LECTURE NOTES (PART 3), MATH 500 (FALL 2022)

CHARLES REZK

1. Field extensions

M 31 Oct

A **subfield** of a field K is a subring $F \subseteq K$ which is also a field. This implies that the subring has 1, which is equal to the identity element of K. **subfield**

We say that K is an **extension field** of F if F is a subfield of K. The notation "K/F" means "K is an extension field of F", so it is the same as "$F \subseteq K$". We tend to represent this by the picture **extension field**

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Every field K contains a prime field $F \subseteq K$, which is the smallest subfield of K. The prime field is either isomorphic to $\mathbb{Q}$, which case we say $\mathrm{char}(K) = 0$, or is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p$, in which case we say $\mathrm{char}(K) = p$. Equivalently, $(\mathrm{char}\, K) = \mathrm{Ker}\, \phi$, where $\phi\colon \mathbb{Z} \to K$ is the unique ring homomorphism preserving 1.

Degree of an extension. If S is a ring and $R \subseteq S$ is a subring with $1_R = 1_S$, then the ring S also gets the structure of an R-module, via multiplication in S.

In particular, if $F \subseteq K$ is a field extension, K is naturally an F-vector space. We define the **degree** of the extension K/F to be **degree**

$$[K : F] := \dim_F K.$$

The extension is **finite** if $[K : F] < \infty$. **finite**

Example. We have $[\mathbb{C} : \mathbb{R}] = 2$, while $[\mathbb{R} : \mathbb{Q}]$ is uncountably infinite.

The following very important.

Proposition (Tower law)**.** *Suppose we have inclusions of field $F \subseteq K \subseteq L$. Then*

$$[L : F] = [L : K]\,[K : F]$$

Proof. Note: this formula is correct even for infinite degrees, but is mainly useful when all degrees are finite.

Let $\{\alpha_i\}_{i\in I}$ be a basis of K as an F-vector space, and let $\{\beta_j\}_{j\in J}$ be a basis of L as a K-vector space. I will show that the indexed collection $(\alpha_i\beta_j)_{i\in I,\, j\in J}$ is a basis of L as an F-vector space. (This will also show $\alpha_i\beta_j \neq \alpha_{i'}\beta_{j'}$ if $(i, j) \neq (i', j')$, and thus that the cardinality of this new basis is the product of the cardinalities of the original bases.)

Date: December 2, 2022.

To see this, write $x \in L$ as

$$\begin{aligned} x &= \sum_j x_j \beta_j, && x_j \in K, \\ &= \sum_j \left(\sum_i y_{ij} \alpha_i \right) \beta_j, && y_{ij} \in F, \\ &= \sum_{i,j} y_{ij}\, \alpha_i \beta_j, \end{aligned}$$

where there are only finitely many $j \in J$ such that $x_j \neq 0$, for each $j \in J$ only finitely many $i \in I$ such that $y_{ij} \neq 0$, and $y_{ij} = 0$ for all i if $x_j = 0$. Then there are only finitely many $(i,j) \in I \times J$ such that $y_{ij} \neq 0$. Thus we have shown that $\{\alpha_i \beta_j\}$ spans L over F.

Now suppose $0 = \sum_{i,j} y_{ij} \alpha_i \beta_j$. Then

$$0 = \sum_i \left(\sum_j y_{ij} \alpha_i \right) \beta_j,$$

so $\sum_j y_{ij} \alpha_i = 0$ for all j since $\{\beta_j\}$ is linearly independent. Then $y_{ij} = 0$ for all i and j since $\{\alpha_i\}$ is linearly independent. □

This gives rise to the general *tower law*.

Corollary (General tower law)**.** *If $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$, then $[L : F] = [K_r : K_{r-1}] \cdots [K_1 : K_0]$.*

2. Homomorphisms of fields

By a **homomorphism** of fields, we mean a ring homomorphism $\phi\colon K \to L$ between fields such that $\phi(1) = 1$. We have shown that such ϕ are always injective (since $\mathrm{Ker}(\phi) \subsetneq K$ is a proper ideal, and 0 is the only proper ideal in a field). Thus I will also call such maps **embeddings**. **homomorphism** **embeddings**

(This is just convenient language, so we don't confuse these from other kinds of homomorphisms of algebric objects. Also, it helps with the fact that DF still think that the constant map 0 should be a homomorphism.)

Write $\mathrm{Emb}(K, L)$ for the set of field embeddings of K into L.

Easy observation: every field embedding gives a field extension. If $\phi\colon F \to K$ is a field embedding, then it induces an isomorphism of fields $F \approx \overline{F}$, where $\overline{F} = \phi(F) \subseteq K$ is the image of ϕ, which is a subfield of K. So $K/\overline{F}$ is the extension associated to the embedding ϕ.

We write $\mathrm{Aut}(K)$ for the group of **automorphisms**, i.e., the bijective field homomorphism $\phi\colon K \to K$. **automorphism of a field**

Maps of extensions. If K/F and L/F are two extension fields of F, a **homomorphism of extensions** is a field homomorphism $\phi\colon K \to L$ such that $\phi|F = \mathrm{id}_F$. **homomorphism of extensions**

Given an extension K/F, we write $\mathrm{Aut}(K/F)$ for the group of isomorphisms of K which restrict to the identity of F. Thus $\mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$.

3. Construction of field extensions

Let F be a field. I am going to write $\mathrm{Irred}(F) \subseteq F[x]$ for the set of *monic and irreducible* polynomials over F.

Given $f \in \mathrm{Irred}(F)$, we can form

$$K := F[x]/(f).$$

Since f is irreducible, $(f) \subseteq F[x]$ is a maximal ideal, so the quotient is a field. The composite

$$F \rightarrowtail F[x] \twoheadrightarrow K$$

of the inclusion map with the quotient map is an embedding $F \to K$. We silently identify F with its image under this embedding, and thus we regard this as a field extension F/K.

This implies silent identification: we regard $F[x]$ as a subring of $K[x]$.

Write $\alpha := \overline{x} \in K$ for the coset $x + (f)$. Then we have

$$f(\alpha) = 0 \qquad \text{in } K.$$

In other words, by forming K we have "adjoined a root" of the irreducible polynomial f to F. Note that every element of K can be written in terms of α and elements of F, and in fact uniquely in the from

$$c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0, \qquad c_0, \ldots, c_{n-1} \in F, \quad n = \deg f.$$

Thus $[K : F] = n = \deg f$.

Remark. We can do "arithmetic" in K very easily. If we write elements of K in the above "canonical form", i.e., as an expression $c_{n-1}\overline{x}^{n-1} + \cdots + c_1\overline{x} + c_0$ with $c_k \in F$, then addition is given by componentwise addition of coefficients. To multiply we make use of the identity

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

Here is how you compute multiplicative inverses in K. Given $g \in F[x]$ with $\deg g < n$ and $g \neq 0$ and image $\overline{g} \in F[x]/(f)$, to compute $\overline{g}^{-1}$, use polynomial long division to find for each $k = 0, \ldots, n-1$,

$$x^k g = -s_k f + r_k, \qquad s_k, r_k \in F[x], \qquad \deg r_k < n.$$

Thus, each r_k is a "canonical form" representing the image of $x^k g$ in $K = F[x]/(f)$. Use linear algebra to solve for $c_k \in F$ such that

$$\sum_{k=0}^{n-1} c_k r_k = 1.$$

Then $\overline{g}^{-1} = \sum_{k=0}^{n-1} c_k \overline{x}^k$. (If you couldn't find a solution, then $\overline{g} = 0$.)

We can get another extension of F from $F[x]$. Let

$$F(x) := \operatorname{Frac} F[x],$$

the field of rational functions in one variable. The composite $F \rightarrowtail F[x] \rightarrowtail F[x]$ defines a field embedding, and thus we get a field extension $F(\alpha)/F$, where $\alpha = x$. We have that $[F(\alpha) : F]$ is infinite. (Note: not necessarily *countably* infinite, e.g., $[F(x) : F]$ is uncountable when F is an uncountable field. To prove this, show that $\{\, (x-c)^{-1} \mid c \in F \,\}$ is F-linearly independent in $F[x]$.)

Note that α is not the root of any non-zero polynomial $f \in F[x]$, basically by construction and the fact that $F[x]$ embeds in its fraction field.

4. Field extensions generated by a set

Given a field K and a subset $X \subseteq K$, the **subfield generated by** X is the intersection of all subfields which contain X.

subfield generated by X

Proposition. *The subfield generated by X is the subset of elements which can be obtained from X by a finite sequence of the arithmetic operations $+, -, \times, \div$ applied to $X \cup \{0, 1\}$. Such a subfield always contains the prime subfield of K.*

Proof. Straightforward: observe that the collection of elements obtain from $X \cup \{0, 1\}$ by arithmetic operations is a subfield, and contains any subfield containing X. □

Typically, we work relative to a fixed subfield. Thus given a field extension K/F and a subset $S \subseteq K$, we write $F(S) \subseteq K$ for the subfield of K generated by $F \cup S$. Typically S is finite, so we write

$$F(\alpha_1, \ldots, \alpha_n) \subseteq K$$

for the subfield generated by $F \cup \{\alpha_1, \ldots, \alpha_n\}$.

A **simple extension** is a K/F such that $K = F(\alpha)$ for a single element $\alpha \in K$. **simple extension**

Example. Consider $D \in \mathbb{Q}$. This has a sqaureroot in $\mathbb{C}$. Pick an element $\alpha \in \mathbb{C}$ such that $\alpha^2 = D$, and call it $\sqrt{D}$.

(If $D \geq 0$, then by convention we usually choose $\sqrt{D} > 0$, but if $D < 0$ there is no standard choice. It doesn't actually matter which root we use for $\sqrt{D}$ in what follows, but a choice needs to be made for the notation to make sense.)

Then we obtain a subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$. There are two cases.

(1) D is the square of an element of $\mathbb{Q}$, so $\sqrt{D} \in \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}$, and $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 1$.
(2) D is not the square of an element of $\mathbb{Q}$. Then every element $\alpha \in \mathbb{Q}(\sqrt{D})$ has a unique representation as
$$\alpha = a + b\sqrt{D}, \qquad a, b \in \mathbb{Q},$$
so $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$.

First: the subset $K = \{\, a + b\sqrt{D} \mid a, b \in \mathbb{Q} \,\}$ is a subfield of $\mathbb{C}$. Clearly it is an abelian subgroup, is closed under multiplication, and has 1. It remains to show it has multiplicative inverses.

Let $\alpha = a + b\sqrt{D} \neq 0$ with $a, b \in \mathbb{Q}$, and consider

$$\beta := \frac{a}{a^2 - b^2 D} + \frac{-b}{a^2 - b^2 D}\sqrt{D}.$$

This makes sense because $a^2 - b^2 D \neq 0$, since if not then $D = (a/b)^2$, which contradicts the hypothesis on D.

For uniqueness of the representation, note that if $a + b\sqrt{D} = 0$ for some $a, b \in \mathbb{Q}$, then either (i) $b = 0$, whence $a = 0$, or (ii) $b \neq 0$, whence $D = (\sqrt{D})^2 = (-a/b)^2$, which contradicts the hypothesis. Thus we must have $(a, b) = (0, 0)$.

Note: $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{E})$ iff $E = Dc^2$ for some $c \in \mathbb{Q} \smallsetminus \{0\}$. (*Exercise:* prove this.) Thus WLOG any of these fields has the form $\mathbb{Q}(\sqrt{D})$ for a *squarefree integer* D (i.e., $p^2 \nmid D$ for all primes p).

If $D \neq 1$ is a squarefree integer then $\sqrt{D} \notin \mathbb{Q}$ (by unique factorization in $\mathbb{Z}$, since $a^2 = Db^2$ for some $a, b \in \mathbb{Z}$ implies that any prime divides D an even number of times).

Example. I claim that

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{\, a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \,\},$$

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

The key fact I need is that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. This is just a direct calculation. That is, suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, so that $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Then

$$3 = (a^2 + 2b^2) + 2ab\sqrt{2} \qquad \Longrightarrow \qquad a^2 + 2b^2 = 3, \quad 2ab = 0.$$

But then $2ab = 0$ implies we must have either $3 = a^2$ or $3/2 = b^2$, i.e., that $\sqrt{3} \in \mathbb{Q}$ or $\sqrt{3/2} \in \mathbb{Q}$, but this is not the case.

Let $K = \{\, u + v\sqrt{3} \mid u, v \in \mathbb{Q}(\sqrt{2}) \,\}$. This is clearly a subring of $\mathbb{C}$ (with 1). To see that it is a subfield, let $\alpha = u + v\sqrt{3}$ with $u, v \in \mathbb{Q}(\sqrt{2})$. Then $u^2 - 3v^2 \neq 0$, since otherwise $3 = (u/v)^2$ and so $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then it is easy to check that

$$\alpha^{-1} = \frac{u}{u^2 - 3v^2} + \frac{-v}{u^2 - 3v^2}\sqrt{2} \in K.$$

Since $K = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, we have $[K : \mathbb{Q}(\sqrt{2})] = 2$ and so $[K : \mathbb{Q}] = [K : \sqrt{2}]\,[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 4$.

Exercise. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{2} + \sqrt{3}$. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a simple extenison.

Example. We have that $[\mathbb{Q}(\sqrt{8}, \sqrt{32}) : \mathbb{Q}] = 2$, since $\sqrt{32} = 2\sqrt{8} \in \mathbb{Q}(\sqrt{8})$.

Exercise. If $D, E \in \mathbb{Q}$, then $[\mathbb{Q}(\sqrt{D}, \sqrt{E}) : \mathbb{Q}] = 4$ iff $\sqrt{D}, \sqrt{E}, \sqrt{DE} \notin \mathbb{Q}$.

Example. $\mathbb{Q}(\sqrt[3]{2}) = \{\, a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q} \,\}$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Note that to show this, one must prove that the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is unique (i.e., that $\sqrt[3]{4} \neq a + b\sqrt[3]{2}$), and that multiplicative inverses of elements of that form have the same form. This can be done, but we will soon have a better method.

5. Algebraic and transcendental elements

F 4 Nov

Let K/F be a field extension, and suppose $\alpha \in K$. Consider the subfield $F(\alpha) \subseteq K$ generated over F by α. Observe that we can always evaluate a a polynomial $f \in F[x]$ at α.

There are two cases:

(1) There exists a non-zero $f \in F[x]$ such that $f(\alpha) = 0$. In this case we say that α is **algebraic** over F. **algebraic**

(2) There does not exist a non-zero $f \in F[x]$ such that $f(\alpha) = 0$. In this case we say that α is **transcendental** over F. **transcendental**

Proposition. *Let $\alpha \in K$ be algebraic over F. Then there exists a unique irreducible monic polynomial $m \in \mathrm{Irred}(F)$ such that $m(\alpha) = 0$. Furthermore, a polynomial $f \in F[x]$ has α as a root iff $m \mid f$ in $F[x]$.*

Proof. There exists a unique ring homomorphism $\psi\colon F[x] \to K$ (preserving 1), such that $\psi|F = \mathrm{id}_F$, and $\psi(x) = \alpha$. This homomorphism is given by evaluation: $\psi(f) = f(\alpha)$, and so $f(\alpha) = 0$ iff $f \in \mathrm{Ker}(\psi)$.

Since α is algebraic, $\mathrm{Ker}(\psi) \neq (0)$, so there exists a unique monic polynomial $m \in F[x]$ such that $(m) = \mathrm{Ker}(\psi)$.

