is of type A, then x, y, the coordinates of the k^{th} construction point, lie in F_n.

For B and C, the coordinates of the two intersections can be written as $a \pm b\sqrt{e}, c \pm d\sqrt{e}$, where a, e are rational functions of the coordinates of $\{P_i, Q_i\}$. So for the two newly constructed points, $x, y \in F_n(\sqrt{e})$, which is a constuctible extension of $\mathbb{Q}$. □

Remark. It is not hard to show that the converse is true: if $\mathbb{Q}(x)$ is a constructible extension of $\mathbb{Q}$, then x is constructible.

Classical problems:

- "Square the circle" – construct a square with area equal to that of a given circle, i.e. construct $\sqrt{\pi}$. But since π is transcendental, $\sqrt{\pi}$ is not constructible.
- "Duplicate the cube" – Construct a cube with volume twice that of a given cube, i.e. construct $\sqrt[3]{2}$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2, so $\mathbb{Q}[\sqrt[3]{2}]$ and therefore $\sqrt[3]{2}$ is not constructible.
- "Trisect the angle". Say we are trying to trisect $\frac{2\pi}{3}$, which is certainly constructible. So if we can trisect $\frac{2\pi}{3}$, the angle $\frac{2\pi}{9}$ is constructible, i.e. the real numbers $\cos\left(\frac{2\pi}{9}\right)$ and $\sin\left(\frac{2\pi}{9}\right)$ are constructible. By the formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, $\cos\left(\frac{2\pi}{9}\right)$ is a root of $8X^3 - 6x + 1$ and $2\cos\left(\frac{2\pi}{9}\right) - 2$ is a root of $X^3 + 6X^2 + 9X + 3$. This is irreducible by Eisenstein, so $\deg_{\mathbb{Q}}(\cos\left(\frac{2\pi}{9}\right)) = 3$. So a regular 9-gon is not constructible.

Later, Gauss proved that a regular n-gon is constructible if and only if n is the product of a power of 2 and distinct primes of the form $2^{2^k} + 1$ (Fermat primes).

6 Splitting fields

Problem: Given K a field, $f \in K[T]$, find an extension L/K (preferably as small as possible) such that f factors in $L[T]$ as a product of linears.

For example, if $F = \mathbb{Q}$, then the Fundamental Theorem of Algebra says that we can factor a monic $f \in \mathbb{Q}[T]$ as $f = \prod(T - x_i), x_i \in \mathbb{C}$. Later we will give another slick proof. So in this case, the best L would be $\mathbb{Q}(x_1, \ldots, x_n)$, a finite extension of $\mathbb{Q}$.

Example 6.1. Take $K = \mathbb{F}_p$ and f irreducible of degree $d > 1$. How to find L? The first step is to find an extension in which f has at least one root.

The **key construction**: suppose $f \in K[T]$ is irreducible (and monic). Let $L_f = K[T]/(f)$. As f is irreducible, (f) is maximal, so L_f is a field. By construction, if $x = T \pmod{(f)} \in L_f$ (i.e. just the coset $T + (f)$), then $f(x) = 0$, i.e. L_f/K is a field extension in which f has a root.

Questions: Is L_f unique? How do we find the remaining roots?