Part II - Galois Theory

Lectured by Prof. A. J. Scholl

Artur Avameri

Michaelmas 2022

Contents

0 Introduction **2**

1 Polynomials **3**

2 Symmetric polynomials **3**

3 Fields **6**

4 Algebraic elements and extensions **9**

5 Algebraic numbers in $\mathbb{R}$ and $\mathbb{C}$ **13**

5.1 Ruler and compass constructions 13

6 Splitting fields **15**

7 Normal extensions **18**

8 Separability **19**

9 Galois Theory **23**

10 Finite fields **29**

11 Cyclotomic extensions **32**

12 Kummer extensions **36**

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

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

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

If we cyclically permute x_1,x_2,x_3, we find $u\mapsto\omega u\mapsto\omega^2u$ and $v\mapsto\omega v\mapsto\omega^2v$, 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 $(1 + \text{number of roots of } g)$ 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

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

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 $\{s_r \mid 1 \le r \le n\}$ with coefficients in R.

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

08 Oct 2022, Lecture 2

Remarks.

(a) Consider the homomorphism

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

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

$$\prod_{i=1}^{n} (T + x_i) = T_n + s_1 T^{n-1} + \dots + s_{n-1} T + s_n.$$

(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 $X_I = X_1^{i_1} \dots X_n^{i_n}$ for some $I \in \mathbb{Z}_{\ge 0}^n$.
- Its **(total) degree** is $\sum i_\alpha$.
- A **term** β is some $cX_I, 0 \ne c \in R$, 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 $1 \le r < n$, $i_1 = j_1, \dots, i_r = j_r$ and $i_{r+1} > j_{r+1}$. This is a **total ordering**: for each pair $I \ne J$, 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 $i_1 \ge i_2 \ge \dots \ge i_n$ (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

$$X_I = X_1^{i_1 - i_2}(X_1 X_2)^{i_2 - i_3} \dots (X_1 \dots X_n)^{i_n}.$$

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. $\square$

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

$$s_1 s_2 = \sum_i \sum_{j<k} X_i X_j X_k = \sum_{i \neq j} X_i^2 X_j + 3 \sum_{i<j<k} X_i X_j X_k.$$

So $f = s_1 s_2 - 3 s_3$.

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 $\forall k \geq 1$,

$$p_k - s_1 p_{k-1} + \ldots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0.$$

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

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

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

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 $|G|\le m$, 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. $\square$

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 $\text{ev}_x : K[T] \to L$ is $K[X] \subset L$. x is algebraic over $K \implies \ker(\text{ev}_x) = (m_{x,K})$ 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

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

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 $a, b \in \mathbb{Q} \implies m = a^2+b^2n+2ab\sqrt{n}$. So $ab = 0$, whence either $b = 0$, so $m = a^2$ is a square, or $a = 0$, so $mn = b^2n^2$ 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. $\square$

$\square$

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$^{\text{th}}$ 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? 20 Oct 2022, Lecture 7

We start off by redoing what we did last time.

Theorem 6.1. Let $f \in K[T]$ be irreducible and monic. Let $L_f = K[T]/(f)$ and $t \subset L_f$ the residue class $T \bmod (f)$. Then L_f/K is a finite extension of fields, $[L_f : K] = \deg(f)$ and f is the minimal polynomial of t over K.

So we have an extension of K in which f has at least one root. To what extent is this unique?

Also recall that if x is algebraic over K, then $K(x) \cong K[T]/(m_{x,K})$, where $m_{x,K}$ is the minimal polynomial.

Definition 6.1. Let K be a field and M/K, L/K two extensions of K. Then a K**-homomorphism** from L to M is a field homomorphism $\sigma : L \to M$ which is the identity on K. (We might also call this a K**-embedding**, since σ is an injection.)

Theorem 6.2. Let $f \in K[T]$ be irreducible and L/K an arbitrary extension. Then

(i) If $x \in L$ is a root of f, then there exists a unique K-homomorphism $\sigma : L_f = K[T]/(f) \to L$ sending $T \bmod (f) \mapsto x$.

(ii) Every K-homomorphism $L_f \to L$ arises as in (i). So there is a bijection between

$$\{K\text{-homomorphisms } L_f \xrightarrow{\sigma} L\} \cong \{\text{roots of } f \text{ in } L\}$$

In particular, there are at most $\deg(f)$ such σ.

Proof. $f(x) = 0 \iff \mathrm{ev}_x(f) = 0$, where $\mathrm{ev}_x : K[T] \to L$ is the homomorphism $g \mapsto g(x)$, i.e. "evaluate at x" $\iff \ker(\mathrm{ev}_x) = (f) \iff \mathrm{ev}_x$ comes from a homomorphism $\sigma : K[T]/(f) \to L$ which is identity on K. ☐

Corollary 6.3. If $L = K(x)$ for x algebraic over K, then there exists a unique **isomorphism** $\sigma : L_f \to K(x)$ such that $\sigma(t) = x$, where $f = m_{x,K}$.

Proof. Take $L = K(x)$ in the above theorem. ☐

Definition 6.2. Let x, y be algebraic over K. Say x, y are K**-conjugate** if they have the same minimal polynomial.

Then both $K(x)$ and $K(y)$ are isomorphic to L_f (with $f = m_{x,K} = m_{y,K}$), and more precisely:

Corollary 6.4. x, y are K-conjugate if and only there exists a K-isomorphism $\sigma : K(x) \to K(y)$ with $\sigma(x) = y$.

Proof. By Corollary 6.3, $\Longleftarrow$ follows since $\forall g \in K[T], \sigma(g(x)) = g(\sigma(x))$, so x, y have the same minimal polynomial. ☐

So the roots of an irreducible polynomial are algebraically indistinguishable.

It is useful for inductive arguments to have a generalization of Theorem 6.2:

Definition 6.3. Let L/K and L'/K' be field extensions, and let $\sigma : K \to K'$ a field homomorphism. If $\tau : L \to L'$ is a homomorphism such that $\tau(x) = \sigma(x)\ \forall x \in K$, we say τ a σ**-homomorphism** from L to L'.

We also say τ **extends** σ, or that σ is the **restriction** of τ onto K, and write $\sigma = \tau|_K$.

Theorem 6.5 (Variant of Theorem 6.2)**.** Let $f \in K[T]$ be irreducible, and $\sigma : K \to L$ any homomorphism of fields. Let σf be the polynomial given by applying σ to all the coefficients of f. Then

(i) If $x \in L$ is a root of σf, then there exists a unique σ-homomorphism $\tau : L_f \to L$ such that $\tau(t) = x$.

(ii) Every σ-homomorphism $L_f \to L$ is of this form and we have a bijection

$$\{\sigma\text{-homomorphisms } L_f \to L\} \cong \{\text{roots of } \sigma f \text{ in } L\}.$$

Example 6.2. σ might not be the obvious homomorphism. Take $K = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $L = \mathbb{C}$. There is a homomorphism $\sigma : K \to \mathbb{C}$ by $\sqrt{2} \mapsto -\sqrt{2}$. So if we take $f = T^2 - (1 + \sqrt{2})$, so the map $L_f \xrightarrow{\tau} \mathbb{C}$ must take t to $\pm\sqrt{1 - \sqrt{2}} = \pm i\sqrt{\sqrt{2} - 1} \in \mathbb{C}$.

If instead we take σ to be the inclusion, then τ takes t to $\sqrt{\sqrt{2} + 1}$.

What about all roots?

Definition 6.4. Suppose $f \in K[T]$ is a nonzero polynomial. We say an extension L/K is a **splitting field** for f over K if:

(i) f splits into linear factors in $L[T]$,

(ii) $L = K(x_1, \ldots, x_n)$, where the x_i are the roots of f in L.

Remark. (ii) says that f doesn't split into linear factors over any field L' with $K \subset L' \subsetneq L$.

Remark. A splitting field is necessarily finite over K (all x_i are algebraic).

Theorem 6.6. Every nonzero polynomial in $K[T]$ has a splitting field.

Proof. By induction on $\deg(f)$ (for all K). If $\deg(f)$ is 0 or 1, then K is a spltting field, so we're done. So assume that for all fields K' and all polynomials of degree $< \deg(f)$ there is a splitting field.

Consider g, an irreducible factor of f. Consider $K' = L_g = K[T]/(g)$ and let $x_1 = T \bmod (g)$. Then $g(x_1) = 0$, so $f = (T - x_1)f_1$ for $f_1 \in K'[T]$ and $\deg(f_1) < \deg(f)$. So by induction, $\exists$ a spltting field L for f_1 over K'. Let $x_2, \ldots, x_n \in L$ be the roots of f_1 in L. Then f splits into linear factors in L with roots $x_1, \ldots, x_n$, and $L = K'(x_2, \ldots, x_n) = K(x_1, \ldots, x_n)$. So L is a splitting field for f over K. $\square$

22 Oct 2022, Lecture 8

Remark. If $K \subset \mathbb{C}$, this is no big deal, since we can take $x_1, \ldots, x_n \in \mathbb{C}$ to be the roots of f in $\mathbb{C}$ (by FTA), then $K(x_1, \ldots, x_n) \subset \mathbb{C}$ is a splitting field.