By the isomorphism theorem, ϕ factors through a ring isomorphism

$$\phi\colon F[x]/(m) \xrightarrow{\sim} \phi(F[x]) \subseteq K.$$

Since $\phi(F[x])$ is a subring of a field (with 1), it is an integral domain. Thus $fg \in (m)$ implies either $f \in (m)$ or $g \in (m)$, and in particular m is irreducible. □

For any $\alpha \in K$ algebraic over F, we write $m = m_{\alpha/F} \in \mathrm{Irred}(F)$ for the unique monic irreducible such that $m(\alpha) = 0$. It is called the **minimal polynomial** of α over F. **minimal polynomial**

This proof also gives the following.

Proposition. *If $\alpha \in K$ is algebraic over F with minimal polynomial $m = m_{\alpha/F}$, then there is a unique isomorphism of F-extensions*

$$\phi\colon F[x]/(m) \xrightarrow{\sim} F(\alpha), \qquad \text{such that } \phi(\overline{x}) = \alpha.$$

As a consequence, $[F(\alpha) : F] = \deg m_{\alpha/F}$.

Proof. We already have a injective ring homomorphism

$$\phi\colon F[x]/(m) \rightarrowtail K, \qquad \phi(\overline{x}) = \alpha,$$

with m irreducible. We have shown that $F[x]/(m)$ is therefore a field, and thus its image $L \subseteq K$ in K is a subfield. Clearly $F[x]/(m)$ is the generated over F by $\overline{x}$, and thus L is generated over F by $\alpha = \phi(\overline{x})$.

□

Example. The real number $\alpha = \sqrt[3]{2}$ is a root of $f = x^3 - 2 \in \mathbb{Q}[x]$. This f has no roots in $\mathbb{Q}$, so is irreducible over $\mathbb{Q}$ since $\deg f = 3$. Therefore

$$\mathbb{Q}(\alpha) \approx \mathbb{Q}[x]/(f).$$

As a consequence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and all elements of $\mathbb{Q}(\alpha)$ have a unique expression $a + b\alpha + c\alpha^2$, $a, b, c \in \mathbb{Q}$.

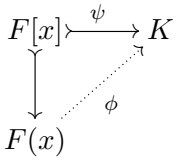
What if α is transcendental?

Proposition. *If $\alpha \in K$ is transcendental over F, then there is a unique isomorphism of F-extensions*

$$\phi\colon F(x) \xrightarrow{\sim} F(\alpha), \qquad \text{such that } \phi(x) = \alpha,$$

where $F(x) = \operatorname{Frac} F[x]$ is the field of rational functions in one variable over F. As a consequence, $[F(\alpha) : F]$ is infinite.

Proof. There is a unique ring homomorphism $\psi\colon F[x] \to K$ such that $\psi|F = \mathrm{id}_F$ and $\psi(x) = \alpha$. Because α is transcendental, $\operatorname{Ker}(\psi) = (0)$, so ψ is injective. Therefore ψ extends over the fraction field $F(x) = \operatorname{Frac} F[x]$:



□

We get a complete classification of simple extensions.

Proposition. *Suppose K/F is a field extension with $K = F(\alpha)$ for some $\alpha \in K$. There are two cases:*

1. *$[K : F] < \infty$. Then α is algebraic over F, and there is unique isomorphism of F-extensions of the form*
$$\phi\colon F[x]/(f) \to K, \qquad f = m_{\alpha/F} \in \operatorname{Irred}(F), \qquad \phi(\overline{x}) = \alpha.$$
2. *$[K : F] = \infty$. Then α is transcendental over F, and there is a unique isomorphism of F-extensions of the form*
$$\phi\colon F(x) \to K, \qquad \phi(x) = \alpha.$$

6. Finitely generated extensions

An extension K/F is a **finite extension** if $[K : F] < \infty$. **finite extension**

An extension K/F is a **finitely generated extension** if $K = F(\alpha_1, \ldots, \alpha_n)$ for some finite list of elements $\alpha_1, \ldots, \alpha_n \in K$. **finitely generated extension**

Note: every finite extension is finitely generated (use a vector space basis as the generating set). The converse is not true (e.g., a simple transcendental extension).

Proposition. *Let L/F be an extension, and $\alpha_1, \ldots, \alpha_n \in L$ a finite list of elements. Let $K = F(\alpha_1, \ldots, \alpha_n)$. Then TFAE.*

1. *$[K : F] < \infty$.*
2. *Every element $\beta \in K$ is algebraic over F.*
3. *The element α_k is algebraic over F for all $k = 1, \ldots, n$.*

Furthermore, if any of these hold, then $[K : F] \leq d_1 \cdots d_n$ where $d_j = \deg m_{\alpha_j/F}$.

Proof. (1) $\implies$ (2). If $\beta \in K$ then $[K : F] = [K : F(\beta)]\,[F(\beta) : F] < \infty$ implies $[F(\beta) : F] < \infty$, and thus β is algebraic over F.

(2) $\implies$ (3). Immeditae.

(3) $\implies$ (1). Let $K_j = F(\alpha_1, \ldots, \alpha_j)$. By the tower law $[K : F] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$. Since $\alpha_j \in K_j$ is algebraic over F, it is algebraic over K_{j-1}, since $F \subseteq K_{j-1} \subseteq K_j$. Thus $[K_j : K_{j-1}] = [K_{j-1}(\alpha_j) : K_{j-1}] < \infty$ for all $j = 1, \ldots, n$, so $[K : F] < \infty$.

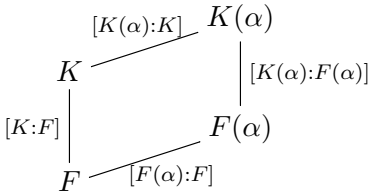
For the final statement, we use the following lemma to get that

$$[K_j : K_{j-1}] \leq [F(\alpha_j) : F] = d_j.$$

□

Lemma. *Let $F \subseteq K \subseteq L$ and $\alpha \in L$, such that α is algebraic over F and $[K : F] < \infty$. Then*

$$[K(\alpha) : K] \leq [F(\alpha) : F] \qquad \textit{and} \qquad [K(\alpha) : F(\alpha)] \leq [K : F].$$



Proof. We have $[F(\alpha) : F] = d = \deg m_{\alpha/F}$ and $[K(\alpha) : K] = e = \deg m_{\alpha/K}$. Since $m_{\alpha/K}$ is the minimal polynomial of α over K, it divides any polynomial $f \in K[x]$ which has α as a root. In particular, $m_{\alpha/K} \mid m_{\alpha/F}$ in $F[x]$, and so $e \leq d$. The second claim follows from the tower law: $[K(\alpha) : F(\alpha)]\,[F(\alpha) : F] = [K(\alpha) : K]\,[K : F]$. □

Given subfields $F \subseteq K, K' \subseteq L$, the **composite extension** is the subfield of L generated over F by $K \cup K'$. It is usually written $KK' \subseteq L$ (but be careful: it is *not* in general a set of linear combinations of products). **composite extension**

Clearly, if $K = F(\alpha_1, \ldots, \alpha_m)$ and $K' = F(\beta_1, \ldots, \beta_n)$, then $KK' = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$.

Proposition. *If K/F and K'/F are subextensions of L/F which are finite over F, then*

$$[KK' : K] \leq [K' : F], \qquad [KK' : K'] \leq [K : F], \qquad [KK' : F] \leq [K : F][K' : F].$$

Proof. Factor K'/F as a sequence of simple extensions $F = K'_0 \subseteq \cdots \subseteq K'_n = K'$ with $K'_j = K'_{j-1}(\alpha_j)$, and use the tower law and the previous lemma. □

7. Algebraic extensions

We say K/F is **algebraic** if every $\alpha \in K$ is algebraic over F. **algebraic extension**

We have seen that every *finite* extension is algebraic. There are, however, algebraic extensions which are not finite.

Example. An **algebraic number** is an $\alpha \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$, i.e., is the root of some non-zero $f \in \mathbb{Q}[x]$. **algebraic number**

Let $\mathbb{Q}^{\text{alg}}$ be the set of algebraic numbers. Then $\mathbb{Q}^{\text{alg}}$ is a subfield of $\mathbb{C}$, by the following proposition. The extension $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ is obviously algebraic, but is infinite.

That $\mathbb{Q}^{\text{alg}}$ is a subfield follows from the following.

Proposition. *If L/F is an extension and $\alpha, \beta \in L$ are algebraic over F, then $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$ are algebraic over F.*

Proof. Since $F(\alpha)/F$ and $F(\beta)/F$ are finite extensions, the composite extension $F(\alpha, \beta)/F$ is also finite and thus algebraic. Since $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1} \in F(\alpha, \beta)$, these are algebraic elements. □

Exercise. Let $p_1, \dots, p_r$ be distinct prime numbers. Show that $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}) : \mathbb{Q}] = 2^r$. This implies that $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ is an infinite extension.

Note: We can also say that $\mathbb{Q}^{\text{alg}} = \bigcup L$, where the union is over subfields $L \subseteq \mathbb{C}$ which are finite over $\mathbb{Q}$.

If we stack algebraic extensions, it is still algebraic.

Proposition. *If $F \subseteq K \subseteq L$ such that K/F and L/K are algebraic extensions, then L/F is an algebraic extension.*

Proof. Suppose $\alpha \in L$. Since L/K is algebraic, there exists a non-zero $f \in K[x]$ with α as a root. Write $f = \sum_{k=0}^{n} c_k x^k$ with $c_k \in K$, and let $F' = F(c_0, \dots, c_n)$. Since the c_k are in K they are algebraic over F, so $[F' : F] < \infty$, and thus $[F'(\alpha) : F] = [F'(\alpha) : F'] \, [F' : F] \leq (\deg f)[F' : F]$ is finite. Thus α is algebraic over F. □

8. Algebraically closed fields

We say that K is **algebraically closed** if every non-constant $f \in K[x]$ has a root in K. **algebraically closed**

If f has a root $c \in K$ then f factors as $(x - c)g \in K[x]$ with $g \in K[x]$, and we can apply the same argument to g (unless g is constant). Thus K is algebraically closed iff every non-zero polynomial over K **splits** over K, i.e., is a product of degree 1 polynomials. That is, if $\text{Irred}(K) = \{ x - c \mid c \in K \}$. **splits**

To check that K is algebraically closed, it sufffices to check only that all $f \in \text{Irred}(K)$ have a root in K.

Example. The complex numbers $\mathbb{C}$ is algebraically closed, by "The Fundamental Theorem of Algebra", which is really a theorem of analysis.

Proposition. *K is algebraically closed iff for any algebraic extension L/K we have $L = K$, iff for any $\alpha \in L$ in an extension L of K which is algebraic over K, we have $\alpha \in K$.*

Proof. If K is algebraically closed and $\alpha \in L$ in some algebraic extension L/K, then α is the root of some non-zero $f \in K[x]$, which splits over F and thus $\alpha \in K$. Therefore $L = K$.

Suppose K is such that the only algebraic extension L/K has $L = K$. If $f \in K[x]$ is non-constant, form $K(\alpha)/K$ where $f(\alpha) = 0$. Then by hypothesis $K(\alpha) = K$, whence $\alpha \in K$. □

Example. The field $\mathbb{Q}^{\text{alg}}$ of algebraic numbers is algebraically closed, since if α is algebraic over $\mathbb{Q}^{\text{alg}}$, then it is algebraic over $\mathbb{Q}$ (since $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ is an algebraic extenison).

9. Algebraic closure of fields

An **algebraic closure** is an extension $\overline{F}/F$ which is algebraic, and is such that every non-constant polynomial $f \in F[x]$ splits over $\overline{F}$, i.e., is a product of degree 1 factors. **M 7 Nov** **algebraic closure**

Recall that K is *algebraically closed* if every $f \in K[x]$ has a root in K (and thus splits over K).

Proposition. *Given an extension K/F, we have that K is an algebraic closure of F iff (i) K/F is algebraic, and (ii) K is algebraically closed. Algebraic closures are algebraically closed.*

Proof. $\Longrightarrow$. (i) is immediate from the definition. For (ii), suppose $f \in K[x]$ non-constant. We need to show f splits over K. Form an extension $K(\alpha)/K$ with α a root of f. Then since both $K(\alpha)/K$ and K/F are algebraic, so is $K(\alpha)/K$, so there exists a non-zero $g \in F[x]$ with $g(\alpha) = 0$. But by definition of algebraic closure, g splits over K, so $\alpha \in K$.

$\Longleftarrow$. Property (i) says K/F is algebraic. It remains to show that every non-constant $f \in F[x]$ splits over K, but this is immediate from (ii), since such an f is also in $K[x]$, and algebraic closure implies these split over K. □

Example. Any algebraically closed field is its own algebraic closure. Thus $\overline{\overline{F}} = \overline{F}$ for any F.

Example. The field $\mathbb{Q}^{\mathrm{alg}}$ of algebraic numbers is an algebraic closure of $\mathbb{Q}$, since $\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q}$ is algebraic and $\mathbb{Q}^{\mathrm{alg}}$ is algebraically closed.

Proposition. *If K/F is an extension and K is algebraically closed, then K contains a unique algebraic closure $\overline{F}$ of F, which is equal to the subset of elements which are algebraic over F.*

Proof. A special case of this is $F = \mathbb{Q}$, $K = \mathbb{C}$, and $\overline{F} = \mathbb{Q}^{\mathrm{alg}}$. The general proof is no different.

Let $\overline{F}$ be the set of all elements of K which are algebraic over F; this is a subfield (as we saw in the case of $\mathbb{Q}^{\mathrm{alg}}$). Note that any $\alpha \in K$ which is algebraic over $\overline{F}$ is also algebraic over F (since then α is algebraic over the finite subextension of F generated by coefficients of its minimal polynomial).

Thus for any $f \in \overline{F}[x]$, since it splits completely over K into linear factors $x - \alpha_i$ where the α_i are algebraic over $\overline{F}$, hence over F, we have that $\alpha_i \in \overline{F}$. Therefore $\overline{F}$ is algebraic over F (since any $f \in F[x]$ is also in $\overline{F}[x]$), and is algebraically closed. □

10. 2-radical extensions

We basically understand degree 2 extensions (as long as we are not in characteristic 2).

Proposition. *Let K/F be an extension, with $\mathrm{char}(F) \neq 2$ and $[K : F] = 2$. Then $K = F(\sqrt{d})$ for some $d \in F$ which is not a square in F.*

Proof. Because $[K : F] = 2$, we have $K = F(\alpha)$ for any $\alpha \in K \smallsetminus F$. Let $f = m_{\alpha/F} = x^2 + bx + c$ with $b, c \in F$, and let $d = b^2 - 4c$. Then

$$(2\alpha + b)^2 = 4\alpha^2 + 4b\alpha + b^2 = 4(-b\alpha - c) + 4b\alpha + b^2 = b^2 - 4c = d,$$

so we can set $\sqrt{d} := 2\alpha + b \in K$. Clearly $\sqrt{d} \notin F$, since otherwise we would have $\alpha = (-b + \sqrt{d})/2 \in F$. Thus $K = F(\sqrt{d})$. □

Remark. If $\mathrm{char}\, F = 2$, then if we try to do this it turns out that $\sqrt{d} = b \in F$, so it does not generate K over F.

Let's say that a finite extension K/F is **2-radical**[1] if there exists a finite tower of subfields of the form **2-radical extension**

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K, \qquad [K_j : K_{j-1}] = 2.$$

Example. In each of

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{Q}(\sqrt[16]{2}) \subseteq \cdots$$

and

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{1+\sqrt{2}}}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{2}}}}) \subseteq \cdots,$$

each intermediate extension has degree 2. (Exercise: prove this.)

Remark. If K/F is 2-radical then $[K : F] = 2^r$ for some r, but the converse is not true. (We will see an example later.)

Proposition. *If K/F and K'/F are finite subextensions of L/F which are 2-radical, then the composite extension is 2-radical.*

Proof. Factor K/F as a sequence of degree 2-extensions $K_j = K_{j-1}(\alpha_j)$ with $K_0 = F$ and $K_r = K$. Then we have a chain of extensions

$$K' = K'K_0 \subseteq K'K_1 \subseteq K'K_2 \subseteq \cdots \subseteq K'K_n = KK'.$$

Each intermediate extension is a simple extension since $K'K_j = K'K_{j-1}(\alpha_j)$, and we know that $[K'K_j : K'K_{j-1}] \leq [K_j : K_{j-1}] = 2$. □

[1] I don't think this is standard terminology.

Given $F \subseteq \mathbb{C}$, let

$$F^{2\text{rad}} = \bigcup_{\substack{F \subseteq L \subseteq \mathbb{C} \\ L/F \text{ is 2-radical}}} L.$$

Thus, $\alpha \in F^{2\text{rad}}$ iff and only if there exists a finite 2-radical extension $L : F$ with $\alpha \in L$. We see that $F^{2\text{rad}}$ is a subfield of $\mathbb{C}$, using that if L, L' are 2-radical extensions over F then so is LL'.

Say that a field K is **squareroot closed** if every element of K has a squareroot in K. **squareroot closed**

Proposition. *For $F \subseteq \mathbb{C}$, the subfield $F^{2\text{rad}}$ is the smallest subfield containing F which is squareroot closed.*

Proof. First, $F^{2\text{rad}}$ is clearly squareroot closed. If $\alpha \in F^{2\text{rad}}$, then there exists a finite 2-radical extension L/F with $\alpha \in L$, and then $L(\sqrt{\alpha})/F$ is also a 2-radical extension.

Let $L \subseteq \mathbb{C}$ be any squareroot closed subfield containing F. Clearly if $K \subseteq L$, and given K'/K with $[K' : K] = 2$, then $K' = K(\sqrt{d})$ for some $d \in K$, and so $K' \subseteq L$. Using this it is easy to see that any 2-radical extension of F is contained in L, so $F^{2\text{rad}} \subseteq L$. □

11. Straightedge and compass constructions

Greek geometers developed the notion of "straightedge and compass" constructions in plane geometry. The idea is that given a set $\mathcal{P}$ of points in the plane, you are allowed to construct:

- a line between any two distinct points of $\mathcal{P}$ ("straightedge"), and
- a circle with center at a point of $\mathcal{P}$ and radius r = distance between two given distinct points in $\mathcal{P}$ ("compass").

From this you get a bigger set of points $\mathcal{P}'$, which contains $\mathcal{P}$ as well as all points of intersection of the lines and circles you drew. You can iterate this to get a bigger set $\mathcal{P}''$ and so on, until you obtain the set $\overline{\mathcal{P}}$ of points which are "constructible from $\mathcal{P}$" by ruler and compass.

Note: you need at least 2 points in $\mathcal{P}$ to start with.

The problem is to use this to make geometric constructions. For instance, you can:

- Bisect an angle.
- Raise a perpendicular. (I.e., given two points, form a square with those two points as adjacent vertices.)
- Construct a regular triangle or regular pentagon.

The following problems were unsolved by Greek geometers (by straightedge and compass construction):

- Trisect an angle.
- "Square the circle." (I.e., given a circle, construct a square with the same area.)
- "Duplicate the cube." (I.e., given a line segment L construct a line segment L' so a cube with edge L' has twice the volume of a cube with edge L.)
- Construct a regular 7-gon.

In fact, these are all impossible.

Given a set of points $\mathcal{P}$ in the plane, designate two of them as 0 and 1, so that we can identify the plane with $\mathbb{C}$ and thus $\mathcal{P} \subseteq \mathbb{C}$. Let $F \subseteq \mathbb{C}$ be the subfield generated by the $\mathcal{P}$. (You can show that the subfield F doesn't depend on which points you choose as 0 and 1.) Then we get the following.

Theorem. *A point α is constructible from $\mathcal{P}$ iff $\alpha \in F^{2\text{rad}}$.*

If $\mathcal{P} = \{0, 1\}$, then this is $F^{2\text{rad}} = \mathbb{Q}^{2\text{rad}}$. We say that $\alpha \in \mathbb{C}$ is **constructible** if $\alpha \in \mathbb{Q}^{2\text{rad}}$. **constructible number**

The proof is involved. I like the account in Stewart, *Galois Theory.* (DF §13.3 talks about it too, but their way of setting things up is a little different.) The basic idea is:

(1) Show how to carry out field operations in $\mathbb{C}$ using ruler and compass constructions, and also how to calculate square roots. Thus all elements of $F^{2\text{rad}}$ are constructible from $\mathcal{P}$.

(2) Show that all all points constructible from $\mathcal{P}$ are in $F^{2\mathrm{rad}}$. This amounts to showing that computing intersection points of lines and/or cicles involves solving polynomial equations of degree at most 2.

Here are some impossibility results which follow from this, using only the fact that $\alpha \in \mathbb{Q}^{2\mathrm{rad}}$ must have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$.

- *Cannot duplicate the cube.* Given r we want to produce $r\sqrt[3]{2}$, i.e., to construct $\alpha = \sqrt[3]{2}$. But $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
- *Cannot trisect every angle.* In particular, $\theta = 2\pi/3$ cannot be trisected. This amounts to showing that $\zeta := e^{2\pi i/9}$ is not constructible.

  We know that $\zeta^9 = 1$, but $\zeta^3 \neq 1$. Since $0 = \zeta^9 - 1 = (\zeta^3 - 1)(\zeta^6 + \zeta^3 + 1)$, we see that ζ is a root of $f = x^6 + x^3 + 1 \in \mathbb{Q}[x]$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq 3$. Let $\alpha = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$. Using $f(\zeta) = 0$, you can show that
  $$\alpha^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha - 1.$$
  So α is a root of $g = x^3 - 3x + 1 \in \mathbb{Q}[x]$. By the rational roots test this has no root in $\mathbb{Q}$ so is irreducbile over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}]$, we see that 3 divides $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.
- *Cannot square the circle.* That is, given a circle with radius r, produce a square with side $\sqrt{\pi}\, r$. But $\sqrt{\pi}$ is not constructible. If it were, then it would be algebraic over $\mathbb{Q}$, and thus $\pi \in \mathbb{Q}(\sqrt{\pi})$ would be algebraic over $\mathbb{Q}$, but by Lindemann's theorem it is not.
- *Cannot construct the regular heptagon.* Show that $\zeta := e^{2\pi i/7} \notin \mathbb{Q}^{2\mathrm{rad}}$. Its minimal polynomial over $\mathbb{Q}$ is $\Phi_7 = x^6 + \cdots + x + 1$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.

Remark. If p is a prime number, then $\zeta_p = e^{2\pi i/p}$ satisfies
$$\mathbb{Q}(\zeta_p) = \deg \Phi_p = p - 1,$$
since Φ_p is irreducible over $\mathbb{Q}$. Thus, it is impossible to construct a regular p-gon for a prime p, unless it is a **Fermat prime**, i.e., of the form $p = 2^m + 1$. Examples include **Fermat prime**
$$3 = 2^1 + 1, \qquad 5 = 2^2 + 1, \qquad 17 = 2^4 + 1, \qquad 257 = 2^8 + 1, \qquad 65537 = 2^{16} + 1.$$
These are the only known examples, and it is unknown whether there are more. (Note that a Fermat prime must always have the form $2^{2^d} + 1$ for some d, because $a + 1 \mid a^k + 1$ whenever k is odd.)

12. Splitting fields

Let $f \in F[x]$ with $f \neq 0$. A **splitting field** of f is an extension Σ/F such that **splitting field**

- f *splits* over Σ, i.e., $f = c(x - \alpha_1) \cdots (x - \alpha_n)$ for some $c, \alpha_1, \ldots, \alpha_n \in \Sigma$ with $c \neq 0$, and
- Σ is generated over F by the roots of f, i.e., $\Sigma = F(\alpha_1, \ldots, \alpha_n)$. (Equivalently: the only subfield of Σ over which f splits is Σ itself.)

If a polynomial splits over some field then we certainly get a splitting field.

Proposition. *If L/F is an extension and $f \in F[x]$ splits over L, then the subfield $\Sigma = F(\alpha_1, \ldots, \alpha_n)$ generated by the roots of f in L is a splitting field of f.*

Proof. Obvious. □

Example. If $f = (x^2 + 1)(x^2 - 5) \in \mathbb{Q}[x]$, then $\Sigma = \mathbb{Q}(i, \sqrt{5})$ is a splitting field.

We always have an "abstract" construction of splitting fields.

Proposition. *Every non-zero polynomial $f \in F[x]$ admits a splitting field.*

Proof. We use induction on degree $n = \deg f$. If $n \leq 1$ take $\Sigma = F$.

Suppose $n \geq 2$. Let p be any irreducible factor of f, so $1 \leq \deg p \leq n$. Let $K := F[x]/(p) = F(\alpha_1)$ with $\alpha_1 = \overline{x}$, and view this as an extension of F.

Over K we have $f = (x - \alpha_1)g$, $g \in K[x]$ with $\deg g = n - 1$. By induction g has a splitting field Σ/K. I claim that Σ/F is a splitting field for F. Over Σ we have $g = c(x - \alpha_2) \cdots (x - \alpha_n)$ for $\alpha_2, \ldots, \alpha_n \in \Sigma$ and $c \in K^\times$, and $\Sigma = K(\alpha_2, \ldots, \alpha_n)$. Thus $f = c(x - \alpha_1) \cdots (x - \alpha_n)$ and $\Sigma = F(\alpha_1, \ldots, \alpha_n)$. □

This argument also shows the following.

Corollary. *If Σ/F is a splitting field of $f \in F[x]$, then $[\Sigma : F] \leq n!$ where $n = \deg f$.*

Proof. Induction on degree, using that if $\alpha \in \Sigma$ is a root of f, then $[F(\alpha) : F] = \deg m_{\alpha/F} \leq n$ and $\Sigma/F(\alpha)$ is a splitting field of a polynomial of degree $n - 1$, so $[\Sigma : F] = [\Sigma : F(\alpha)]\,[F(\alpha) : F] \leq (n-1)! \cdot n$. □

Notation: I will sometimes write $\Sigma = \Sigma_{f/F}$ for some choice of splitting field of $f \in F[x]$. (The splitting field is not unique. However, we will see that it is unique up to isomorphism.)

13. Examples of splitting fields

W 9 Nov

Example (Cyclotomic extensions). Let $\zeta \in L$ be a primitive nth root of unity, i.e., an element of order n in $L^\times$. Then for $F \subseteq L$, the subfield $K = F(\zeta)$ is the splitting field of $f = x^n - 1$.

This is because, since $|\zeta| = n$, the elements $1, \zeta, \ldots, \zeta^{n-1}$ are pairwise distinct, and are all clearly roots of f contained in K. Thus $f = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1})$ and clearly K is generated over F by the roots.

The degree of the extension $[F(\zeta) : F]$ will be less than n since $f = (x-1)g$ (unless $n = 1$).

Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. The field $\mathbb{Q}(\zeta_n)$ is called a **cyclotomic field**. We know that if $n = p$ is prime, then $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, since Φ_p is irreducible over $\mathbb{Q}$.

cyclotomic field

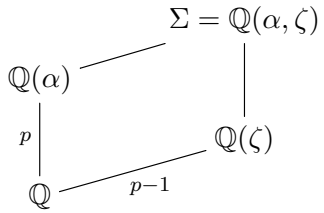
Example (Splitting field of $x^p - 2$). Let p be a prime number, and let $f = x^p - 2 \in \mathbb{Q}[x]$. Note that f is irreducible by Eisenstein's criterion.

If α is an root of this (e.g., $\sqrt[p]{2} \in \mathbb{R}$), so is $\alpha\zeta^k$ where ζ is some fixed primitive pth root of unity. That is, the roots of f in $\mathbb{C}$ are

$$\alpha,\ \alpha\zeta,\ \ldots,\ \alpha\zeta^{p-1}.$$

As these are distinct (since $\zeta^k \neq 1$ if $p \nmid k$), these are distinct roots of f, so $\Sigma = \mathbb{Q}(\alpha, \zeta)$ is a splitting field of f. (Note that $\zeta = (\alpha\zeta)\alpha^{-1}$ can be written in terms of roots of f, so it must be in the splitting field.)

We have the following diagram of subfields.



Since $[\Sigma : \mathbb{Q}(\zeta)] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, we have $[\Sigma : \mathbb{Q}] \leq (p-1)p$, but it is necessarily divisible by both p and $p - 1$, so (since these are relatively prime), $[\Sigma : \mathbb{Q}] = p(p-1)$.

14. Separable polynomials

Given a polynomial

$$f = a_0 + a_1 x + \cdots + a_n x^n \in F[x],$$

define its **formal derivative** by the formula

formal derivative

$$Df := a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in F[x].$$

Exercise. Check that the formal derivative satisfies: $D(f+g) = Df + Dg$, $D(fg) = (Df)g + f(Dg)$, $Dc = 0$ and $D(cf) = cD(f)$ if $c \in F$.

We say that a non-zero polynomial $f \in F[x]$ is **separable** if f and Df are relatively prime in $F[x]$. That is, if (f, Df) is the unit ideal in $F[x]$.

separable polynomial

Exercise. Show that if $f = gh \in F[x]$ and f is a separable polynomial, so are g and h.

Exercise. Show that any degree 1 polynomial is separable.

Remark. If $F \subseteq K$ and $f \in F[x]$, then f is separable as a polynomial over F iff it is separable as a polynomial over K.

To see this: (i) If f is separable over F, then $1 = uf + vD(f)$ for some $u, v \in F[x]$, and since this equation also holds in $K[x]$, f is also separable over K. (ii) If f is separable over K, then any common divisor $d \in F[x]$ of $\{f, D(f)\}$ is also a common divisor of these in $K[x]$, so $d \in F^\times$, and thus f is separable over F.

Thus, we don't need to say things like "separable over K", we just say *f is separable.*

Exercise. Show that if $\phi\colon F \to K$ is a homomorphism of fields, then $f \in F[x]$ is a separable polynomial iff $\phi(f) \in K[x]$ is a separable polynomial.

You probably know that $\alpha \in \mathbb{R}$ is a repeated root of some $f \in \mathbb{R}[x]$ if and only if α is a critical point of $\mathbb{R}$. This is actually a purely algebraic fact.

Proposition. *Let L/F be any extension over which $f \in F[x]$ splits. Then f is separable iff f has no multiple roots in L, iff f and Df have no common roots in L.*

Proof. Since $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ over L, it suffices to show for each k that $(x-\alpha_k)^2 \mid f$ iff $x - \alpha_k \mid Df$. In fact, since $f = (x-\alpha_k)h$ with $h \in L[x]$, we have

$$Df = h + (x-\alpha_k)(Dh),$$

so $(x-\alpha_k)^2 \mid f$ iff $(x-\alpha_k) \mid h$ iff $(x-\alpha_k) \mid Df$. □

Thus, we can say f is separable if and only if it has simple roots over its splitting field.