Our next result is nontrivial, even for subfields of $\mathbb{C}$.

Theorem 6.7 (Splitting fields are unique)**.** Let $f \in K[T]$ be nonzero, L/K be a splitting field for f, and let $\sigma : K \to M$ be an extension (homomorphism) such that σf splits (into linear factors) in $M[T]$. Then

(i) σ can be extended to a homomorphism $\tau : L \to M$.

(ii) If M is a splitting field for σf over σK, then any τ is an isomorphism. In particular, any two splitting fields for f are K-isomorphic.

Remark. It is not obvious (without this theorem) that two splitting fields have the same degree, because of the choices we make.

Remark. Typically there will be more than one τ.

Proof. (i) Induction on $n = [L : K]$. If $n = 1$, then $L = K$ and we're done.

Now let $x \in L \setminus K$ be some root of an irreducible factor $g \in K[T]$ of f with $\deg(g) > 1$. Let $y \in M$ be a root of $\sigma g \in M[T]$. By Theorem 6.5, there exists $\sigma_1 : K(x) \to M$ such that $\sigma_1(x) = y$ and σ_1 extends σ. Now,

$[L : K(x)] < [L : K]$, and L is certainly a splitting field for f over $K(x)$, and $\sigma_1 f = \sigma f$ splits in M. So by induction, we can extend $\sigma_1 : K(x) \to M$ to a homomorphism $\tau : L \to M$.

(ii) Assume M is a splitting field for σf over σK. Let τ be as in (i), and $\{x_i\}$ the roots of f in L. Then the roots of σf in M are just $\{\tau(x_i)\}$. So $M = \sigma K(\tau(x_1), \ldots, \tau(x_n)) = \tau L$ as $L = K(x_1, \ldots, x_n)$. So τ is an isomorphism. If $K \subset M$ and σ is the inclusion map, then τ is a K-isomorphism $L \to M$.

□

Example 6.3. (i) $f = T^3 - 2 \in \mathbb{Q}[T]$. In $\mathbb{C}$, we have

$$f = (T - \sqrt[3]{2})(T - \omega\sqrt[3]{2})(T - \omega^2\sqrt[3]{2}),$$

where $\omega = e^{2\pi i/3}$. So a splitting field for f over $\mathbb{Q}$ is $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \subset \mathbb{C}$. We have $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ but $\omega \notin \mathbb{R}$, $\omega^2 + w + 1 = 0$, so $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$ and $[L : \mathbb{Q}] = 6$. In particular, $\frac{f}{(T - \sqrt[3]{2})} = T + \sqrt[3]{2}T + (\sqrt[3]{2})^2$ is irreducible in $\mathbb{Q}(\sqrt[3]{2})[T]$.

(ii) $f = \frac{T^5 - 1}{T - 1} = T^4 + T^3 + T^2 + T + 1 \in \mathbb{Q}[T]$. Let $z = e^{2\pi i/5}$. Then $f = \prod_{1 \le a \le 4}(T - z^a)$. So $\mathbb{Q}(z)$ is already a splitting field for f over $\mathbb{Q}$, and $[\mathbb{Q}(z) : \mathbb{Q}] = 4$.

(iii) $f = T^3 - 2 \in \mathbb{F}_7[T]$. This is irreducible, as 2 is not a cube mod 7. Consider $L = \mathbb{F}_7[X]/(X^3 - 2) = \mathbb{F}_7(x)$, where $x^3 = 2$. Now $2^3 = 1 = 4^3$ in $\mathbb{F}_7$, so $(2x)^3 = (4x)^3 = 2$ and so $f = (T - 2)(T - 2x)(T - 4x) \in L[T]$. Note that joining one root is not enough to get a splitting field.

7 Normal extensions

We have this nice philosophy to pass from polynomials and their properties to fields generated by the roots of polynomials. Here we'll give an "intrinsic" characterization of splitting fields.

Definition 7.1. L/K is a **normal** extension if L/K is algebraic, and for every $x \in L$, $m_{x,K}$ splits into linear factors over L.

Remark. The condition is equivalent to: for every $x \in L$, L contains a splitting field for $m_{x,K}$. Or again, for every irreducible $f \in K[T]$, if f has a root in L, then it splits in $L[T]$.

Theorem 7.1 (Splitting fields are normal)**.** Let L/K be a finite extension. Then L/K is normal if and only if L is the splitting field for some $f \in K[T]$ (not necessarily irreducible).

Proof. $\implies$: Suppose L/K is normal, and write $L = K(x_1, \ldots, x_n)$. Then $m_{x,K}$ splits in L, and L is generated by the roots of $f = \prod_i m_{x_i,K}$. So L is a splitting field for f over K.

$\impliedby$: Suppose L is a splitting field for $f \in K[T]$. Let $x \in L$ and let $g = m_{x,K}$ be its minimal polynomial. We want to show that g splits in L. Let M be a splitting field for g over L and $y \in M$ a root of g. We want to show that $y \in L$. Since L is a splitting field for f over K:

- L is a splitting field for f over $K(x)$.
- $L(y)$ is a splitting field for f over $K(y)$.

Now there exists a K-isomorphism $K(x) \cong K(y)$, as x, y are roots of the irreducible polynomial $g \in K[T]$. So by the uniqueness of splitting fields, $[L : K(x)] = [L(y) : K(y)]$. Multiply by $[K(x) : K] = [K(y) : K] = \deg(g)$ and use the tower law to get that $[L : K] = [L(y) : K]$. So $L = L(y)$, i.e. $y \in L$. □

25 Oct 2022, Lecture 9

A "field-theoretic" version of splitting fields:

Corollary 7.2 (Normal closure)**.** Let L/K be a finite extension. Then there exists a finite extension M/L such that

(i) M/K is a normal extension,

(ii) If $L \subset M' \subset M$ and M'/K is normal, then $M' = M$.

Moreover, any two such extensions are L–isomorphic.

M is said to be a **normal closure** of L/K.

Proof. Let $L = K(x_1, \ldots, x_n)$ and let $f = \prod_i m_{x_i,K}$. Let M be a splitting field for f over L. Then, as the x_i are roots of f, M is also a splitting field for f over K, so it is normal.

Let M' be as in (ii), then as $x_i \in M'$, $m_{x_i,K}$ splits in M' (as M'/K is normal). So $M' = M$.

For uniqueness: any M satisfying (i) must contain a splitting field for f, and by the above, (ii) implies that M is a splitting field for f, so the result follows from uniqueness of splitting fields. □

8 Separability

Over $\mathbb{C}$, we can tell if a polynomial has a multiple zero by looking at its derivative f'. Over arbitrary fields, it turns out that the same is true, if we replace analysis by algebra.

Definition 8.1. The **formal derivative** of $f = \sum_{0 \le i \le d} a_i T^i \in K[T]$ is

$$f' = \sum_{1 \le i \le d} i a_i T^{i-1}.$$

Exercise : Check from the definition that $(f+g)' = f' + g'$, $(fg)' = fg' + f'g$ and $(f^n)' = nf'f^{n-1}$.

Example 8.1. In K of characteristic $p > 0$, $f = T^p + a_0 \implies f' = pT^{p-1} = 0$.

Proposition 8.1. Let $f \in K[T]$, L/K an extension and $x \in L$ a root of f. Then x is a simple root if and only if $f'(x) \neq 0$.

Proof. Write $f = (T-x)g \in L[T]$. Then $f' = g + (T-x)g'$, so $f'(x) = g(x)$ and $g(x) \neq 0$ if and only if $(T-x) \nmid g$, i.e. f has a simple zero at x. □

Definition 8.2. Say $f \in K[T]$ is **separable** if it splits into distinct linear factors (times a constant) in a splitting field (i.e. has $\deg(f)$ distinct roots).

Corollary 8.2. $f \in K[T]$ is separable if and only if $\gcd(f, f') = 1$.

Aside: we'll take $\gcd(f,g)$ to be the unique monic h such that $\gcd(f,g) = h$. Then $h = af + bg$, and Euclid's algorithm allows us to compute h, a, b. End of aside.

Observe that $\gcd(f,g)$ is the same in $K[T]$ as in $L[T]$ for any extension L of K, since Euclid's algorithm gives the same result in $K[T]$ and $L[T]$.

Proof. Replace K by a splitting field for f, so we may assume f has all its roots in K. It is separable if f, f' have no common root, which is true if and only if $\gcd(f, f') = 1$. □

Example 8.2. $\mathrm{char}(K) = p > 0$, $f = T^p - b, b \in K$. Then $f' = 0$, so $\gcd(f, f') = f \neq 1$. So f is inseparable. Let L be any extension of K containing $a \in L$ such that $a^p = b$. Then $f = (T-a)^p = T^p + (-a)^p = T^p - b$.