Example. The polynomial $f = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ has $Df = 4x^3 + 4x$. It is not hard to see (e.g., using the Euclidean algorithm) they have a common factor $x^2 + 1$. Thus f is not separable. In fact, $f = (x^2+1)^2$ over $\mathbb{Q}$, and $f = (x-i)^2(x+i)^2$ over $\mathbb{C}$, so all roots are multiple roots.

Example. The polynomial $f = x^n - 1$ is separable over $\mathbb{Q}$ since $Df = x^{n-1}$ and $x \nmid f$. Thus f has n distinct roots over $\mathbb{C}$, as we know.

Here is a generalization, which does not require passing to an extension where f splits.

Proposition. *A non-zero polynomial $f \in F[x]$ is separable iff for some irreducible factorization $f = g_1 \cdots g_n$ over F, we have that (i) each g_k is separable, and (ii) there are no repeated factors, i.e., if $i \neq j$ then $g_i \nmid g_j$.*

Proof. I'll show that an irreducible factor g of f divides Df iff either (i) g is not separable or (ii) $g^2 \mid f$. Given this, the claim is immediate from the existence of irreducible factorizations.

So let $g \in \mathrm{Irred}(F)$ such that $g \mid f$, so $f = gh$ for some $h \in F[x]$. The claim is immediate from the identity

$$Df = (Dg)h + g(Dh)$$

and the fact that g is a prime element of $F[x]$, so that $g \mid Df$ iff $g \mid (Dg)h$ iff ($g \mid Dg$ or $g \mid h$) iff ($g \mid Dg$ or $g^2 \mid f$). □

15. Irreducible separable polynomials

We would like to be able to say that irreducible polynomials are always separable. This is true for fields of characteristic 0, e.g., subfields of $\mathbb{C}$, but it not *quite* true generally.

Proposition. *Suppose $f \in F[x]$ is irreducible. Then f is separable iff $Df \neq 0$.*

In particular, if $\mathrm{char}\, F = 0$*, all irreducible polynomials over F are separable.*

Proof. We have that $\deg Df < \deg f$, and if also $Df \neq 0$ we have $f \nmid Df$. Since f is irreducible, this means f and Df are relatively prime. If instead $Df = 0$, then f and Df are not relatively prime since $f \mid Df$. □

The problem with non-0 characteristic is that it is *not* generally the case that $\deg Df = \deg f - 1$, and in fact it is possible that $Df = 0$ even when f is not a constant polynomial.

Example. Consider a field of prime characteristic p and

$$f = x^p - a \in F[x], \qquad a \in F.$$

Then $Df = px^{p-1} = 0$, so $\deg Df = -\infty$ rather than $p - 1$. So f actually does divide Df in this case. So f is not separable.

Let b be a root of f in some extension field $K = F(b)$. Then $b^p = a$, and in fact

$$(x-b)^p = \sum_{j=0} \binom{p}{j} x^j (-b)^j = x^p + (-1)^p b^p = x^p - b^p = x - a = f.$$

Thus f can only have *one* root in any splitting field, which has multiplicity p. (Note: $(-1)^p \equiv -1 \mod p$ for every prime p, but the reason is different depending on whether p is odd or even!)

It turns out that there are actually *irreducible* polynomials of this form. In fact, we'll show later that in the above setup, if $b \notin F$ then f is irreducible over F. As an example, consider the field $F = \mathbb{F}_p(t)$ of rational functions over $\mathbb{F}_p$ and let $f = x^p - t \in F[x]$. It turns out that t does not have a pth root in F, and so f is irreducible over F but not separable. (We will discuss this example soon.)

You can tell immediately from the form of a polynomial in finite characteristic when its derivative is 0.

Proposition. *If $f \in F[x]$ with* $\mathrm{char}\, F = p \neq 0$*, then $Df = 0$ iff $f = \sum_{k=0}^{n} c_k x^{pk}$, iff $f = g(x^p)$ for some $g \in F[x]$.*

Example. Let $n \geq 1$ and $f = x^n - 1 \in F[x]$. For $\mathrm{char}\, F = p \neq 0$, the polynomial f is separable as long as $p \nmid n$.

On the other hand, $x^p - 1 = (x-1)^p$. So in characteristic p, there are no *primitive* pth roots of unity.

16. Homomorphisms from simple finite extensions

Given an embedding $\lambda\colon F \rightarrowtail F'$ of fields, we get an induced homomorphism of polynomial rings, which by abuse of notation we also call λ:

$$\lambda\colon F[x] \to F'[x], \qquad \lambda(\sum c_k x^k) := \sum \lambda(c_k) x^k, \qquad c_k \in F.$$

Proposition. *Let $F(\alpha)/F$ be a finite extension, where α has minimal polynomial $m \in F[x]$. Suppose given an embedding of fields $\lambda\colon F \rightarrowtail F'$, and an extension L/F'. Let $m' = \lambda(m) \in F'[x]$.*

Then for any root root $\beta \in L$ of m', there exists a unique embedding $\mu\colon F(\alpha) \to L$ such that $\mu|F = \lambda$ and $\mu(\alpha) = \beta$.

$$\begin{array}{ccc} F(\alpha) & \overset{\alpha\mapsto\beta}{\underset{\mu}{\dashrightarrow}} & L \\ | & & | \\ F & \xrightarrow[\lambda]{} & F' \end{array}$$

That is, there is a bijection

$$\left\{ \begin{array}{c} \mu\colon F(\alpha) \rightarrowtail L \\ \text{such that } \mu|F = \lambda \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \beta \in L \\ \text{such that } m'(\beta) = 0 \end{array} \right\}$$

$$\mu \longmapsto \mu(\alpha)$$

In particular, the number of such homomorphisms is equal to the number of distinct roots of $m' = \lambda(m)$ in L.

Proof. Recall that there is an isomorphism $F(\alpha) \approx F[x]/(m)$ of extensions of F, under which α corresponds to $\overline{x}$. WLOG we can assume $F(\alpha) = F[x]/(m)$.

Now we use various universal properties to describe ring homomorphisms (preserving 1) of the form $\mu\colon F[x]/(m) \to L$. In particular, given $\lambda\colon F \to F' \subseteq L$ and $\beta \in F$, there exists a unique ring homomorphism

$$\widetilde{\mu}\colon F[x] \to L, \qquad \widetilde{\mu}|F = \lambda', \quad \widetilde{\mu}(x) = \beta.$$

By the homomorphism theorem for quotients, this factors through the quotient map $F[x] \to F[x]/(m)$ iff $\widetilde{\mu}(m) = 0$. Since $\widetilde{\mu}(m) = \lambda(m)(\beta) = 0$, such a factorization $\mu\colon F[x]/(m) \to L$ exists iff $m'(\beta) = 0$, and there is only one such factorization.

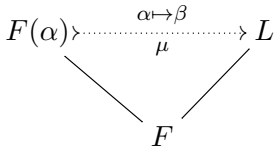
$$\begin{array}{ccc} & F[x]/(m) & \\ \nearrow & & \overset{\overline{x}\mapsto\beta}{\searrow} \\ F[x] & \overset{x\mapsto\beta}{\underset{\widetilde{\mu}}{\dashrightarrow}} & L \\ \uparrow & & \uparrow \\ F & \xrightarrow[\lambda]{} & F' \end{array}$$

□

Often we just need the special case when $\lambda = \mathrm{id}_F$.

Corollary. *Let $F(\alpha)/F$ be a finite extension, where α has minimal polynomial $m \in F[x]$. Suppose an extension L/F.*

Then for any root root $\beta \in L$ of m, there exists a unique embedding $\mu\colon F(\alpha) \to L$ such that $\mu|F = \mathrm{id}_F$ and $\mu(\alpha) = \beta$.



That is, there is a bijection

$$\left\{ \begin{array}{c} \mu\colon F(\alpha) \to L \\ \text{such that } \mu|F = \mathrm{id}_F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \beta \in L \\ \text{such that } m(\beta) = 0 \end{array} \right\}$$

$$\mu \longmapsto \mu(\alpha)$$

In particular, the number of such homomorphisms is equal to the number of roots of m in L.

Example. Let $f = x^3 - 2 \in \mathbb{Q}[x]$, and let $\alpha = \sqrt[3]{2}$. Since $f = m_{\alpha/\mathbb{Q}}$, there are *three* distinct embeddings $\mu\colon \mathbb{Q}(\alpha) \to \mathbb{C}$, corresponding to the roots $\alpha, \alpha\omega, \alpha\omega^2$, where $\omega = e^{2\pi i/3}$.

17. Homomorphisms from splitting fields

F 11 Nov

Given a finite extension K/F, we now have a recipe for constructing homomorphisms of extensions $K \to L$ over F: write K/F as a composite of simple extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = K, \qquad K_j = K_{j-1}(\alpha_j),$$

and *inductively* construct homomorphisms $\phi_j\colon F(\alpha_1, \ldots, \alpha_j) \to L$ extending ϕ_{j-1}. At each step there is one choice: $\phi_j(\alpha_j) \in L$ can be any root of $m_{\alpha_j/K_{j-1}}$.

Proposition. *Consider*

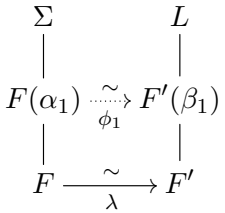
- *an isomorphism of fields $\lambda\colon F \xrightarrow{\sim} F'$,*
- *a non-zero polynomial $f \in F[x]$,*
- *a splitting field Σ/F of f, and*
- *an extension L/F' over which $f' = \lambda(f) \in F'[x]$ splits.*

Then there exists a homomorphism $\phi\colon \Sigma \to L$ such that $\phi|F = \lambda$. The image $\phi(\Sigma)$ of ϕ is a splitting field of f' over F'.

Proof. We use induction on $\deg f$. If f is constant, then $\Sigma = F$ and we take $\phi = \lambda$. So suppose $\deg f \geq 1$, whence $\deg f' = \deg f \geq 1$.

Let α_1 be some root of f in Σ, and let $m = m_{\alpha_1/F} \in \mathrm{Irred}(F)$ be its minimal polynomial. Then $f = mg$ for some $g \in F[x]$. Under $\lambda\colon F[x] \to F'[x]$ we get a factorization $f' = m'g'$ with $m' = \lambda(m)$. By hypothesis f' splits over L, so we choose a root $\beta_1 \in L$ of m'.

By the previous proposition, there exists an isomorphism ϕ_1 fitting in



(It is an isomorphism because $F'(\beta_1) = \phi_1(F(\alpha_1))$ is the image of ϕ_1.) We can factor $f = (x - \alpha_1)h$ over $F(\alpha_1)$. Now note that we are in the same sitation: we have

- an isomorphism of fields $\phi_1\colon F(\alpha_1) \to F'(\beta_1)$,
- a nonzero polynomial $h \in F(\alpha_1)[x]$,

- a splitting field $\Sigma/F(\alpha_1)$ of h, and
- an extension $L/F'(\alpha_1)$ over which $\phi_1(h)$ splits.

Since $\deg h < \deg f$, induction applies to produce the desired homomorphism ϕ. □

This is important even when $F = F'$ and $\iota = \mathrm{id}_F$. In this case, we see that there is an embedding of extensions $\Sigma \to L$ whenever g splits over L. In particular, we learn that any two splitting fields of f are isomorphic.

Corollary. *Let Σ/F and Σ'/F be two splitting fields for the same non-zero polynomial $f \in F[x]$. Then Σ and Σ' are isomorphic as extensions over F.*

Proof. By the previous proposition, there exists a map $\phi\colon \Sigma \to \Sigma'$ of F-extensions, whose image $\phi(\Sigma)$ is a splitting field of F, and thus $\phi(\Sigma) = \Sigma'$. □

Important: this isomorphism of splitting fields is not generally unique. In particular, $\mathrm{Aut}(\Sigma/F)$ is usually not a trivial group.

Notation: I sometimes write $\Sigma = \Sigma_{f/F}$ for any choice of a splitting field of $f \in F[x]$.

18. Automorphisms of field extensions

Proposition. *Suppose $G \leq \mathrm{Aut}(K)$ is a group of automorphisms of a field K. Then the set $K^G := \{\, \alpha \in K \mid g(\alpha) = \alpha,\ \forall g \in G \,\}$ is a subfield of K.*

We call K^G the **fixed field** of the action of the group G. **fixed field**

We have seen that if $\phi \in \mathrm{Aut}(K/F)$ is an automorphism of a field extension, and if $\alpha \in L$ is a root of some $f \in F[x]$, then $\phi(\alpha)$ is also a root of f. We can apply this observation to spltting fields.

Proposition. *Let $f \in F[x]$, and let $R_f = \{\, \alpha \in K \mid f(\alpha) = 0 \,\}$ be the set of roots of f in some extension K/F. Then any $\phi \in \mathrm{Aut}(K/F)$ restricts to a permutation of the set R_f, and this defines a group homomorphism*

$$\iota\colon \mathrm{Aut}(K/F) \to \mathrm{Sym}(R_f).$$

Furthermore, if $K = F(R_f)$ (i.e., if K is a splitting field of f), then ι is injective, so $\mathrm{Aut}(K/F)$ is isomorphic to a subgroup of $\mathrm{Sym}(R_f)$.

Proof. It is clear that restricting to $R_f \subseteq K$ defines such a homomorphism, since $\phi(\alpha)$ is a root of f whenever α is, and vice-versa by considering ϕ^{-1}.

For injectivity, note that if $\phi \in \mathrm{Aut}(K/F)$ satisfies $\phi(\alpha) = \alpha$ for all roots α of f, then $R_f \subseteq K^G$ and $F \subseteq K^G$, where $G = \langle \phi \rangle \leq \mathrm{Aut}(\Sigma/F)$ is the cyclic subgroup generated by ϕ. Since K^G is a subextension of K containing the roots of f we must have $F(R_f) \subseteq K^G$, so when $K = F(R_f)$ we have $\phi = \mathrm{id}$. □

19. Examples of automorphisms of field extensions

We can use the techniques we have developed to compute the automorphism groups of some field extensions.

Example (Important). Consider $g = x^3 - 2 \in \mathbb{Q}[x]$. This factors

$$g = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha),$$

where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/3}$. Thus $\Sigma = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{C}$ is the splitting field. In fact, Σ is generated over $\mathbb{Q}$ by any two of the roots, since any quotient α_i/α_j with $i \neq j$ is either ω or ω^{-1}. Earlier we showed that $[\Sigma : \mathbb{Q}] = 6$, since it contains the subfield $\mathbb{Q}(\omega)$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

There are *six* distinct embeddings $\Sigma \to \mathbb{C}$. One of them is the "obvious" inclusion, but there are others. We construct them in two steps, as indicated in the following diagram.

$$\begin{array}{ccc} \mathbb{Q}(\alpha,\omega\alpha) & \overset{\omega\alpha\mapsto ?}{\dashrightarrow} & \Sigma \\ | & & | \\ \mathbb{Q}(\alpha) & \overset{\alpha\mapsto ?}{\dashrightarrow} & \mathbb{Q}(\phi(\alpha)) \\ | & & | \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$

with two places to make choices. The possible choices are:

$\phi(\alpha)$	α	α	$\omega\alpha$	$\omega\alpha$	$\omega^2\alpha$	$\omega^2\alpha$
$\phi(\omega\alpha)$	$\omega\alpha$	$\omega^2\alpha$	α	$\omega^2\alpha$	α	$\omega\alpha$
$\phi(\omega^2\alpha)$	$\omega^2\alpha$	$\omega\alpha$	$\omega^2\alpha$	α	$\omega\alpha$	α

First construct $\phi_1\colon \mathbb{Q}(\alpha) \to \mathbb{C}$ sending α to some root of g, so $\phi_1(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$.

Consider the case of $\phi_1(\alpha) = \alpha$. Over $\mathbb{Q}(\alpha)$ we have

$$g = (x-\alpha)g_1, \qquad g_1 = x^2 + \alpha x + \alpha^2,$$

so that the roots of g_1 in $\mathbb{C}$ are $\{\omega\alpha, \omega^2\alpha\}$. In fact, g_1 is irreducible over $\mathbb{Q}(\alpha)$. We know this is true because we know that $[\Sigma : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, whence $[\Sigma : \mathbb{Q}(\alpha)] = 2$ by the tower law. Since Σ is generated over $\mathbb{Q}(\alpha)$ by $\omega\alpha$, we conclude that $m_{\omega\alpha/\mathbb{Q}(\alpha)}$ has degree 2. Since $g_1(\omega\alpha) = 0$ we conclude that $g_1 = m_{\omega\alpha/\mathbb{Q}(\alpha)}$. Thus we can construct $\phi\colon \mathbb{Q}(\alpha,\omega\alpha) \to \Sigma$ extending ϕ_1 so that $\phi(\omega\alpha) \in \{\omega\alpha, \omega^2\alpha\}$.

In general, if $\phi_1(\alpha) = \omega^k\alpha$, then $\phi(g_1) = x^2 + \omega^k\alpha x + \omega^{2k}\alpha^2$, whose roots are $\{\alpha, \omega\alpha, \omega^2\alpha\} \smallsetminus \{\omega^k\alpha\}$, and is irreducible over $\mathbb{Q}(\omega^k\alpha)$ because $[\Sigma : \mathbb{Q}(\omega^k\alpha)] = 2$. Thus we can construct $\phi\colon \mathbb{Q}(\alpha,\omega\alpha) \to \mathbb{C}$ extending ϕ_1, so that $\phi(\omega\alpha)$ is one of the roots of g_1.

The image of ϕ is $\mathbb{Q}(\alpha,\omega\alpha)$ again, since the images of the roots of g are still roots of g.

The above argument shows that $G = \mathrm{Aut}(\Sigma/\mathbb{Q})$ is a group of order 6, and examining the possible formulas for $\phi \in G$, we see that $G \approx S_3$. In fact, if we label the roots of g as $\alpha_1 = \alpha$, $\alpha_2 = \omega\alpha$, $\alpha_3 = \omega^2\alpha$, then for every $\sigma \in S_3$ there is a unique $\phi \in G$ such that $\phi(\alpha_k) = \alpha_{\sigma(k)}$.

Example. Consider $g = (x^2-2)(x^2-3) \in \mathbb{Q}$, with roots $\pm\sqrt{2}, \pm\sqrt{3}$. The splitting field is $\Sigma = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Earlier we showed that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ so $[\Sigma : \mathbb{Q}] = 4$.

We can construct isomorphisms $\phi\colon \Sigma \to \Sigma$ according to the diagram:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2},\sqrt{3}) & \overset{\sqrt{3}\mapsto ?}{\dashrightarrow} & \Sigma \\ | & & | \\ \mathbb{Q}(\sqrt{2}) & \overset{\sqrt{2}\mapsto ?}{\dashrightarrow} & \mathbb{Q}(\phi(\sqrt{2})) \\ | & & | \\ \mathbb{Q} & = & \mathbb{Q} \end{array}$$

The choices here are described by

$\phi(\sqrt{2})$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\phi(\sqrt{3})$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$

The first choice gives $\phi_1\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ sending $\sqrt{2}$ to a root of $g_1 = x^2 - 2$. Note that the image of ϕ_1 is $\mathbb{Q}(\sqrt{2})$ under either case.

The remaining factor of g is $g_2 = x^2 - 3 \in \mathbb{Q}[x]$, so we have that $\phi_1(g_2) = g_2$. This remains irreducible over $\mathbb{Q}(\sqrt{2})$ since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Thus the second choice extends to $\phi_2\colon \mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{C}$ sending $\sqrt{3}$ to a root of g_2.

Using this, we see that $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \approx C_2 \times C_2$.

Example. Consider $g = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. We see $g \in \mathrm{Irred}(\mathbb{Q})$ by the rational roots test, and since g is separable it has three distinct roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. Picking a root at random, we get three choices of homomorphism $\phi\colon \mathbb{Q}(\alpha_1) \to \mathbb{C}$, determined by $\phi(\alpha_1) \in \{\alpha_1, \alpha_2, \alpha_3\}$.

What may not be obvious is that g already *splits* over $\mathbb{Q}(\alpha_1)$. In fact, it turns out that the roots of this polynomial are

$$\alpha_1 = \zeta + \zeta^{-1}, \qquad \alpha_2 = \zeta^2 + \zeta^{-2}, \qquad \alpha_3 = \zeta^3 + \zeta^{-3}, \qquad \zeta = e^{2\pi i/7}.$$

(These are actually all real numbers. All you need to check this is that $\zeta^7 = 1$ and $\zeta \neq 1$.) Using this you can check that: $\alpha_2 = \alpha_1^2 - 2$, $\alpha_3 = \alpha_2^2 - 2$. Thus $\Sigma = \mathbb{Q}(\alpha_1)$ is already a splitting field of g, and a homomorphism $\phi\colon \Sigma \to \Sigma$ is determined by where it sends α_1. The possible choices are:

$\phi(\alpha_1)$	α_1	α_2	α_3
$\phi(\alpha_2)$	α_2	α_3	α_1
$\phi(\alpha_3)$	α_3	α_1	α_2

Thus $[\Sigma : \mathbb{Q}] = 3$ and $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \approx C_3$.

Question: what if we didn't already know the roots of g? How could we have analyzed this in that case?

Example. $x^4 - 2 \in \mathbb{Q}[x]$. Here the roots are $\{\pm\alpha, \pm i\alpha\}$, where $\alpha = \sqrt[4]{2}$. In this case, we can show that $[\Sigma : \mathbb{Q}] = 8$ and $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \approx D_8$. I'll leave this as an exercise, except to note that this relies on the chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, i), \qquad [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4, \quad [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2.$$

(Note that $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ so $i \notin \mathbb{Q}(\alpha)$.)

20. Normal extensions

We noted that a given finite extension can be the splitting field of many different polynomials. There is an abstract characterization of when such an extension is a splitting field, which doesn't require mentioning a particular polynomial.

An algebraic extension L/F is **normal** if every $f \in \mathrm{Irred}(F)$ which has a root in L splits in L. **normal**

Note: this definition is different than as given in DF, but is equivalent to their definition as I will show.

Example. $\mathbb{Q}^{\mathrm{alg}}/F$ for any subfield $F \subseteq \mathbb{Q}^{\mathrm{alg}}$ is a normal extension, since it is an algebraic extension and all polynomials over $\mathbb{Q}^{\mathrm{alg}}$ (and hence over F) split in $\mathbb{Q}^{\mathrm{alg}}$.

Exercise. Show that every degree 2 extension is normal.

Example. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, since $f = x^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$.

Theorem. *A finite extension L/F is normal if and only if it is a splitting field for some polynomial $f \in F[x]$.*

Proof part 1: Finite normal extensions are splitting fields: If L/F is a finite extension then

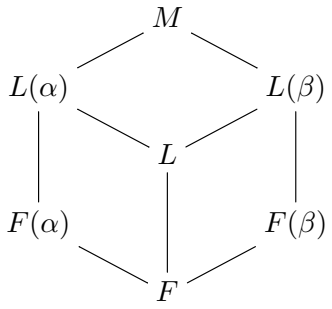
$$L = F(\alpha_1, \ldots, \alpha_m)$$

for some finite list of elements $\alpha_1, \ldots, \alpha_m \in L$. Let $f = \prod_{k=1}^m m_{\alpha_k/F} \in F[x]$, the product of minimal polynomials of these elements. Normality of L/F says thet each $m_{\alpha_k/F}$ splits over L, and thus f splits over L. Since L/F is generated by the α_ks, it is clear L/F is a splitting field of f. □

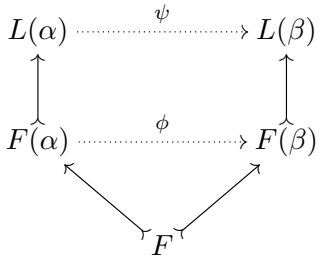
We get the second part as a special case of a more general claim.

Lemma. *Suppose $F \subseteq L \subseteq M$, where $L = \Sigma_{f/F}$ is a splitting field of some $f \in F[x]$. If $\alpha, \beta \in M$ are roots of the same irreducible polynomial $g \in \mathrm{Irred}(F)$, then $[L(\alpha) : L] = [L(\beta) : L]$.*

Proof. Consider the following diagram of subfields of M.



To prove the result it suffices to show that $[F(\alpha) : F] = [F(\beta) : F]$ and $[L(\alpha) : F(\alpha)] = [L(\beta) : F(\beta)]$, using the tower law. In fact, I claim there exist isomorphisms ϕ and ψ which are compatible with the inclusions in



That is, $\phi|_K$ is the inclusion of the subfield $K \subseteq K(\beta)$, and $\psi|_{K(\alpha)}$ is ϕ.

In fact, there exists $\phi\colon F(\alpha) \to F(\beta)$ sending $\phi(\alpha) = \beta$, because α, β are both roots of $g \in \mathrm{Irred}(F)$.

Note that $\phi(f) = f$ since $f \in F[x]$, and that both $L(\alpha)/F(\alpha)$ and $L(\beta)/F(\beta)$, being generated over the ground fields by roots of f, are splitting fields of f relative to their subfields. Thus by previous theory, ϕ extends to an isomorphism ψ. □

Proof of part 2: splitting fields are normal extensions. Suppose L/F is a splitting field of $f \in F[x]$, and $g \in \mathrm{Irred}(F)$ is some irreducible polynomial with root $\alpha \in L$.

Form a splitting field Σ/L of the polynomial $g \in F[x] \subseteq L[x]$. If β is any root of g in Σ, the previous lemma says

$$[L(\alpha) : L] = [L(\beta) : L].$$

But $\alpha \in L$ so these are 1, so $\beta \in L$. Thus all roots of g are in L, so g splits over L as desired. □

As a consequence, a splitting field Σ/F contains a splitting field for *any* $f \in \mathrm{Irred}(F)$ which has a root in Σ.

We can generalize this to infinite extensions.

Theorem. *An algebraic extension L/F is normal iff it is a splitting field for a set $S \subseteq F[x] \setminus \{0\}$ of polynomials, i.e., if all $f \in S$ split over L and L is generated over F by the roots of all $f \in S$.*

Proof. $\Longrightarrow$: Let $S = \{\, m_{\alpha/F} \mid \alpha \in L \,\}$, the set of all minimal polynomials of all elements (which exist because L/F) is algebraic. Then $L = F(S)$ and every $m_{\alpha/F}$ splits over L since the extension is normal.

$\Longleftarrow$: Suppose L/F is a splitting field of a set of polynomials $S \subseteq F[x] \setminus \{0\}$, so L is generated over F by the set $\bigcup_{f \in S} R_f$, where $R_f \subseteq L$ is the set of roots f in L. Given $\alpha \in L$ and $g \in \mathrm{Irred}(F)$ such that $g(\alpha) = 0$, we see that α must be contained in a subfield generated by a finite set of such roots, so $\alpha \in F(R_f) \subseteq L$ where $f = f_1 \cdots f_k$ for some finite list $f_1, \ldots, f_k \in S$. Since $F(R_f)/F$ is a splitting field of f, it is normal so g splits over $F(R_f)$ and hence over L.

□

We also have the following, which will be important for us.

Proposition. *Consider fields $F \subseteq K \subseteq L$. If L/F is normal then L/K is normal.*

Proof. First note that since L/F is normal then it is algebraic by definition, so L/K and K/F are also algebraic.

Consider $f \in \mathrm{Irred}(K)$ with a root $\alpha \in L$. Since K/F is algebraic there is a minimal polynomial $g = m_{\alpha/F} \in F[x]$ over F. Since g has α as a root, over K we must have $f \mid g$. Since L/F is normal we have that g splits over Σ, and therefore its factor f splits over Σ. □

Remark (Warning). It is *not* true that L/F normal implies K/F normal. For instance, $F = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\alpha, \omega)$, with $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$.

Remark (Warning). It is *not* true that L/K and K/F normal imply L/F normal. For instance, $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, and $L = \mathbb{Q}(\sqrt[4]{2})$. Both L/K and K/F are degree 2 and so normal, but L/F is not normal since the minimal polynomial $x^4 - 2$ of $\sqrt[4]{2}$ does not split over $L \subseteq \mathbb{R}$.

21. Existence of algebraic closure

M 14 Nov

Every field F is contained in an algebraically closed field, and thus admits an algebraic closure. The general proof is somewhat non-constructive, ultimately relying on the axiom of choice.

Lemma. *Given any field F, there exists a field extension $F \subseteq K$ such that every non-constant $f \in F[x]$ has a root in K.*

Proof. To do this, we need the notion of a polynomial ring on an infinite set of variables:

$$R = F[x_s \mid s \in S].$$

Any element in here is just a polynomial involving a finite subset of the variables x_s. (That is, R is set theoretically a union of polynomial rings in finitely many variables.)

Let $S = \mathrm{Irred}(F)$, the set of monic irreducible polynomials. The goal is to produce K/F so that K has a root for every $f \in S$. Form $R := F[x_f \mid f \in S]$ as above. Let $I = (f(x_f) \mid f \in S)$, the ideal generated by elements $f(x_f) \in R$, where we plug in the variable x_f into the polynomial it corresponds to.

I claim $I \neq R$. Given that I is a proper ideal, we then know that there exists a maximal ideal M so that $I \subseteq M \subsetneq R$. Let $K = R/M$, which is a field, and comes with injective homomorphism $F \to K$, which we use to identify F as a subfield of K. This field K is thus constructed to have the property that every irreducible polynomial over F has at least one root in K, as desired.

To show that $I \neq R$, suppose not and derive a contradiction. Then there exist $f_1, \ldots, f_n \in S$ and $g_1, \ldots, g_n \in R$ such that

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}).$$

Note that there are only finitely variables which appear here ($x_{f_1}, \ldots, x_{f_n}$, together with the variables which appear in the $g_1, \ldots, g_n$). So this is really an identity in a polynomial ring on finitely many variables, which I'll write as $x_{f_1}, \ldots, x_{f_n}, x_{f_{n+1}}, \ldots, x_{f_m}$.

Construct an extension E/F which contains a root α_k of f_k for all $k = 1, \ldots, n$. Plugging in $x_{f_k} = \alpha_k$ when $k = 1, \ldots, n$, and $x_{f_k} = 0$ for the remaining variables into the above identity, gives $1 = 0$ in E, which is impossible. This is our contradiction. □

Theorem. *Every field F admits an algebraic closure.*

Proof. Given F, form

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_j \subseteq \cdots, \qquad j \in \mathbb{Z}_{>0},$$

where each K_j is chosen as in the lemma, so that every non-constant polynomial in $K_{j-1}[x]$ has a root in K_j. Let $K = \bigcup K_j$. This set has the structure of a field, compatible with the structures

on the K_js. Any polynomial $h(x) \in K[x]$ must actually lie in some $K_j[x]$ and so has a root in $K_{j+1} \subseteq K$. Thus K is algebraically closed, and so contains an algebraic closure $\overline{F}$ of F. □

22. Uniqueness of algebraic closure

Algebraic closures are also unique, up to isomorphism.