So f has only one root in a splitting field. In fact, if b isn't a p^{th} power in K, then f is irreducible (exercise!)

Theorem 8.3. (i) Let $f \in K[T]$ be irreducible. Then f is separable if and only if $f' \neq 0$.

(ii) If $\mathrm{char}(K) = 0$, then every irreducible polynomial in $K[T]$ is separable.

(iii) If $\mathrm{char}(K) = p > 0$, then an irreducible $f \in K[T]$ is **inseparable** (i.e. not separable) if and only if $f = g(T^p)$ for some $g \in K[T]$.

Proof. (i) Assume WLOG that f is monic. Then, as f is irreducible, we have $\gcd(f, f') = f$ or 1. If $\gcd(f, f') = f$, then as $\deg(f') < \deg(f)$, we must have $f' = 0$ (and the converse is obvious - if the gcd is 1, then f is separable).

(ii) Write $f = \sum_{i=0}^d a_i T^i$, so $f' = \sum_{i=1}^d i a_i T^{i-1}$, so $f' = 0 \iff i a_i = 0$ for all $1 \leq i \leq d$. If $\operatorname{char}(K) = 0$, then $a_i = 0 \ \forall i \implies f = a_0$ is a constant, so not irreducible.

(iii) Analogously to above, if $\operatorname{char}(K) = p > 0$, then $f' = 0 \iff a_i = 0$ for all i not divisible by $p \iff f = g(T^p) = \sum a_i T^{pi}$.

□

We now go from polynomials to fields.

Definition 8.3. Let L/K be an extension. We say $x \in L$ is **separable** over K if x is algebraic over K and its minimal polynomial $m_{x,K}$ is separable. We say L/K is **separable** if $\forall x \in L$, x is separable over K.

We say an extension is inseparable if it is not separable, i.e. some element is not separable over K.

Theorem 8.4. Let x be algebraic over K, and L/K any extension in which $m_{x,K}$ splits. Then x is separable over K if and only if there are exactly $\deg_K(x)$ K–homomorphisms from $K(x) \to L$.

Proof. Recall from Theorem 6.2 that the number of such homomorphisms is the number of roots of $m_{x,K}$ in L. This is equal to the degree of x if and only if x is separable, because the minimal polynomial splits. □

27 Oct 2022, Lecture 10

Notation: We write $\operatorname{Hom}_K(L, M)$ for the set of K–homomorphisms from L to M (not to be confused with K–linear maps L to M).

Theorem 8.5 (Counting embeddings)**.** Let $L = K(x_1, \dots, x_k)$ be a finite extension of K, and M/K any extension. Then

$$|\operatorname{Hom}_K(L, M)| \leq [L : K]$$

with equality holding if and only if

(i) $\forall i, m_{x_i,K}$ splits into linear factors over M; and

(ii) all the x_i are separable over K.

Remark. (i), (ii) are just saying that $m_{x_i,K}$ splits into distinct linear factors over M.

Remark. There is an obvious variant of this: take any homomorphism $\sigma : K \to M$, then $|\{\sigma\text{-homomorphisms } L \to M\}| \leq [L : K]$ with equality if and only if $\forall i, \sigma m_{x_i,K}$ splits over M.

Proof. Induction on k. $k = 0$ is obvious.

Now write $K_1 = K(x_1)$, $\deg_K(x_1) = d = [K_1 : K]$. Then, by Theorem 8.4,

$$|\mathrm{Hom}_K(K_1, M)| = e = |\{\text{number of roots of } m_{x_1,K} \text{ in } M\}| \leq d.$$

Let $\sigma : K_1 \to M$ be a K–homomorphism. Apply induction to L/K_1, so there exist at most $[L : K_1]$ extensions of σ that are a homomorphism $L \to M$. Hence

$$|\mathrm{Hom}_K(L, M)| \leq e[L : K_1] \leq d[L : K_1] = [L : K].$$

If equality holds, then $e = d$, i.e. $m_{x_1,K}$ has d distinct roots in M. Replacing x_1 by another x_i, we get (i) and (ii).

Conversely, assuming that (i) and (ii) hold, we see by Theorem 8.4 that $|\mathrm{Hom}_K(K_1, M)| = d$. (i) and (ii) still hold over K_1, so by induction on k, each $\sigma : K_1 \to M$ has $[L : K_1]$ extensions to $L \to M$, so $|\mathrm{Hom}_K(L, M)| = [L : K]$. □

This result has two corollaries.

Theorem 8.6 (Separably generated implies separable)**.** Let $L = K(x_1, \ldots, x_k)$ be a finite extension of K. Then L/K is separable if and only if all the x_i are separable over K.

Proof. L/K separable $\implies$ x_i separable by definition.

Conversely, assume all the x_i are separable over K, and let M be a normal closure (splitting field of $\prod_i m_{x_i,K}$) over L. Then in Theorem 8.5, (i) and (ii) both hold, so $|\mathrm{Hom}_K(L, M)| = [L : K]$. But if $x \in L$, then $L = K(x, x_1, \ldots, x_k)$ as well. So as all the K–embeddings are separable, by Theorem 8.5, x is separable over K. □

Corollary 8.7. Let x, y in L, an extension of K. If x, y are separable over K, then so are $x + y, xy$ and $\frac{1}{x}$ (for x nonzero).

Proof. Apply Theorem 8.6 to $K(x, y)$. □

So in particular, the elements of L that are separable over K form a subfield of L.

Theorem 8.8 (Primitive element theorem for separable extensions)**.** Let K be an infinite field and $L = K(x_1, \ldots, x_k)$, where $x_1, \ldots, x_k$ are separable over K. Then $\exists x \in L$ such that $L = K(x)$. (By Theorem 8.6, x is also separable over K).

Proof. It is enough to consider the case $k = 2$. Then $L = K(x, y)$ with x, y separable over K. Let $n = [L : K]$, and let M be a normal closure for L/K. Then there exist n distinct K–homomorphisms $\sigma_i : L \to M$ by Theorem 8.5. Let $a \in K$ and consider $z = x + ay$. We will choose $a \in K$ such that $L = K(z)$.

As $L = K(x, y)$, we have $\sigma_i(x) = \sigma_j(x)$ and $\sigma_i(y) = \sigma_j(y)$ if and only if $i = j$. Consider $\sigma_i(z) = \sigma_i(x) + a\sigma_i(y) \in M$. If $\sigma_i(z) = \sigma_j(z)$, then

$$(\sigma_i(x) - \sigma_j(x)) + a(\sigma_i(y) - \sigma_j(y)) = 0.$$

But if $i \neq j$, then at least of the terms in parentheses is nonzero. Therefore there exists at most one $a \in K$ for which $\sigma_i(z) = \sigma_j(z)$.

As K is infinite, $\exists a \in K$ such that all $\sigma_i(z)$ are distinct. But then $\deg_K(z) = n$, so $L = K(z)$. ☐

For finite fields, the result is easy:

Theorem 8.9. If L/K is an extension of finite fields, then $L = K(x)$ for some $x \in L$.

Proof. The multiplicative group $L^\times$ is cyclic, so let x be a generator. Then $L = K(x)$. ☐

9 Galois Theory

Automorphisms of fields: $\sigma : L \to L$ is an **automorphism** of the field L if it is a bijective homomorphism (this is true if and only if it is a homomorphism and has an inverse).

The set of automorphisms of L forms a group (under composition). This is called the automorphism group of L, denoted $\mathrm{Aut}(L)$.

If $S \subset \mathrm{Aut}(L)$ is a subset, let

$$L^S = \{x \in L \mid \forall \sigma \in S, \sigma(x) = x\}.$$

This is a subfield of L (since each σ is a homomorphism), called the **fixed field** of S.

Example 9.1. If $L = \mathbb{C}$ and σ is complex conjugation, then $L^{\{\sigma\}} = \mathbb{R}$.

Let L/K be an extension. Define

$$\mathrm{Aut}(L/K) = \{K\text{-automorphisms of } L\} = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \ \forall x \in K\}.$$

Equivalently, $\sigma \in \mathrm{Aut}(L)$ is in $\mathrm{Aut}(L/K) \iff K \subset L^{\{\sigma\}}$. This is a subgroup of $\mathrm{Aut}(L)$.

Theorem 9.1. Let L/K be finite. Then $|\mathrm{Aut}(L/K)| \leq [L : K]$.

Proof. Take $M = L$ in Theorem 8.5. Then $\mathrm{Hom}_K(L, M) = \mathrm{Aut}(L/K)$. ☐

29 Oct 2022, Lecture 11

Fact. If $K=\mathbb{Q}$ or $K=\mathbb{F}_p$, then $\operatorname{Aut}(K)=\{1\}$ (since $\sigma=(1_K)=1_K \implies \sigma(m1_K)=m1_K\ \forall m\in\mathbb{Z}$, and $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$).

So for any L, $\operatorname{Aut}(L)=\operatorname{Aut}(L/K)$ where K is the prime subfield (copy of $\mathbb{Q}$ or $\mathbb{F}_p$).

We now want to have a notion of when L/K has "many" symmetries.

Definition 9.1. An extension L/K is **Galois** if it is algebraic and

$$L^{\operatorname{Aut}(L/K)}=K.$$

(Recall that if $S\subset\operatorname{Aut}(L)$ is a subset, then $L^S=\{x\in L\mid\sigma(x)=x\ \forall x\in S\}$, the **fixed field** of S). In other words, the automorphisms detect when an element of L is in K.

Example 9.2.

- Simplest example: $\mathbb{C}/\mathbb{R}$ is Galois.
- $\mathbb{Q}(i)/\mathbb{Q}$ is Galois.
- If $K/\mathbb{F}_p$ is a finite extension (so K is a finite field), we have the Frobenius automorphism $\phi_p:K\to K,\phi_p(x)=x^p$. Then

$$K^{\{\phi_p\}}=\{x\in K\mid x\text{ is a root of }T^p-T\}=\mathbb{F}_p.$$

So $K^{\operatorname{Aut}(K/\mathbb{F}_p)}=\mathbb{F}_p$, i.e. $K/\mathbb{F}_p$ is a Galois extension.

Definition 9.2. If L/K is Galois, we write $\operatorname{Gal}(L/K)=\operatorname{Aut}(L/K)$, the **Galois group** of L/K.

Theorem 9.2 (Classification of finite Galois extensions)**.** Let L/K be finite, $G=\operatorname{Aut}(L/K)$. Then the following are equivalent:

(i) L/K is Galois, i.e. $K=L^G$.

(ii) L/K is normal and separable.

(iii) L is a splitting field of a separable polynomial over K.

(iv) $|\operatorname{Aut}(L/K)|=[L:K]$.

If any of the above hold, then the minimal polynomial of any $x\in L$ is $m_{x,K}=\prod_{i=1}^r(T-x_i)$, where $\{x_1,x_2,\dots,x_r\}=\{\sigma(x)\mid x\in G\}$, the orbit of x in G (for x_i distinct).

Proof. (i) $\implies$ (ii) and the last part: Let $x\in L$, $\{x_1,\dots,x_r\}$ the orbit of x in G, $f=\prod(T-x_i)$, so $f(x)=0$. As G permutes $\{x_i\}$, the coefficients of f are fixed by G, so $f\in L^G[T]=K[T]$, so $m_{x,K}\mid f$. Also, since $m_{x,K}(\sigma(x))=$

$\sigma(m_{x,K}(x)) = 0$, every x_i is a root of $m_{x,K}$, so $f = m_{x,K}$. So x is separable over K, and $m_{x,K}$ splits in L, so L/K is normal and separable.

(ii) $\implies$ (iii): By Theorem 7.1, L is a splitting field for some $f \in K[T]$. Write $f = \prod q_i^{e^i}$ where the q_i are irreducible, distinct, and $e_i \geq 1$. As L/K is separable, the q_i are separable, so $g = \prod q_i$ is separable, and L is also a splitting field for g.

(iii) $\implies$ (iv): Write $L = K(x_1, \dots, x_k)$ for the splitting field of some separable f with roots x_i. Take $M = L$ and apply Theorem 8.5. As $m_{x_i,K} \mid f$, the conditions in the theorem are satisfied, so

$$|\mathrm{Aut}(L/K)| = |\mathrm{Hom}_K(L, M)| = [L : K].$$

(iv) $\implies$ (i): Suppose $|G| = [L : K]$ (where $G = \mathrm{Aut}(L/K)$). Then

$$G \subset \mathrm{Aut}(L/L^G) \subset \mathrm{Aut}(L/K),$$

so $G = \mathrm{Aut}(L/L^G)$ and $[L : K] = |G| \leq [L : L^G]$. As $K \subset L^G$, this implies that $L^G = K$ by tower law. □

Corollary 9.3. Let L/K be a finite Galois extension. Then $L = K(x)$ for some x, separable over K, of degree $[L : K]$.

Proof. By Theorem 9.2 (ii), L/K is separable, so by the primitive element theorem, $L = K(x)$ and the result follows. □

Theorem 9.4 (The Galois correspondence)**.** Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$.

(a) Suppose $K \subset F \subset L$. Then L/F is also a Galois extension, $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K)$, and the map $F \mapsto \mathrm{Gal}(L/F)$ is a bijection

$$\{\text{intermediate fields } K \subset F \subset L\} \cong \{\text{subgroups } H \text{ of } G\}$$

whose inverse is the map taking H to the fixed field L^H. This bijection is inclusion–reversing, and if $F = L^H$, then $[F : K] = [G : H]$.[2]

(b) Let $\sigma \in G$, $H \leq G$ a subgroup and $F = L^H$. Then $\sigma H \sigma^{-1}$ corresponds to σF.

(c) We have equivalent statements for $H \leq G$:

(i) L^H/K is Galois;

(ii) L^H/K is normal;

[2] $A \leq B$ means A is a subgroup of B, and $[G : H]$ is the index of H in G.

(iii) $\forall \sigma \in G, \sigma(L^H) = L^H$;

(iv) $H \leq G$ is a normal subgroup.

If these hold, then $\mathrm{Gal}(L^H/K) \cong G/H$.

01 Nov 2022, Lecture 12

Proof. (a) Let $x \in L$. Then $m_{x,F}$ divides $m_{x,K}$ in $F[T]$. As $m_{x,K}$ splits into distinct linear factors in L, so does $m_{x,F}$. So L/F is normal and separable, hence Galois. By definition, $\mathrm{Gal}(L/F)$ is a subgroup of G. To check we have a bijection with the claimed inverse:

- $$F \mapsto H = \mathrm{Gal}(L/F) \mapsto L^H \stackrel{?}{=} F.$$
  But $L^{\mathrm{Gal}(L/F)} = F$ as L/F is Galois, i.e. $L^H = F$.
- $$H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H) \stackrel{?}{=} H.$$
  It is enough to show that $[L : L^H] \leq |H|$, since certainly $H \subset \mathrm{Gal}(L/L^H)$, and $|\mathrm{Gal}(L/L^H)| \leq [L : L^H]$. By Corollary 9.3 we get $L = L^H(x)$, and $f = \prod_{\sigma \in H}(T - \sigma(x)) \in L^H[T]$, with x as a root. So $[L : L^H] = \deg_{L^H}(x) \leq \deg(f) = |H|$. So we have a bijection. If $F \subset F'$, then $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$, so the bijection is inclusion–reversing. Finally, if $F = L^H$, then (as L/K and L/F are both Galois)
  $$[F : K] = \frac{[L : K]}{[L : F]} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/F)|} = \frac{|G|}{|H|} = [G : H].$$

(b) Under (a), $\sigma H \sigma^{-1}$ corresponds to
$$L^{\sigma H \sigma^{-1}} = \{x \in L \mid \sigma\tau\sigma^{-1}(x) = x \ \forall \tau \in H\}$$
and $\sigma\tau\sigma^{-1}(x) = x \iff \tau\sigma^{-1}(x) = \sigma^{-1}(x) \iff \tau(y) = y$, where $x = \sigma(y)$. So $x \in L^{\sigma H \sigma^{-1}} \iff x = \sigma(y), y \in L^H$, i.e. $L^{\sigma H \sigma^{-1}} = \sigma F$.

(c) L/K is separable, so L^H/K is separable. So (i) $\iff$ (ii).

Let $F = L^H, x \in F$. Then $\{\text{roots of } m_{x,K}\}$ is the orbit of x under G. So $m_{x,K}$ splits in F if and only if $\forall \sigma \in G, \sigma(x) \in F$. As this holds $\forall x \in F$, F is normal if and only if $\sigma F \subset F$. As $[\sigma F : K] = [F : K]$ (σF is K–isomorphic to F), this means $\sigma F = F$. By (b), this is equivalent to the statement $\forall \sigma \in G$, $\sigma H \sigma^{-1} = H$, i.e. H is a normal subgroup.

Last part: as $\forall \sigma \in G, \sigma F = F$, we have a homomorphism $G \to \mathrm{Gal}(F/K)$ given by restricting $\sigma \in G$ to F. Its kernel is H (since $F = L^H$), so G/H is isomorphic to a subgroup of $\mathrm{Gal}(F/K)$. But we have an isomorphism, as $[G : H] = [F : K]$ by (a).

□

Remark. This is one of the main results of Galois Theory.

Example 9.3. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \subset \mathbb{C}$, $\omega = e^{2\pi i/3}$. We know from before that L is a splitting field for $T^3 - 2$, and $[L : \mathbb{Q}] = 6$. So $L/\mathbb{Q}$ is the splitting field of a separable polynomial, hence it is Galois. Let $G = \mathrm{Gal}(L/K)$, then we also know $|G| = 6$.