Proposition. *If K/F and L/F are algebraic closures of F, then K and L are isomorphic as F-extensions.*

Proof. We will construct an F-embedding $\phi\colon K \to L$, which gives an isomorphism $K \xrightarrow{\sim} \phi(K) \subseteq L$. The image $\phi(K)$, being isomorphic to K, is also an algebraic closure of F, and so is algebraically closed. But since L/F is algebraic then certainly $L/\phi(K)$ is algebraic, and therefore $L = \phi(K)$.

The map ϕ is constructed as for maps out of a splitting field, except we need to use Zorn's lemma. Let

$$\mathcal{P} = \left\{ (E, \psi) \;\middle|\; \begin{array}{c} F \subseteq E \subseteq K \text{ and,} \\ \phi\colon E \to L \text{ such that } \phi|F = \mathrm{id}_F. \end{array} \right\}.$$

This can given a partial ordering, so that $(E, \psi) \leq (E', \psi')$ iff $E \subseteq E'$ and $\psi'|E = \psi$. It is straightforward that Zorn's lemma applies to give a maximal element (E_0, ψ_0). If $E_0 = K$ we can set $\phi = \psi_0$ and we are done, so suppose not and derive a contradiction.

Choose $\alpha \in K \smallsetminus \widehat{E}$. Since α is algebraic over F, the extension $\widehat{E}(\alpha)/\widehat{E}$ is finite. Let $f = m_{\alpha/\widehat{E}}$ be the minimal polynomial. Then $f' = \psi_0(f) \in L[x]$ has a root β, so we can extend ψ_0 to an embedding $\psi_1\colon \widehat{E}(\alpha) \to L$. This gives $(\widehat{E}(\alpha), \psi_1) \in \mathcal{P}$ contradicting maximality of $(\widehat{E}, \psi)$, so we have our contradiction. □

Note: the isomorphism this produces is *not unique*.

23. The Frobenius endomorphism

Let F be a field of characteristic $p \neq 0$. Then for any $a, b \in F$ we have that

$$(a + b)^p = a^p + b^p,$$

because $p \mid \binom{p}{k} = \frac{p!}{(p-k)!\,k!}$ when $0 < k < p$.

Proposition. *If F is a field of characteristic $p \neq 0$, then the function $\phi\colon F \to F$ defined by $\phi(a) := a^p$ is a homomorphism of fields.*

This map $\phi\colon F \to F$ is called the **Frobenius endomorphism** of F.

Frobenius endomorphism

Example. In $F = \mathbb{F}_p$, we have that $a^p = a$ for every $a \in \mathbb{F}_p$.

Example. Let $K = \mathbb{F}_2[x]/(x^2 + x + 1)$. This is a field because $f = x^2 + x + 1$ clearly has no root in $\mathbb{F}_2 = \{0, 1\}$. Write $\gamma = \overline{x}$, so $K = \{0, 1, \gamma, \gamma + 1\}$ (a field of order 4) and $\gamma^2 = \gamma + 1$.

Then the Frobenius ϕ sends $\phi(\gamma) = \gamma^2 = \gamma + 1$. In fact, $\mathrm{Aut}(K) = \{e, \phi\}$, since $\{\gamma, \gamma + 1\}$ are the two roots of f.

Remark. If $f \in \mathbb{F}_p[x]$, and $K/\mathbb{F}_p$ is some extension field, then the Frobenius automorphism preserves roots of f. That is, if $\alpha \in K$ is a root of f, so is α^p.

In particular, α and α^p have the same minimal polynomial over $\mathbb{F}_p$.

Example. Let $K = \mathbb{F}_2/(x^3 + x + 1)$ with $\gamma = \overline{x}$, a field because $f = x^3 + x + 1$ has no root in $\mathbb{F}_2 = \{0, 1\}$. Write $\gamma = \overline{x}$, and note that K has exactly 8 elements. Then $\mathrm{Aut}(K) = \{e, \phi, \phi^2\}$, since $\{\gamma,\ \gamma^2,\ \gamma^4 = \gamma^2 + \gamma\}$ are the roots of f.

The other three elements of $K \smallsetminus \mathbb{F}_2$ are $\{\gamma^3 = \gamma + 1,\ \gamma^6 = \gamma^2 + 1,\ \gamma^{12} = \gamma^5 = \gamma^2 + \gamma + 1\}$, which are roots of $g = x^3 + x^2 + 1$, also irreducible over $\mathbb{F}_2$.

24. Perfect fields

A field F is called **perfect** if either: **perfect**

(1) it is characteristic 0, or
(2) it is characteristic $p \neq 0$, and every element of F is a pth power (i.e., the Frobenius endomorphism $a \mapsto a^p$ is an automorphism).

Thus, finite fields are perfect, since any injective map $K \to K$ from a finite set to itself must be a bijection.

Example (A non-perfect field). Let $K = F(t)$, the field of rational functions over any field F of characteristic p, e.g., $F = \mathbb{F}_p$. Then the Frobenius $\phi\colon K \to K$ is not surjective: the element t is not in the image of ϕ.

To see this, note that if $t = (g/h)^p$ for some $g, h \in F[t]$, then $g^p = t\,h^p$, and thus $p \deg g = 1 + p \deg h$, which has no solution with g, h non-zero.

Lemma. *Suppose* $\operatorname{char} F = p \neq 0$. *For any* $a \in F$, *consider* $f = x^p - a \in F[x]$. *The polynomial* f *is not separable. Furthermore, either*

(1) $f \in \operatorname{Irred}(F)$, *or*
(2) $f = (x-b)^p$ *for* $b \in F$ *with* $a = b^p$.

Proof. To see that f not separable, simply note that $Df = px^{p-1} = 0$, which is certainly not relatively prime to f.

We have that F splits over an extension field $F(b)$ as $f = (x-b)^p$, where $b^p = a$, since if b is any root of f we can compute $(x-b)^p = x^p - b^p = f$. For any $0 < k < p$ we have

$$(x-b)^k = x^k - kb\,x^{k-1} + \cdots + (-b)^k.$$

In particular $(x-b)^k \in F[x]$ implies $kb \in F$, and thus $b \in F$ since the integer k represents a non-zero element of the prime field $\mathbb{F}_p$. Thus f is reducible over F iff $b \in F$. □

In other words, in characteristic p, for any $a \in F$ we have either $a^{1/p} \in F$ or $[F(a^{1/p}) : F] = p$.

Proposition. *A field* F *is perfect iff every* $f \in \operatorname{Irred}(F)$ *is separable.*

Proof. When $\operatorname{char} F = 0$ there is nothing to prove, so suppose $\operatorname{char} F = p \neq 0$.

Suppose F is perfect. Then any $f \in F[x]$ such that $Df = 0$ itself a pth power of a polynomial in $F[x]$. To see this, note that $Df = 0$ implies $f = \sum_{k=0}^{n} a_k x^{kp}$, so since F is perfect we can choose $b_k \in F$ so that $b_k^p = a_k$, so

$$f = \sum_{k=0}^{n} a_k x^{kp} = \sum_{k=0}^{n} b_k^p x^{kp} = \left(\sum_{k=0}^{n} b_k x^k\right)^p = g^p, \qquad g = \sum_{k=0}^{n} b_k x^k \in F[x].$$

Thus if $f \in \operatorname{Irred}(F)$, we must have $Df \neq 0$, so $(f, Df) = F[x]$, so f is separable.

Conversely, if every irreducible over F is separable, then $f = x^p - a \in F[x]$ is never irreducible for any $a \in F$ (since $Df = 0$), so a has a pth root in F. □

The Frobenius $\phi\colon F \to F$ is always injective. Thus, when $\operatorname{char} F = p \neq 0$, elements $a \in F$ can have *at most* one pth root in F, or even in any extension of F. That is, $a^p = b^p$ implies $a = b$ in such fields.

In particular, there are *no* primitive nth roots of unity in F whenever $p \mid n$.

25. Finite fields

Clearly a field of characteristic 0 is infinite, since it contains $\mathbb{Q}$. Thus any finite field has $\operatorname{char} = p \neq 0$.

If K is finite of characteristic p, then $[K : \mathbb{F}_p] = n < \infty$, whence $|K| = p^n$, since it as a vector space over $\mathbb{F}_p$ it is isomorphic to $\mathbb{F}_p^n$. This means that $|K|$ determines $\operatorname{char} K$.

Let $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Since $Df = -1 \neq 0$ is a unit in $\mathbb{F}_p[x]$, this is separable.

Form a splitting field $K = \Sigma_{f/\mathbb{F}_p}$. Let

$$R := \{\, \alpha \in K \mid f(\alpha) = 0 \,\} = \{\, \alpha \in K \mid \alpha^{p^n} = \alpha \,\} \subseteq K,$$

the set of roots of f in K. Since f is separable, $|R| = p^n$. Since $f = x(x^{p^n-1} - 1) = 0$, the elements of R are either 0 or $(p^n - 1)$st roots of unity.

In fact, R is a subfield of K: it is closed under all field operations, since $(\alpha + \beta)^{p^n} = \alpha^{p^n}\beta^{p^n}$, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n}$, etc. Obviously f already splits over R, so $R = K$.

We have thus obtained a field of order p^n, as a splitting field of $f = x^{p^n} - x$ over $\mathbb{F}_p$, whose elements are exactly the roots of f. This field is usually denoted $\mathbb{F}_{p^n}$ (by pure mathematicians, especially number theorists), or sometimes as $GF(p^n)$ (for "Galois field", especially by people using finite fields in applications such as cryptography).

Proposition. *If K is a field with $|K| = p^n$, then $K \approx \mathbb{F}_{p^n}$.*

Proof. Clearly $\operatorname{char} K = p$. We have shown that $K^\times = K \smallsetminus \{0\}$, being finite, is cyclic of order $p^n - 1$. Thus every element of K is a root of $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Since these are distinct, f splits over K, which is therefore a splitting for f. The claim follows by uniqueness of splitting fields up to isomorphism. □

Proposition. *The automorphism group $\operatorname{Aut}(\mathbb{F}_{p^n}) = \langle \phi \rangle \approx C_n$, a cyclic group of order n generated by Frobenius.*

Proof. Clearly $\phi \in G = \operatorname{Aut}(\mathbb{F}_{p^n})$, and $\phi^n = \mathrm{id}$. There is no smaller $k > 0$ such that $\phi^k = \mathrm{id}$, since in that case every $a \in \mathbb{F}_{p^n}$ would satisfy $a^{p^k} = a$, and we know there are only p^k such elements. Thus $|\phi| = n$, and $|G| \geq n$.

Since $\mathbb{F}_{p^n}^\times$ is cyclic, there exists $\zeta \in \mathbb{F}_{p^n}^\times$ with $|\zeta| = p^n - 1$. Clearly $\mathbb{F}_{p^n} = \mathbb{F}_p(\zeta)$. As this is a simple extension, any automorphism $\alpha \in G$ is determined once we know $\alpha(\zeta)$. But since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, we have $\deg m_{\zeta/\mathbb{F}_p} = n$, so there are at most n possibilities for $\alpha(\zeta)$. Thus $|G| \leq n$.

□

26. Separable extensions

W 16 Nov

Given an extension K/F, say that $\alpha \in K$ is **separable** over F it is algebraic over F, and if its minimal polynomial $m = m_{\alpha/F}$ is a separable polynomial (i.e., $Dm \neq 0$ when characteristic is non-zero.). **separable**

Therefore, α is separable over F if it is the root of *any* separable polynomial $f \in F[x]$, since $m_{\alpha/F} \mid f$, and any factor of a separable polynomial must also be separable.

We say that K/F is a **separable extension** if all elements of K are separable over F. **separable extension**

Example. Every algebraic extension K/F of fields of characteristic 0 is separable.

Example. Let F be a perfect field. We have shown this means exacly that every $f \in \operatorname{Irred}(F)$ is separable. Then any algebraic extension K/F of a perfect field is separable.

Example. The standard example of an inseparable extension is L/K, where F is any field of characteristic p, $L = F(t)$ is a function field over F, and $K = F(t^p)$. The element t generates L over K, but is not contained in K, since $t = g(t^p)/h(t^p)$ for some $g, h \in \mathbb{F}_p[x]$ is impossible for degree reasons.

Furthermore, t is algebraic over K but not separable, since its minimal polynomial $m_{t/K} = x^p - t^p$ is not separable.

Proposition. *If $F \subseteq K \subseteq L$ such that L/F is separable, then L/K and K/F are separable.*

Proof. By hypothesis, every $\alpha \in L$ is a root of a separable polynomial $f \in F[x]$. It is an immediate consequence that every $\alpha \in K$ is separable over F, so K/F is separable. Furthermore, since f remains separable over the larger field K, we have that α is separable over K, so L/K separable. □

We have the following criterion for separability of an element.

Lemma. *Let K/F be an extension in characteristic $p \neq 0$. Then $\alpha \in K$ is separable over F iff $\alpha \in F(\alpha^p)$.*

Proof. Note that if α is transcendental over F (and so not separable over F), then $F(\alpha)$ is isomorphic to a function field $F(x)$ on one variable x. It is clear in this case that $x \notin F(x^p)$, since $x = g(x^p)/h(x^p)$ for polynomials $g, h \in F[x]$ is impossible for degree reasons. So we can reduce to the case of α algebraic over F.

So assume that α is algebraic over F, so we have algebraic extensions

$$F \subseteq F(\alpha^p) \subseteq F(\alpha).$$

Let $g = m_{\alpha/F} \in \operatorname{Irred}(F)$, so $k = \deg g = [F(\alpha) : F]$. I will show that $\alpha \notin F(\alpha^p)$ iff g is not separable.

- Suppose g is not separable. Since it is irreducible over F, this means $Dg = 0$, so $g = h(x^p)$ for some $h \in F[x]$ with $\deg h = k/p$. But we know $h(\alpha^p) = 0$, so $[F(\alpha^p) : F] \leq \deg h = \frac{1}{p}[F(\alpha) : F] < [F(\alpha) : F]$, and thus $\alpha \notin F(\alpha^p)$.
- Suppose g is separable. Consider $f = x^p - \alpha^p \in F(\alpha^p)$, and recall that f *either* splits over $F(\alpha^p)$ or is irreducible over $F(\alpha^p)$. If it is irreducible over $F(\alpha^p)$ then $f = m_{\alpha/F(\alpha^p)}$, and therefore $f \mid g$, which would imply g has repeated roots, so this does not happen.

  So f must split over $F(\alpha^p)$, which means $\alpha \in F(\alpha^p)$.

□

Example (An example of an inseparable extension). Let F be any field with $\operatorname{char} F = p > 0$. Let $L = F(t)$ be the function field, and let $K = F(t^p) \subseteq L$. The element $t \in L$ is not separable over K by the lemma, since $t \notin K = K(t^p)$.

27. Separably generated extensions

Given a field F in characteristic $p > 0$, let

$$F^p := \{\, a^p \in F \mid a \in F \,\},$$

the subset of elements which are pth powers. This is exactly the image $\phi(F)$ of the Frobenius endomorphism $\phi\colon F \to F$, so F^p is a subfield of F, which is isomorphic to F (but possibly *not equal* to F).

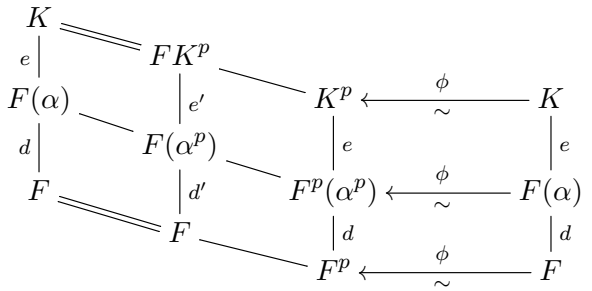
This operation is compatible with the formation of subfields generated by subsets: if $K = F(S)$ for some subset $S \subseteq K$, then $K^p = F^p(S^p)$, where $S^p = \{\, s^p \mid s \in S \,\}$. This implies that for any two subfields $F, F' \subseteq K$, we have $(FF')^p = F^p F'^p$.

Finally, note that $[K : F] = [K^p : F^p]$. This is because Frobenius gives an isomorphism $\phi\colon K \xrightarrow{\sim} K^p$ of fields which takes F to F^p.

Proposition. *Let K/F be a finite extension in characteristic $p \neq 0$. Then K/F is separable iff $K = FK^p$, i.e., iff K is generated over F by pth powers in K.*

Proof. $\Longrightarrow$. Suppose K/F is separable. Then for any $\alpha \in K$ we have $\alpha \in F(\alpha^p) \subseteq FK^p$. Therefore $K \subseteq FK^p$ whence $K = FK^p$.

$\Longleftarrow$. Suppose $K = FK^p$. Let $\alpha \in K$, and consider the diagram of extensions



The Frobenius maps gives isomorphisms which tell us that $[K^p : F^p(\alpha^p)] = [K : F(\alpha)]$ and $[F^p(\alpha^p) : F^p] = [F(\alpha) : F]$. Note that $FK^p = F(\alpha^p)K^p$, so $e' \leq e$. But according to the tower law, $e \mid e'$, whence $e = e'$ and so $F(\alpha) = F(\alpha^p)$, whence α is separable over F. □

Remark. This criterion doesn't work if the extension is infinite. For instance, starting with the function field $K = F(t)$, we can form an infinite chain of non-separable extensions

$$K = F(t) \subsetneq K_1 = F(t^{1/p}) \subsetneq K_2 = F(t^{1/p^2}) \subsetneq \dots.$$

Then $L = \bigcup_n K_n$ is such that $L = KL^p$, since $KK_n^p = K_{n-1}$, but L/K is certainly not a separable extension.

Corollary. *We have the following.*

1. *If $F \subseteq K \subseteq L$ are finite extensions such that K/F and L/K are separable, then L/F is separable.*
2. *If $F \subseteq L$ is a field extension, and $K, K' \subseteq L$ such that K/F and K'/F are finite separable extensions, then KK'/F is separable.*
3. *If $L = F(\alpha_1, \dots, \alpha_n)$ such that each α_k is separable over F, then L/F is separable.*
4. *Given an extension K/F, let $K^{\text{sep}} \subseteq K$ be the subset of elements which are separable over F. Then K^{sep} is a subfield of K.*
5. *Every splitting field Σ/F of a separable polynomial $f \in F[x]$ is a separable extension.*

Proof. These are all trivial if we are in characteristic 0, so assume characteristic is $p > 0$.

For (1), we have $L = KL^p = FK^pL^p = FL^p$, since $K^p \subseteq L^p$.

For (2), we have $(KK')^p = K^pK'^p$, whence $F(KK')^p = FK^pK'^p = (FK^p)(FK'^p) = KK'$.

Statement (3) follows by inductively applying (2) with $K = F(\alpha_1, \dots, \alpha_{j-1})$ and $K' = F(\alpha_j)$, since $FK'^p = F(F^p(\alpha_j^p)) = F(\alpha_j^p)$, which equals $F(\alpha_j)$ when α_j is separable over F.

Statement (4) and (5) follow immediately from (3).

□

28. Roots of unity over $\mathbb{Q}$

We want to understand the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. To do this we need to understand the minimal polynomials of nth roots of unity.

An nth root of unity ϵ in $\mathbb{C}$ is a root of $x^n - 1$. This is a monic polynomial in $\mathbb{Z}[x]$, and so in particular is a *primitive* polynomial, i.e., its coefficients are a relatively prime set. By Gauss's Lemma, there is an irreducible factorization of $x^n - 1$ over $\mathbb{Q}$ into primitive polynomials over $\mathbb{Z}$, which must be monic (up to a sign). This implies that the minimal polynomial $f_\epsilon := m_{\epsilon/\mathbb{Q}}$, which is a factor of $x^n - 1$, is an element of $\mathbb{Z}[x]$.

Theorem. *Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. Then every primitive nth root of unity is a root of $f = m_{\zeta/\mathbb{Q}}$.*

The proof will use the following lemma.

Lemma. *Let $\epsilon \in \mathbb{C}$ be a primitive nth root of unity, and let p be a prime not dividing n. Then for any $f \in \mathrm{Irred}(\mathbb{Q})$ which has ϵ as a root, we have $f(\epsilon^p) = 0$.*

Proof of Theorem using Lemma. Every primitive nth root of unity can be written as ζ^k with $\gcd(k, n) = 1$ and $k > 0$. Factor $k = p_1 \cdots p_r$ into primes, where no p_i divides n. Then using the lemma and induction we show successively that $\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \zeta^{p_1 p_2 p_3}, \ldots$ are all roots of f, whence $f(\zeta^k) = 0$. □

Now we prove the lemma. The idea of the proof is this: since $f \in \mathbb{Z}[x]$, we can reduce mod p it to $\overline{f} \in \mathbb{F}_p[x]$. This $\overline{f}$ will have the same degree as f (since f is monic). In a splitting field over $\mathbb{F}_p$, its roots will still be some nth roots of unity, since $\overline{f} \mid x^n - 1$. It will also be separable over $\mathbb{F}_p$ (since $x^n - 1$ is, since $p \nmid n$).

However $\overline{f}$ may not be irreducible any more. But if it has irreducible factorization $\overline{f} = g_1 \cdots g_k$ over $\mathbb{F}_p$, then we know for any root $\overline{\epsilon}$ of g_k, we have that $\overline{\epsilon}^p$ is also a root of g_k. Thus in characteristic p, the set of roots of $\overline{f}$ must be "closed under pth powers". We can hope that this property "lifts" to f itself.

Proof of Lemma. We can assume $f = m_{\epsilon/\mathbb{Q}}$. Let $g = m_{\epsilon^p/\mathbb{Q}}$. As noted above these are both factors of $x^n - 1$, and so are both in $\mathbb{Z}[x]$ since $x^n - 1$ is primitive and f, g are monic. We want to show $f = g$, so we assume $f \neq g$ and derive a contradiction. If that is the case we must have $x^n - 1 = fgh$ for some $h \in \mathbb{Z}[x]$.

Let $G := g(x^p) \in \mathbb{Z}[x]$. Then $G(\epsilon) = g(\epsilon^p) = 0$, so $f \mid G$, so $G = fk$ for some monic $k \in \mathbb{Z}[x]$, since G is also monic polynomial with integer coefficients.

Now we can reduce everything modulo p, by taking images under the homomorphism $\pi\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ which sends integer coefficients to integers modulo p. Write $\overline{f}, \overline{g}, \overline{h}, \overline{k}, \overline{G}$ for the images of f, g, h, k, G under π. Note that since f, g are monic of positive degree, $\overline{f}, \overline{g}$ are also monic of positive degree (but they might not be irreducible over $\mathbb{F}_p$). Also since elements of $\mathbb{F}_p$ satisfy $a^p = a$, we have $\overline{g}(x^p) = \overline{g}(x)^p$. Thus

$$\overline{g}^p = \overline{G} = \overline{f}\,\overline{k}, \qquad x^n - 1 = \overline{f}\overline{g}\overline{h}.$$

The first identity implies that $\overline{f}, \overline{g}$ must have some irreducible factor $m \in \mathrm{Irred}(\mathbb{F}_p)$ in common, since neither is a unit, and any irreducible factor of $\overline{f}$ must also divide $\overline{g}$. Since $m \mid f$ and $m \mid g$, the second identity implies that $m^2 \mid x^n - 1$ in $\mathbb{F}_p[x]$. But $x^n - 1 \in \mathbb{F}_p[x]$ is separable, since $D(x^n - 1) = nx^{n-1}$ and $p \nmid n$, and these are relatively prime since $x \nmid x^n - 1$. So $x^n - 1$ cannot have a repeated irreducible factor, so we have a contradiction. □

29. Cyclotomic polynomials

We write $\Phi_n := f \in \mathbb{Z}[x]$ for the minimal polynomial of one primitive nth root of unity, and hence of all primitive nth roots of unity. Every nth root of unity is a primitive dth root of unity for some d dividing n, so since $x^n - 1$ is separable we must have **F 18 Nov**

$$x^n - 1 = \prod_{d \mid n} \Phi_d.$$

This means that we can compute the Φ_n by induction on n, using polynomial long division.

The degree of Φ_n is the Euler ϕ-function

$$\phi(n) := |(\mathbb{Z}/n)^\times| = \text{number of } d \in \{1, 2, \ldots, n\} \text{ such that } \gcd(d, n) = 1.$$

$$\Phi_1 = x - 1,$$
$$\Phi_2 = x + 1,$$
$$\Phi_3 = x^2 + x + 1,$$
$$\Phi_4 = x^2 + 1,$$
$$\Phi_5 = x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_6 = x^2 - x + 1,$$
$$\Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_8 = x^4 + 1,$$
$$\Phi_9 = x^6 + x^3 + 1,$$
$$\Phi_{10} = x^4 - x^3 + x^2 - x + 1,$$
$$\Phi_{11} = x^{10} + x^9 + \cdots + x^2 + x + 1,$$
$$\Phi_{12} = x^4 - x^2 + 1,$$
$$\Phi_{13} = x^{12} + x^{11} + \cdots + x^2 + x + 1,$$
$$\Phi_{14} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,$$
$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$
$$\Phi_{16} = x^8 + 1.$$

Exercise. Show that:

(1) if m is odd and $m > 1$, then $\Phi_{2m} = \Phi_m(-x)$, and
(2) if $p \mid m$ where p is prime, then $\Phi_{pm} = \Phi(x^p)$.

Use this to show that you can reduce the problem of computing cyclotomic polynomials to the case when n is a product of distinct odd primes.

Remark. It's not true that every coefficient in Φ_n must be in $\{-1, 0, 1\}$. The first counterexample is:

$$\begin{aligned}\Phi_{105} = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.\end{aligned}$$

In particular, we have that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n)$, the value of the **Euler ϕ-function**, defined by **Euler ϕ-function**

$$\phi(n) = |(\mathbb{Z}/n)^\times| = |\{\, k \in \{1, \ldots, n\} \mid \gcd(k, n) = 1 \,\}|.$$

30. Galois extensions

Given a field extension L/F, we say it is a **Galois extension** iff it is both normal and separable. **Galois extension**

In other words, L/F is Galois if for every $\alpha \in L$, there exists a separable polynomial $f \in F[x]$ which (i) has α as a root, and (ii) splits over L. (Note: if any f has these properties then so does the minimal polynomial $m_{\alpha/F}$.)

Note: this is different from what DF say in two ways. (1) In §14.1 they only define *finite* Galois extension (though they do the infinite case in §14.9). (2) Their definition is different than the above in the finite case, but I will show they are equivalent.

Proposition. *A finite extension L/F is Galois iff it is a splitting field of some separable polynomial $f \in F[x]$.*

Proof. We have shown that a splitting field of any f is normal, and that it is also separable if f is a separable polynomial.

Conversely, suppose L/F is finite and Galois. We can write $L = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_k \in F$. Let $m_k = m_{\alpha_k/F} \in F[x]$. Each m_k is a separable polynomial. Note that there could be repetition in the list $m_1, \ldots, m_n$. Let $f =$ the product of distinct elements from the list of minimal polynomials.

Since f is a product of pairwise distinct up-to-units separable irreducible polynomials, it is separable. Clearly all α_ks are roots of f, so L/F is a splitting field of f. □

Given extensions K/F and L/F over F, write $\mathrm{Emb}_F(K, L)$ for the set of homomorphisms $\phi\colon K \to L$ with $\phi|_F = \mathrm{id}_F$ ("embeddings" of extensions). We will prove the following theorem on embeddings.

Theorem (Theorem on Embeddings)**.** *Let K/F and L/F be extensions with K/F finite. Then*

$$|\mathrm{Emb}_F(K,L)| \le [K:F],$$

with equality iff

(1) *K/F is a separable extension, and*
(2) *every $f \in \mathrm{Irred}(F)$ which has a root in K splits over L.*

As a consequence, we will get the following (which is DFs definition of finite Galois extension).

Corollary. *If L/F is a finite extension, then it is Galois iff $|\mathrm{Aut}(L/F)| = [L:F]$.*

Proof. We apply the theorem in the case of $K = L$. Let $G = \mathrm{Aut}(L/F)$. Note that since $K = L$, we have $\mathrm{Emb}_F(L,L) = G$. Then the Corollary is an immediate consequence of the theorem: equality $|G| = [L:F]$ holds iff L/F is separable and normal. □

Remark. If F is a perfect field, then every finite extension L/F is separable. This applies when F is characteristic 0 or F is finite. Thus all finite normal extensions over perfect F are Galois.

31. Proof of the theorem on embeddings

I'm going to prove the theorem as a consequence of a slightly more general statement, which will allow for an inductive argument. Suppose given extensions K/F and L/F', and an isomorphism $\lambda\colon F \to F'$. We define

$$\mathrm{Emb}_\lambda(K,L) = \{\text{embeddings } \phi\colon K \to L \text{ such that } \phi|F = \lambda\}.$$

$$\begin{array}{ccc} K & \overset{\phi}{\dashrightarrow} & L \\ \uparrow & & \uparrow \\ F & \underset{\lambda}{\xrightarrow{\sim}} & F' \end{array}$$

If $F = F'$ and $\lambda = \mathrm{id}_F$, then this is just $\mathrm{Emb}_F(K,L)$.

Proposition. *Let K/F and L/F' be extensions, with K/F finite. Suppose that $\lambda\colon F \xrightarrow{\sim} F'$ is an isomorphism of fields. Then*

$$|\mathrm{Emb}_\lambda(K,L)| \le [K:F],$$

with equality iff

(1) *K/F is separable, and*
(2) *if $f \in \mathrm{Irred}(F)$ has a root in K, then $f' := \lambda(f) \in F'[x]$ splits over L.*

The theorem is exactly the special case of $F = F'$ and $\lambda = \mathrm{id}_F$.

The induction will be by handling one simple extension at a time, so lets do that.

Lemma. *Let K/F and L/F' be extensions and $\lambda\colon F \xrightarrow{\sim} F'$ an isomorphism. Then for any $\alpha \in K$ we have*

$$|\mathrm{Emb}_\lambda(F(\alpha),L)| \le [F(\alpha):F],$$

with equality iff

(i) *α is separable over F, and*
(ii) *$m' := \lambda(m_{\alpha/F}) \in F'[x]$ splits over L.*

Proof. We have a bijection of sets

$$\mathrm{Emb}_\lambda(F(\alpha),L) \longleftrightarrow \{\, \alpha' \in L \mid m'(\alpha') = 0 \,\}.$$

Since m' has at most $d := \deg m' = \deg m = [F(\alpha):F]$ roots, this gives the inequality.

Note that α is separable iff m is a separable polynomial, iff m' is a separable polynomial (since $\lambda\colon F[x] \xrightarrow{\sim} F'[x]$ is an isomorphism, it preserves separability). So (i) just says m' has no repeated roots in any extension field.