What obvious subfields of L do we see? We have $F_1 = \mathbb{Q}(\omega)$, $F_2 = \mathbb{Q}(\sqrt[3]{2})$ with $[F_1 : \mathbb{Q}] = 2, [F_2 : \mathbb{Q}] = 3$. Now draw a picture:

$$\begin{tikzcd}
 & L \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
F_1 = \mathbb{Q}(\omega) \arrow[dr, dash, "2"'] & & F_2 = \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{1\} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
H_1 \arrow[dr, dash, "2"'] & & H_2 \arrow[dl, dash, "3"] \\
 & G &
\end{tikzcd}$$

Fields Groups

This gives us a subfield lattice with a corresponding subgroup lattice, where each field is the fixed field of the corresponding group. The numbers on the edges correspond to the degrees of field extensions on the left and the indices of the subgroups on the right.

Since $|G| = 6$, G is isomorphic to either C_6 or S_3. Note that $F_2/\mathbb{Q}$ is not normal, as $\omega\sqrt[3]{2} \notin F_2$, so $H_2 = \mathrm{Gal}(L/F_2)$ is not a normal subgroup. Hence G is nonabelian, so $G \cong S_3$.

Hence we have $H_2 \cong \{(12), e\}$ (by relabeling if necessary) and we must have $H_1 \cong A_3$. We have two other subgroups $\{(13), e\}$ and $\{(23), e\}$. There are the **conjugates** of H_2, so the corresponding subfields are $\{\sigma F_2 \mid \sigma \in G\}$, which are $\mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega^2\sqrt[3]{2})$ (the conjugates of $\sigma(\sqrt[3]{2})$, $\sigma \in G$ are the roots of the minimal polynomial).

So this describes all F with $\mathbb{Q} \subset F \subset L$.

In fact, we could have seen at once that $G \cong S_3$:

Suppose $f \in K[T]$ is a separable polynomial, $x_1, \dots, x_n$ are its roots in a splitting field L (where $n = \deg(f)$). Then $G = \mathrm{Gal}(L/K)$ permutes the $\{x_i\}$ (as $f(\sigma x_i) = \sigma f(x_i) = 0$), and if $\sigma(x_i) = x_i\ \forall i$, then since $L = K(x_1, \dots, x_n)$, $\sigma = \mathrm{id}$. This gives an injective homomorphism $G \to S_n$.

So in the above example, we have a subgroup of S_3 of order 6, so it must be S_3.

Definition 9.3. The subgroup $\mathrm{Gal}(f/K) \subset S_n$ given by the image of G is the **Galois group** of f over K.

Note. $[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(f/K)|$, which is a subgroup of S_n, so it divides $n!$.

There exist several methods for determining the Galois group $\mathrm{Gal}(f/K)$. Two useful results to know:

Definition 9.4. A subgroup $G \subset S_n$ is **transitive** if $\forall i, j \in \{1, 2, \dots, n\}, \exists \sigma \in G$ with $\sigma(i) = j$, i.e. G only has one orbit.

Proposition 9.5. f is irreducible $\iff$ $\mathrm{Gal}(f/K)$ is **transitive**.

Proof. Let x be a root of f in the splitting field L. Then its orbit under $G = \mathrm{Gal}(f/K)$ is the set of roots of $m_{x,K}$ (by Theorem 9.2). As $m_{x,K} \mid f$, we have $m_{x,K} = f$ if and only if f is irreducible. Furthermore, $m_{x,K} = f$ if and only if every root of f is in the orbit of x, i.e. if and only if G acts transitively on the roots of f. $\square$

Remark. If G is transitive, then by orbit-stabilizer theorem, $n \mid |G|$.

Recall from Section 2 that we defined the **discriminant**: if $f \in K[T]$ is monic and $f = \prod_{1 \le i \le n}(T - x_i)$ in a field L, then

$$\mathrm{Disc}(f) = \Delta^2 \in K,$$

where $\Delta = \prod_{1 \le i < j \le n}(x_i - x_j)^2$. The discriminant is nonzero if and only if f is separable.

Proposition 9.6. Let L be a splitting field over K and G a Galois group for a monic separable polynomial $f \in K[T]$. Assume $\mathrm{char}(K) \neq 2$. Then the fixed field of $G \cap A_n$ is $K(\Delta)$.

In particular, $\mathrm{Gal}(f/K) \subset A_n$ if and only if $\mathrm{Disc}(f)$ is a square in K.

03 Nov 2022, Lecture 13

Proof. $\pi \in S_n$, and π has a sign ± 1, where

$$\prod_{1 \le i < j \le n} (T_{\pi(i)} - T_{\pi(j)}) = \mathrm{sgn}(\pi) \prod_{1 \le i < j \le n} (T_i - T_j).$$

So if $\sigma \in G$, then $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$. As $\Delta \neq 0$ and $\mathrm{char}(K) \neq 2$, this implies that $\Delta \in K \iff G \in A_n$ and Δ lies in the fixed field F of $G \cap A_n$. As $[F : K] = [G : G \cap A_n] = \begin{cases} 1 & \text{if } G \subset A_n \\ 2 & \text{otherwise} \end{cases}$, we have $F = K(\Delta)$. $\square$

Example 9.4. Take $n = 3$ and $f = T^3 + aT + b = \prod_{i=1}^3 (T - X_i)$. Then $x_3 = -x_1 - x_2$, $a = x_1x_2 - (x_1 + x_2)^2$ and $b = x_1x_2(x_1 + x_2)$. Thus

$$\mathrm{disc}(f) = ((x_1 - x_2)(2x_1 + x_2)(x_1 + 2x_2))^2 = -4a^3 - 27b^2.$$

So $\mathrm{Gal}(f/K) \subset A_3 \iff -4a^3 - 27b^2$ is a square in K.

For example, take $f = T^3 - 21T - 7 \in \mathbb{Q}[T]$, which is irreducible. Then $\mathrm{disc}(f) = 4 \cdot 21^3 - 27 \cdot 7^2 = (27 \cdot 7)^2$. So $\mathrm{Gal}(f/\mathbb{Q}) \subset A_3$. As f is irreducible, the Galois group is **transitive**. So $\mathrm{Gal}(f/\mathbb{Q}) = A_3$.

This allows us to compute the Galois group of any cubic polynomial (of say $\mathrm{char}(K) \neq 2, 3$).

10 Finite fields

Let p be a prime and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We aim to describe all finite fields of characteristic p (i.e. finite extensions F of $\mathbb{F}_p$) and their Galois theory. Recall that:

- $|F| = p^n, [F : \mathbb{F}_p] = n$.
- $F^\times$ is cyclic and of order $p^n - 1$.
- $\phi_p : F \to F$ by $x \mapsto x^p$ is an automorphism of F (Frobenius).

Theorem 10.1. Let $n \geq 1$. Then there exists a field with $q = p^n$ elements. Any such field is a splitting field of the polynomial $f = T^q - T$ over $\mathbb{F}_p$. In particular, any two finite fields of the same order are isomorphic.

Proof. Let F be a field with $q = p^n$ elements. Then if $x \in F^\times, x^{q-1} = 1$, so $\forall x \in F, x^q = x$. So $f = \prod_{x \in F}(T - x)$ splits into linear factors in F, and not in any proper subfield of F. So F is a splitting field for f over $\mathbb{F}_p$. By uniqueness of splitting fields, F is unique up to isomorphism.

Conversely, given n, let $q = p^n$, let $L/\mathbb{F}_p$ be a splitting field for $f = T^q - T$ and let $F \subset L$ be the fixed field of $\phi_p^n : x \mapsto x^q$. So F is the set of roots of $f = T^q - T$ in L. So $|F| = q$ (and $F = L$). $\square$

Notation. We write $\mathbb{F}_q$ for any finite field with q elements. By Theorem 10.1, any two are isomorphic, although there is no "preferred" or "canonical" isomorphism.

Theorem 10.2. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, with Galois group cyclic of order n, generated by ϕ_p (the Frobenius automorphism).

Proof. $T^{p^n} - T = \prod_{x \in \mathbb{F}_{p^n}}(T - x)$ is separable, so $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$ (as it is the splitting field of a separable polynomial). Let $G \subset \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ be the subgroup generated by ϕ_p. Then $\mathbb{F}_{p^n}^G = \{x \mid x^p = x\} = \mathbb{F}_p$. So by Galois correspondence, $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. $\square$

Theorem 10.3. $\mathbb{F}_{p^n}$ has a unique subfield of order p^m for each $m \mid n$, and no others. If $m \mid n$, then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ is the fixed field of ϕ_p^m.

Proof. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_n) \cong \mathbb{Z}/n\mathbb{Z}$. The subgroups of $\mathbb{Z}/n\mathbb{Z}$ are $m\mathbb{Z}/n\mathbb{Z}$ for $m \mid n$. So by Galois correspondence, the subfields of $\mathbb{F}_{p^n}$ are the fixed fields of these subgroups, i.e. the subgroups $\langle \phi^m \rangle$, which have degree equal to the indices $[\mathbb{Z}/n\mathbb{Z} : m\mathbb{Z}/n\mathbb{Z}] = m$. □

Remark. If $m \mid n$, then $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi_p^m \rangle$ with order $\frac{n}{m}$.

Theorem 10.4. Let $f \in \mathbb{F}_p[T]$ be separable of degree $n \geq 1$ whose irreducible factors have degrees $n_1, \dots, n_r$ with $\sum n_i = n$. Then $\mathrm{Gal}(f/\mathbb{F}_p) \subset S_n$ is cyclic, generated by an element of cycle type $(n_1, \dots, n_r)$. In particular, $|\mathrm{Gal}(f/\mathbb{F}_p)| = \mathrm{lcm}(n_1, \dots, n_r)$.

Remark. Cycle type $(n_1, \dots, n_r)$ means that σ is a product of disjoint cycles of lengths n_i.

Proof. Let L be a spliting field for f over $\mathbb{F}_p$ and let the roots be $x_1, \dots, x_n$. Then $\mathrm{Gal}(L/\mathbb{F}_p)$ is cyclic and generated by ϕ_p. As the irreducible factors of f are the minimal polynomials of the x_i's and the set of roots of the minimal polynomial of x_i is the orbit of ϕ_p on x_i, the cycle type of ϕ_p is $(n_1, \dots, n_r)$. The order of such a permutation is the LCM of $\{n_i\}$. □

05 Nov 2022, Lecture 14

Theorem 10.5 (Reduction mod p)**.** Suppose $f \in \mathbb{Z}[T]$ is monic and separable, p is a prime, and $n = \deg(f) \geq 1$. Suppose that the reduction $\overline{f} \in \mathbb{F}_p[T]$ of f mod p is also separable. Then

$$\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subset \mathrm{Gal}(f/\mathbb{Q})$$

as subgroups of S_n.

Corollary 10.6. With the same assumptions as in Theorem 10.5, suppose that $\overline{f} = g_1 \dots g_r$ with $g_i \in \mathbb{F}_p[T]$ irreducible of degree n_i. Then $\mathrm{Gal}(f/\mathbb{Q})$ contains an element of cycle type $(n_1, \dots, n_r)$.

Proof. Combine Theorem 10.4 and Theorem 10.5. □

Example 10.1. $f = T^4 - 3T + 1$.

- If $p = 2$, then $f = T^4 + T + 1 \pmod 2$, which is irreducible (as it is not divisible by $T^2 + T + 1$, the only irreducible polynomial of degree 2).
- If $p = 5$, then $f = (T+1)(\underbrace{T^3 - T^2 + T + 1}_{\text{irreducible}})$. So by Corollary 10.6, we see that $\mathrm{Gal}(f/\mathbb{Q}) = G$ contains a 4–cycle and a 3–cycle, so $|G|$ is divisible by 12 and so is either S_4 or A_4 (as it is the unique subgroup of S_4 of order 12). But 4–cycles are odd, so $G = S_4$.

Remark. If $\overline{f}$ is separable, then $\mathrm{Disc}(f) \neq 0$, so $p \nmid \mathrm{Disc}(f)$, i.e. f is separable.

Remark. If f is separable, then $\overline{f}$ will be separable for all but the finite set $\{p \mid \mathrm{Disc}(f)\}$. So we have lots of values of p to try.

Remark. The meaning of $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subset \mathrm{Gal}(f/\mathbb{Q})$: The identification of $\mathrm{Gal}(f/\mathbb{Q})$ with a subgroup of S_n depends on fixing a labeling/ordering of the roots. Taking a different ordering conjugates $\mathrm{Gal}(f/\mathbb{Q})$ inside S_n (by the permutation giving the reordering). So the above statement really means that $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ is conjugate to a subgroup of $\mathrm{Gal}(f/\mathbb{Q})$.

There exist at least two proofs of Theorem 10.5. One of the proofs is difficult to understand, and will be posted on the Moodle page. The other proof has a flavor of algebraic number theory, but is self-contained and we present it here:

Proof of Theorem 10.5 (non-examinable). Let $L = \mathbb{Q}(x_1, \ldots, x_n)$ be the splitting field for $f = \prod(T - x_i)$ of degree $N = [L : \mathbb{Q}]$. Consider $R = \mathbb{Z}[x_1, \ldots, x_n]$. As $f(x_i) = 0$, f is monic and every element of R is a $\mathbb{Z}$–linear combination of $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$ for $0 \leq a_i \leq n$. So R is finitely generated as an abelian group. As $R \subset L \cong \mathbb{Q}^N$, we must have $R \cong \mathbb{Z}^M$ for $M \leq N$. (In fact, $M = N$, but we don't prove that here).

Now consider $\overline{R} = R/pR$, which has p^M elements. Let $\overline{P}$ be a maximal ideal of $\overline{R}$, corresponding to an ideal P of R containing pR. Then $F = R/pR \cong \overline{R}/\overline{P}$ (by the isomorphism theorems) is a finite field with of characteristic p, so say it has p^d elements. $F = \mathbb{F}_p(\overline{x_1}, \ldots, \overline{x_n})$, where $\overline{x_i} = x_i + P \in F$ and $\overline{f} = \prod_{n=1}(T - \overline{x_i})$. As $\overline{f}$ is separable, the $\overline{x_i}$ are distinct, so F is a splitting field for $\overline{f}$.

$G = \mathrm{Gal}(f/\mathbb{Q})$ takes R to itself (as it permutes the x_i). Let $H \subset G$ be the stabilizer of P, i.e. $\{\sigma \in G \mid \sigma P = P\}$. Then H acts on $R/P = F$, permuting the $\overline{x_i}$'s in the same way as it permutes the x_i's. So we have an injective homomorphism $H \hookrightarrow \mathrm{Gal}(f/\mathbb{F}_p)$. It is enough to show that this is an isomorphism. Let $\{P_1, \ldots, P_r\}$ be the orbit of G under G ($P_i = \sigma P$ for some $\sigma \in G$). P_i are all maximal ideals (because P is), $R/P_i \cong R/P$ has p^d elements as well. As the P_i are maximal, $P_i + P_j = R$ if $i \neq j$. So by Chinese Remainder Theorem, $R/(P_1 \cap \ldots \cap P_r) \cong R/P_1 \times \ldots \times R/P_r$. As $p \in P_i$, $pR \subset P_1 \cap \ldots \cap P_r$, so

$$p^N \geq p^M = |R/pR| \geq |R/(P_1 \cap \ldots \cap P_r)| = \prod_{i=1}^{r} |R/P_i| = p^{rd},$$

so $N \geq^{rd}$. By the Orbit-Stabilizer Theorem, $r = [G : H] = \frac{N}{|H|}$, and because $H \hookrightarrow \mathrm{Gal}(F/\mathbb{F}_p)$ (i.e. H injects into $\mathrm{Gal}(F/\mathbb{F}_p)$), we have $|H| \leq d$ if and only if the above map is an isomorphism. So $N \leq rd$. Hence $N = rd$, so $H \cong \mathrm{Gal}(\overline{f}/\mathbb{F}_p)$. $\square$

Remark. If $\text{Gal}(f/\mathbb{Q})$ contains an element of cycle type $(n_1, \dots, n_r)$, then it is a (hard!) fact that exist infinitely many primes such that $\overline{f}$ factors into irreducibles of degrees $n_1, \dots, n_r$. This is called Chebotarov's density theorem – it is a generalization of Dirichlet's theorem on primes in arithmetic progressions. This might be proved in II Number Fields.

11 Cyclotomic extensions

We consider polynomials of the form $T^n - 1$ (and later $T^n - a$).

Lemma 11.1. Let C be a cyclic group of order $n \geq 2$ (written multiplicatively). If $a \in \mathbb{Z}$ and $(a, n) = 1$, then the map $[a] : C \to C$ by $[a]g = g^a$ is an **automorphism** of C, and the map

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \text{Aut}(c), a \mapsto [a]$$

is an isomorphism.

Proof. $[a]$ is obviously a homomorphism, and it is an automorphism since $\exists b$ with $ab \equiv 1 \pmod{n}$. So we have an injective map $(\mathbb{Z}/n\mathbb{Z})^\times \hookrightarrow \text{Aut}(C)$ by $a \mapsto [a]$, which is obviously a homomorphism. If $\phi \in \text{Aut}(C)$ and g is a generator of C, then $\phi(g) = g^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, so $\phi = [a]$, so we have an isomorphism. $\square$

08 Nov 2022, Lecture 15

Let K be a field and $n \geq 1$. Define $\mu_n(K) = \{x \in K \mid x^n = 1\}$, the group of n^{th} roots of unity in K under multiplication. This is finite, hence cyclic (by Proposition 3.5), hence of order dividing n.

We say $\zeta \in \mu_n(K)$ is a **primitive** n^{th} root of 1 if ζ has order exactly n in $K^\times$. Such a ζ exists if and only if $\mu_n(K)$ has order n (and then ζ is a generator for $\mu_n(K)$). In particular, $f = T^n - 1$ has n distinct roots, so it is separable.

In general, $T^n - 1 = f$ is separable $\iff$ $(f, f') = 1$ and since $f' = nT^{n-1}$, this holds if and only if $n \cdot 1_K \neq 0$.

Important: From now on, until the end of the section, assume that either $\text{char}(K) = 0$ or $\text{char}(K) = p > 0$ and $p \nmid n$ (in other words, that $f = T^n - 1$ is separable).

Let L/K be a splitting field for $T^n - 1$ and let $G = \text{Gal}(L/K)$ (L/K is Galois as f is separable). Then $|\mu_n(L)| = n$, so there exists a primitive n^{th} root of 1, $\zeta = \zeta_n \in L$. L/K is called a **cyclotomic extension**.

Proposition 11.2. (i) $L = K(\zeta)$.

(ii) There exists an injective homomorphism $\chi = \chi_n : G = \text{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ such that if $\chi(\sigma) = a \pmod{n}$, then $\sigma(\zeta) = \zeta^a$. In particular, G is abelian.

(iii) χ is an isomorphism if and only if G acts transitively on the set of primitive roots of unity in L. (χ is called the **cyclotomic character**).

Proof. (i) $\mu_n(L) = \langle\zeta\rangle$, so the roots of $f = T^n - 1$ are the powers of ζ, so $L = K(\{\zeta^a\}) = K(\zeta)$.

(ii) Consider the action on G on L. It permutes the roots $\mu_n(L)$ and if $\zeta, \zeta' \in \mu_n(L)$, $\sigma \in G$, then $\sigma(\zeta\zeta') = \sigma(\zeta)\sigma(\zeta')$, so σ acts as an automorphism on $\mu_n(L)$, and $\sigma(\zeta_n) = \zeta_n \iff \sigma = \mathrm{id}$. So we have an injective homomorphism $G \hookrightarrow \mathrm{Aut}(\mu_n(L)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ by Lemma 11.1.

(iii) ζ_n^a is primitive if and only if $(a, n) = 1$, so the set of primitive n^{th} roots of 1 is the set $\{\zeta^a \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ which by (ii) equals the orbit of ζ under G. Hence the result follows.

□

Example 11.1. If $K = \mathbb{Q}$, take $L = \mathbb{Q}(e^{\frac{2\pi i}{n}})$. What is the minimal polynomial of $e^{2\pi/n}$?

Definition 11.1. Let K be a field satisfying the above earlier hypothesis. The n^{th} **cyclotomic polynomial** is $\Phi_n(T) = \prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}(T - \zeta_n^a)$ (where the roots are the primitive n^{th} roots of 1 in L, the splitting field for $T^n - 1$).

As G permutes the primitive n^{th} roots of 1 in L, $\Phi_n \in L^G[T] = K[T]$. So we can rephrase (iii) in Proposition 11.2 as saying that χ is surjective if and only if $\Phi_n \in K[T]$ is irreducible.

Φ_n doesn't really depend on K. In fact, $x \in L$ satisfies $x^n = 1$ if and only if x is a primitive root of 1 for some (unique) $d \mid n$. So

$$T^n - 1 = \prod_{d\mid n} \Phi_d \implies \Phi_n = \frac{T^n - 1}{\prod_{d\mid n, d\neq n} \Phi(d)}.$$

This gives an inductive definition of Φ_n and we see that Φ_n is the image in $K[T]$ of a polynomial in $\mathbb{Z}[T]$ which doesn't depend on K.

For example, $\Phi_p = \frac{T^p-1}{T-1} = T^{p-1} + T^{p-2} + \ldots + T + 1$, $\Phi_1 = T - 1$, and $\Phi_{p^n} = \frac{T^{p^n}-1}{T^{p^{n-1}}-1} = \Phi_p(T^{p^{n-1}})$. Also, $\deg(\Phi_n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, the Euler phi function.

We have two special cases:

Theorem 11.3 (Irreducibility of cyclotomic polynomials)**.** Let $K = \mathbb{Q}$. Then χ_n is an isomorphism for every $n > 1$. In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, and Φ_n is irreducible over $\mathbb{Q}$.

Proof. By Proposition 11.2, these statements are all equivalent. So it suffices to prove that Φ_n is irreducible over $\mathbb{Q}$. If n is prime (or a prime power), we can prove this using Eisenstein's criterion, but this doesn't work in the general case.

χ_n is an isomorphism if for all primes such that $(p, n) = 1$, the class of $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ lies in the image of χ (because we can factor a with $(a, n) = 1$ as a product of such primes).

Let f be the minimal polynomial of ζ over $\mathbb{Q}$, and g the minimal polynomial of ζ^p over $\mathbb{Q}$. If $f = g$, then ζ^a lies in the orbit of G on $\zeta \implies p$ is in the image of χ and we're done.

If $f \neq g$, then $(f, g) = 1$ and they both divide $T^n - 1$, so $fg \mid T^n - 1$. As ζ is a root of $g(T^p)$, $f \mid g(T^p)$. Reduce this modulo p to get $\overline{f} = f \pmod{p} \in \mathbb{F}_p[T]$ that divides $g(T^p) = \overline{g}(T)^p$ (as we're in characteristic p) and as both $\overline{f}$ and $\overline{g}$ divide $T^n - 1 \in \mathbb{F}_p[T]$, which is separable (as $p \nmid n$), this implies $\overline{f} \mid \overline{g}$. Hence $\overline{f}^2 \mid \overline{f}\overline{g} \mid T^n - 1$, contradicting separability of $T^n - 1$. Hence this case is impossible and we're done. □

So the minimal polynomial of $e^{2\pi/n}$ over $\mathbb{Q}$ is $\Phi_n(T)$. 10 Nov 2022, Lecture 16

Now we consider $K = \mathbb{F}_p$. Recall that $\phi_p \in G$ is the map $\phi(x) = x^p$, the Frobenius map, and ϕ_p generates G.

Proposition 11.4. Let $K = \mathbb{F}_p, (n, p) = 1$. Then

(i) $\chi_n : G \to \langle \phi \rangle \subset (\mathbb{Z}/n\mathbb{Z})^\times$ (the subgroup generated by a residue class mod p) and $\chi_n(\phi_p) = p \pmod{n}$.

(ii) $[L : K] = r$, the order of p mod n.

(iii) ϕ_p has cycle type $(r, \ldots, r)$ as a permutation of the roots of Φ_n.

Proof. $\phi_p(\zeta) = \zeta^p$, and $L = K(\zeta)$, so $\chi(\phi_p) = p$, hence $\chi_n(G) = \langle p \rangle$ and $[L : K] = |G| = |\langle p \rangle| =$ the order of p mod n. This implies (i) and (ii).

If $(a, n) = 1$, then when is $\phi_p^k(\zeta^a) = \zeta^a \iff \phi_p^k(\zeta) = \zeta \iff r \mid k$. So the orbits of ϕ_p on $\{\zeta^a \mid (a, n) = 1\}$, i.e. the set of roots of Φ_n, all have length r, which implies (iii). □

Remarks.

- This almost gives another proof of the irreducibility of Φ_n over $\mathbb{Q}$. By the reduction mod p theorem, $\mathrm{Gal}(\Phi_n/\mathbb{Q}) \supset \mathrm{Gal}(\Phi_n/\mathbb{F}_p)$ as subgroups (up to conjugacy) of the symmetric group $S_{\phi(n)}$. It is not hard to show that $\chi_n(\mathrm{Gal}(\Phi_n/\mathbb{Q})) \supset \chi_n(\mathrm{Gal}(\Phi_n/\mathbb{F}_p)) = \langle p \rangle$. As this holds for all $p \nmid n$, we get $\chi(\mathrm{Gal}(\Phi_n/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^\times$.
- (iii) implies that the factorization of Φ_n over $\mathbb{F}_p$ is $\prod$(irred. of degree r), which only depends on the order of p mod n. For a general polynomial

$f \in \mathbb{Z}[T]$, the factorization of f mod p doesn't follow any obvious pattern. Trying to answer this question is a part of the Langlands Program, and the case where there is a congruence pattern is when $\mathrm{Gal}(f/\mathbb{Q})$ is abelian ("Class Field Theory").

Application 1. Quadratic reciprocity.

Recall that if p is an odd prime and $a \in \mathbb{Z}$ with $(a,p)=1$, then the Legendre symbol is defined as $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p. \\ -1 & \text{if not.} \end{cases}$ Euler's formula says $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Now let $q \neq p$ be another odd prime and say $n = q$. Then $L = K(\zeta_q)$ is a splitting field for $f = T^q - 1 = (T-1)\Phi_q$. So on roots of f in L, the Frobenius map ϕ_p has cycle type $(1, r, \dots, r)$ with $\frac{q-1}{r}$ r–cycles. So its sign is $\mathrm{sgn}(\phi_p) = (-1)^{r-1} \cdot (q-1)/r = (-1)^{(q-1)/r}$ and $2 \mid \frac{q-1}{r} \iff r \mid \frac{q-1}{2} \iff p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$. So $\mathrm{sgn}(\phi_p) = \left(\frac{p}{q}\right)$ by Euler's formula. But as $G = \langle \phi_p \rangle$, $\mathrm{sgn}(\phi_p) = 1 \iff G \subset A_q$ (for $q = \deg(f)$). But this holds if and only if $\mathrm{Disc}(f)$ is a square in $\mathbb{F}_p$.

A lemma we prove on Example Sheet 3:

Lemma 11.5. Let $f = \prod^{(T-x_i)}$ over any field. Then

$$\mathrm{Disc}(f) = (-1)^{d(d-1)/2} \prod f'(x_i)$$

for $d = \deg(\mathrm{f})$.

So in our case, $f = T^q - 1 = \prod_{a=0}^{q-1}(T - \zeta_q^a)$ and $f' = qT^{q-1}$. So as q is odd,

$$\mathrm{Disc}(f) = (-1)^{q(q-1)/2} \prod_{a=0}^{q-1} q(\zeta_q^a)^{q-1} = (-1)^{(q-1)/2} q^q \zeta_q^{q-1} = (-1)^{\frac{q-1}{2}} q^q.$$

So $\left(\frac{p}{q}\right) = \left(\frac{\mathrm{Disc}(f)}{p}\right) = \left(\frac{(-1)^{(q-1)/2}q}{p}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$, which gives quadratic reciprocity.

This is essentially Stickelberger's proof, although he didn't have Galois theory.

Application 2. Construction of regular polygons.

Ruler–and–compass construction of a regular n–gon ($n \geq 3$) is equivalent to constructing $\cos(\frac{2\pi}{n})$.

Theorem 11.6 (Gauss)**.** A regular n–gon is constructible if and only if n is a power of 2 times a product of distinct primes, each of the form $2^{2^k} + 1$.

Remark. When is $F_k = 2^{2^k}+1$ prime? (These are called Fermat numbers). We have $F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$, which are all prime. Fermat conjectured that all F_k are prime. However, Euler showed that $F_5 = 641 \cdot 6700417$. Since then, many F_k's are known to be composite and none prime for $k > 4$.

12 Nov 2022, Lecture 17

Proof. Recall $x \in \mathbb{R}$ is constructible $\iff \exists$ fields $Q = K_0 \subset K_1 \subset \ldots \subset K_m \ni x$ and $[K_{i+1} : K_i] = 2\ \forall i$. In particular, a necessary condition is that $\deg_{\mathbb{Q}}(x)$ is a power of 2. In our case, $x = \cos(\frac{2\pi}{n}) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$ for $\zeta_n = e^{2\pi i/n}$, so $\zeta_n^2 - 2x\zeta_n + 1 = 0$.

We have $x \in \mathbb{R}, \zeta_n \neq \mathbb{R}$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(x)] = 2$. So if x is constructible, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is a power of 2, but if $n = \prod_{i=1}^r p_i^{e_i}$, then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = \prod_i p_i^{e_i - 1}(p-1).$$

So this is a power of 2 if and only if for all odd p_i, $e_i = 1$ and $p_i - 1$ is a power of 2.

Lemma 11.7. If m is a positive integer such that $2^m + 1$ is prime, then m has to be a power of 2.

Proof. $2^{qr} + 1 = (2^r + 1)(2^{qr-r} + 2^{qr-2r} + \ldots + 1)$ if q is odd. □

So we conclude that $\phi(n)$ is a power of 2 if and only if n is of the required form, so x being constructible implies n is of the required form.

For the other direction, suppose $\phi(n) = 2^m$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, with Galois group $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and $|G| = 2^m$. Observe that there exist subgroups $G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_n = \{e\}$ such that $[H_i : H_{i+1}] = 2\ \forall i$.

Indeed, as $2 \mid |G|$, $\exists \sigma \in G$ of order 2 (assuming $G \neq \{e\}$). Now take $H_{m-1} = \langle \sigma \rangle$. Then G/H_{m-1} contains a subgroup of order 2 by the same argument, which we call H_{m-2}/H_{m-1}. Continue this way to construct all H_i. Then $K_i = \mathbb{Q}(\zeta_n)^{H_i}$ satisfy $[K_{i+1} : K_i] = [H_i : H_{i+1}] = 2$, so we're done. □

12 Kummer extensions

Let $L = K(x)$, $x^n = a \in K$ (not necessarily $a = 1$). We know these extensions are not necessarily Galois, for example $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

Let us first prove a result of independent interest.

Theorem 12.1 (Linear independence of field embeddings)**.** Let K, L be fields and let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow L$ be distinct field homomorphisms. If $y_1, \ldots, y_n \in L$ such that $\forall x \in K$, $y_1\sigma_1(x) + \ldots + y_n\sigma_n(x) = 0$, then $y_i = 0\ \forall i$.

In other words, $\sigma_1, \dots, \sigma_n$ are L–linearly independent elements of the set of functions $K \to L$, which is an L–vector space.

This is the special case $G = K^\times$ of a theorem in II Representation Theory:

Theorem 12.2 (Linear independence of characters)**.** For G a group, L a field, $s_1, \dots, s_n : G \to L^\times$ group homomorphisms, we have that $\sigma_1, \dots, \sigma_n$ are linearly independent over L.

Proof. Induction on n. $n = 1$ is clear.

Now suppose that $n > 1$ and we have elements $y_1, \dots, y_n \in L$ such that $\forall g \in G$, $y_1\sigma_1(g) + \dots + y_n\sigma_n(g) = 0$ $(\star)$.

$\exists h \in G$ such that $\sigma_1(h) \neq \sigma_n(h)$. As σ_i are homomorphisms, substitute hg into $(\star)$ and we get

$$y_1\sigma_1(h)\sigma_1(g) + \dots y_n\sigma_n(h)\sigma_n(g).$$

Multiply $(\star)$ by $\sigma_n(h)$ and subtract to get

$$y_1'\sigma_1(g) + \dots + y_{n-1}'\sigma_{n-1}(g) = 0,$$

where $y_i' = y_i(\sigma_i(h) - \sigma_n(h))$. As $\sigma_1(h) \neq \sigma_n(h)$, $y_1 = 0$. Then $(\star)$ is a linear dependence between $\sigma_2, \dots, \sigma_n$, hence by induction, $y_2 = \dots = y_n = 0$. $\square$

Assume now that $n > 1$ and $n \cdot 1_K \neq 0$.

Theorem 12.3. Assume K contains a primitive n^{th} root $\zeta = \zeta_n$ of 1. Suppose L/K is an extension with $L = K(x)$, $x^n = a \in K^\times$. Then

(i) L/K is a splitting field for $f(T) = T^n - a$, and it is Galois with cyclic Galois group.

(ii) $[L : K]$ is the least $m \geq 1$ such that $x^m \in K$.

Proof. (i): As $\mu_n(K) = \{\zeta_n^i \mid 0 \leq i < n\}$ has n elements, f has n distinct roots $\{\zeta_i x\}$ in L. So L/K is a splitting field for the separable polynomial f, so it is Galois.

Let $\sigma \in \mathrm{Gal}(L/K) = G$. Then $f(\sigma(x)) = 0$, so $\sigma(x) = \zeta^i x$ for some i which is unique mod n. Define a map $\Theta : G \to \mu_n(K) = \{\zeta^i\} \cong \mathbb{Z}/n\mathbb{Z}$ by $\Theta(\sigma) = \frac{\sigma(x)}{x}$. The claim is that this is a homomorphism: let $\sigma, \tau \in G$, then as $\zeta \in K$, $\tau(\Theta(\sigma)) = \Theta(\sigma)$, so

$$\Theta(\tau\sigma) = \frac{\tau\sigma(x)}{x} = \tau\left(\frac{\sigma(x)}{x}\right)\frac{\tau(x)}{x} = \tau(\Theta(\sigma))\Theta(\tau) = \Theta(\sigma)\Theta(\tau).$$

So Θ is a homomorphism, and $\Theta(\sigma) = 1 \iff \sigma(x) = x \iff \sigma = \mathrm{id}$, hence Θ is injective. So G is isomorphic to a subgroup of a cyclic group, hence cyclic.

(ii): If $m \geq 1$, since L/K is Galois,

$$\begin{aligned} x^m \in K &\iff \forall \sigma \in G, \sigma(x^m) = x^m \iff \\ &\iff \forall \sigma \in G, \Theta(g)^m = 1 \iff |G| = [L : K] \text{ divides } m. \end{aligned}$$

$\square$