Thus, (i) and (ii) together are equivalent to the statement that m' has *exactly* d roots, or equivalently that there are exactly d embeddings $F(\alpha) \to L$ extending λ. □

Proof of Proposition. We work by induction on $n = [K : F]$.

When $n = 1$ so that $K = F$, then $\mathrm{Emb}_\lambda(K, L)$ has only one element, and (i) and (ii) hold trivially. So suppose $n \geq 2$.

Pick $\alpha \in K \smallsetminus F$, so that we get a chain of extensions $F \subsetneq F(\alpha) \subseteq K$. Write $d := [F(\alpha) : F]$ and $e := [K : F(\alpha)]$, and note that $e < ed = n$.

To give $\phi\colon K \to L$ extending λ amounts two choices:

(a) A choice of $\mu\colon F(\alpha) \to L$ extending λ. By the Lemma there are at most d such choices.
(b) Given μ, a choice of $\phi\colon K \to L$ extending μ. Since $e < n$, by induction there are at most e choices.

Thus

$$|\mathrm{Emb}_\lambda(K, L)| \leq \sum_{\mu \in \mathrm{Emb}_\lambda(F(\alpha), L)} |\mathrm{Emb}_\mu(K, L)| \leq de = n.$$

Now suppose (1) and (2) both hold: K/F is separable, and for every $f \in \mathrm{Irred}(F)$ with a root in K the image $f' = \lambda(f)$ splits over L.

- Statement (1) implies that α is separable over F, and that $m' = \lambda(m_{\alpha/F})$ splits over L. Thus by the Lemma we have that $d = |\mathrm{Emb}_\lambda(F(\alpha), L)|$.
- Statement (1) implies that $K/F(\alpha)$ is separable. Furthermore, if $f \in \mathrm{Irred}(F(\alpha))$ has a root $\beta \in K$, then $f' = \mu(f) \in F'[x]$ splits over L: this is because $f \mid m = m_{\beta/F}$, and the hypothesis (2) implies $m' = \lambda(m)$ splits over L, and hence so does its factor f'.

  Therefore since $e < n$, by induction we have that $e = |\mathrm{Emb}_\mu(K, L)|$.

Therefore, (1) and (2) imply equality.

Conversely, suppose we have equality $|\mathrm{Emb}_\lambda(K, L)| = n$. Consider *any* $\alpha \in K$, and as before let $d = [F(\alpha) : F]$ and $e = [K : F(\alpha)]$. By what we have already proved, we have

$$0 \leq |\mathrm{Emb}_\lambda(F(\alpha), L)| \leq d, \qquad 0 \leq |\mathrm{Emb}_\mu(K, L)| \leq e \text{ for any } \mu \in \mathrm{Emb}_\lambda(F(\alpha), L).$$

Thus

$$n = \sum_{\mu \in \mathrm{Emb}_\lambda(F(\alpha), L)} |\mathrm{Emb}_\mu(K, L)| \leq \sum_{\mu \in \mathrm{Emb}_\lambda(F(\alpha), L)} e \leq de = n.$$

This is only possible if $d = |\mathrm{Emb}_\lambda(F(\alpha), L)|$ and $e = |\mathrm{Emb}_\mu(K, L)|$.

In particular since $d = |\mathrm{Emb}_\lambda(F(\alpha), L)|$, the Lemma implies that (i) α separable over F, and (ii) $m' = \lambda(m_{\alpha/F})$ splits over L. Since this applies to any $\alpha \in L$, we see that (1) K/F is separable, and (2) if $f \in \mathrm{Irred}(F)$ has a root in K then $f' = \lambda(f)$ splits over L. □

32. The basic Galois correspondence

M 28 Nov

Recall that a a finite Galois extension L/F is one which is normal and separable. These are exactly the splitting fields of separable polynomials over F.

If L/F is a normal finite extension, then $|\mathrm{Aut}(L/F)| \leq [L : F]$, and equality holds iff L/F is also separable.

For a finite Galois extension we write

$$\mathrm{Gal}(L/F) := \mathrm{Aut}(L/F),$$

and call it the **Galois group**.

Galois group

We are going to be thinking about **intermediate fields** of this extension, i.e., $F \subseteq K \subseteq L$. Note

intermediate fields

that if L/F is finite Galois, then so is L/K. The extension K/F is finite and separable, but might fail to be normal.

Let $G = \mathrm{Gal}(L/F)$.

- If K is an intermediate field of L/F, then L/K is finite Galois, and $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ is a subgroup of G.
- If $H \leq G$ is a subgroup of G, then L^H is an intermediate field of L/F.

We will need the Emebbing Theorem, which tells us that $|\mathrm{Gal}(L/K)| = [L : K]$ whenever L/K is a finite Galois extension. We are also are going to need the following important but technical lemma, which we will prove later.

Lemma (Tech Lemma)**.** *Let $G \leq \mathrm{Aut}(L)$ be a finite subgroup of automorphisms of a field L. Then $|G| = [L : L^G]$.*

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

$$H \qquad \longmapsto \qquad L^H$$

and

$$\mathrm{Gal}(L/K) \qquad \longmapsfrom \qquad K$$

are inverse one-to-one correspondences

$$\{\textit{subgroups of } G\} \qquad \longleftrightarrow \qquad \{\textit{intermediate fields of } L/F\}.$$

Notice that both operations are *order reversing*, where the ordering is inclusion:

$$H \subseteq H' \qquad \Longrightarrow \qquad L^H \supseteq L^{H'},$$
$$K \subseteq K' \qquad \Longrightarrow \qquad \mathrm{Gal}(L/K) \supseteq \mathrm{Gal}(L/K').$$

That is, if $a \in L$ is such that $h(a) = a$ for all $h \in H$, then certainly that is true for all $h \in H' \subseteq H$; and if $g \in G = \mathrm{Gal}(L/F)$ is such that $g|K' = \mathrm{id}$, then certainly $g|K = \mathrm{id}$ since $K \subseteq K'$.

Proof of the basic Galois correspondence, using the Tech Lemma. I show that the two operations are inverse to each other: doing one and then the other (in either order) gets you back where you started.

Let $H \leq G$ be a subgroup, and consider

$$H \qquad \Longrightarrow \qquad L^H \qquad \Longrightarrow \qquad \mathrm{Gal}(L/L^H).$$

Observe that $H \leq \mathrm{Gal}(L/L^H)$ by definition of $L^H = \{\, a \in L \mid h(a) = a \ \ \forall h \in H \,\}$. We have

$$|\mathrm{Gal}(L/L^H)| \underset{\text{Emb Thm}}{=} [L : L^H] \underset{\text{Tech Lemma}}{=} |H|,$$

using that L/L^H is finite Galois. Therefore the two groups must be equal: $H = \mathrm{Aut}(L : L^H)$.

Let K be an intermediate field of $L : F$, and consider

$$K \qquad \Longrightarrow \qquad \mathrm{Gal}(L/K) \qquad \Longrightarrow \qquad L^{\mathrm{Gal}(L/K)}.$$

Observe that $K \subseteq L^{\mathrm{Gal}(L/K)}$ by definition of $\mathrm{Aut}(L/K) = \{\, g \in G \mid g|K = \mathrm{id} \,\}$. We have

$$[L : L^{\mathrm{Gal}(L/K)}] \underset{\text{Tech Lemma}}{=} |\mathrm{Gal}(L/K)| \underset{\text{Emb Thm}}{=} [L : K],$$

again using that L/K is finite Galois. Therefore the two intermediate fields must be equal using the tower law $[L : K] = [L : L^{\mathrm{Gal}(L/K)}][L^{\mathrm{Gal}(L/K)} : K]$, so: $K = L^{\mathrm{Gal}(L/K)}$. □

33. Lattice Galois correspondence

As an immediate consequence of the proof, we get a relation between degrees of extensions and order of subgroups.

Theorem (Degrees Galois correspondence)**.** *For any intermediate field K of L/F we have*

$$[L : K] = |\mathrm{Gal}(L/K)|, \qquad [K : F] = |G : \mathrm{Gal}(L/K)|.$$

For any subgroup $H \leq G$ we have

$$[L : L^H] = |H|, \qquad [L^H : F] = |G : H|.$$

Both the set of subgroups of G and the set of intermediate extensions of L/F are posets. The Galois correspondence gives a "duality" between "joins" and "meets" in these posets.

Theorem (Lattice Galois correspondence)**.** *For intermediate fields K_1, K_2 of L/F, corresponding to subgroups $H_1 = \mathrm{Gal}(L/K_1)$, $H_2 = \mathrm{Gal}(L/K_2)$ of G, the Galois correspondence sends*

$$K_1K_2 \mapsto \mathrm{Gal}(L/K_1K_2) = H_1 \cap H_2 \leq G, \qquad K_1 \cap K_2 \mapsto \mathrm{Gal}(L/K_1 \cap K_2) = \langle H_1 \cup H_2 \rangle \leq G.$$

Proof. The first claim is immediate. For the second claim, it is easier to prove that $L^{\langle H_1 \cup H_2 \rangle} = K_1 \cap K_2$, and use the Galois correspondence.

□

34. Normality in the Galois correspondence

There is an additional part of the correspondence as usually stated. Given an intermediate field K of a Galois extension L/F, we would like to know what $\mathrm{Aut}(K/F)$ is, and understand when K/F is a normal extension.

Recall that for $H \leq G$, its *normalizer* is

$$N_G(H) = \{\, g \in G \mid gHg^{-1} = H \,\} \leq G.$$

Theorem (Normality in the Galois correspondence)**.** *Let L/F be a finite Galois extension with $G = \mathrm{Gal}(L/F)$. Let $H, H' \leq G$ with $K = L^H$, $K' = L^{H'}$.*

(1) *For any $g \in G$, we have that*

$$K' = g(K) \qquad \Longleftrightarrow \qquad H' = gHg^{-1}.$$

(2) *There is an isomorphism of groups*

$$\mathrm{Aut}(K/F) \approx N_G(H)/H.$$

(3) *The extension K/F is normal iff H is a normal subgroup of G. If that is so, then*

$$\mathrm{Gal}(K/F) \approx G/H.$$

Proof. Proof of (1). First we show that $\mathrm{Gal}(L/g(K)) = gHg^{-1}$. In fact, for any $u \in G$, we have that $u \in \mathrm{Gal}(L/g(K))$ iff $ug(c) = g(c)$ for any $c \in K$, iff $(g^{-1}ug)(c) = c$ for all $c \in K$, iff $g^{-1}ug \in H$. Thus $\mathrm{Gal}(L/g(K)) = gHg^{-1}$. The claim follows by the basic Galois correspondence, which says $K' = g(K)$ iff $H' = gHg^{-1}$.

Proof of (2). By (1) we have that

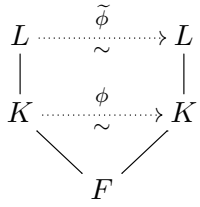
$$N_G(H) = \{\, g \in G \mid gHg^{-1} = H \,\} = \{\, g \in G \mid g(K) = K \,\}.$$

Thus there is a homomorphism of groups

$$\pi \colon N_G(H) \to \mathrm{Aut}(K/F), \qquad \pi(g) := g|K.$$

I claim that π is surjective. That is, I claim that any automorphism $\phi \colon K \to K$ such that $\phi|F = \mathrm{id}_F$ extends to an automorphism $\widetilde{\phi} \colon L \to L$, which necessarily is an element of $N_G(H)$ since $\widetilde{\phi}(K) = K$.

Since L/F is normal it is the splitting field of some polynomial $f \in F[x]$, and so L/K is also a splitting field of f. In our proof of the uniqueness of splitting fields, we showed that for any isomorphism $\phi\colon K \to K$ such that $\phi(f) = f$ splits over L, we can extend ϕ to $\widetilde{\phi}\colon L \to L$, which will also be an isomorphism since $\widetilde{\phi}(L)/F$ is also a splitting field of f.



Thus we have a surjective homomorphism $\pi\colon N_G(H) \twoheadrightarrow \mathrm{Aut}(K/F)$ with kernel

$$\mathrm{Ker}(\pi) = \{\, g \in G \mid g(K) = K,\ g|K = \mathrm{id}_K \,\} = H.$$

Thus this gives an isomorphism $N_G(H)/H \xrightarrow{\sim} \mathrm{Aut}(K/F)$.

Proof of (3). We know that the finite extension K/F is Galois iff $|\mathrm{Aut}(K/F)| = [K : F]$. Since K/F is separable, this implies it is normal iff equality holds in

$$\frac{|N_G(H)|}{|H|} = |N_G(H)/H| = |\mathrm{Aut}(K/F)| = |\mathrm{Emb}_F(K, K)| \leq [K : F] = \frac{[L : F]}{[L : K]} = \frac{|G|}{|H|},$$

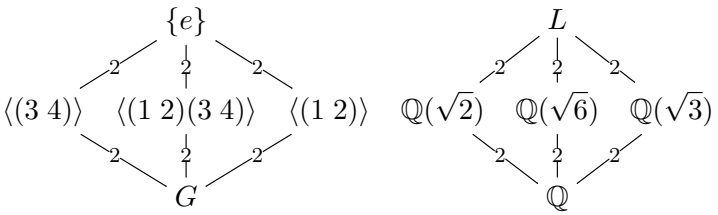
which is true iff $N_G(H) = H$, i.e., iff $H \trianglelefteq G$. □

The list of theorems above (Basic Galois correspondence, Degree Galois correspondence, Lattice Galois correspondence, and Normality in the Galois correspondence) taken together are "The Galois Correspondence".

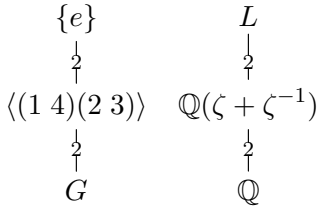
We have proved everything, except for the "Tech Lemma".

35. Example: Galois extensions of degree 4

Example. $f = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. List roots as $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$. Then $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $G \approx \langle (1\ 2), (3\ 4) \rangle \leq S_4$.



Example. $f = \Phi_5 \in \mathbb{Q}[x]$. List roots as $\alpha_1 = \zeta = e^{2\pi i/5}$, $\alpha_2 = \zeta^2$, $\alpha_3 = \zeta^3$, $\alpha_4 = \zeta^4$. Then $L = \mathbb{Q}(\zeta)$, $G \approx \langle (1\ 2\ 4\ 3) \rangle \leq S_4$.

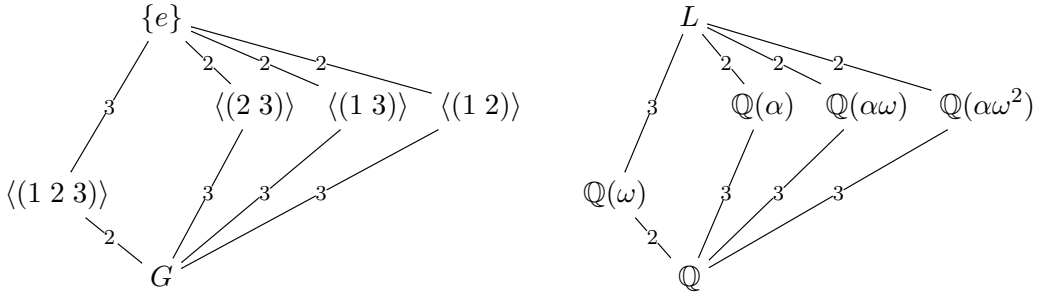


Note that $\zeta + \zeta^{-1} = 2\cos 2\pi/5$.

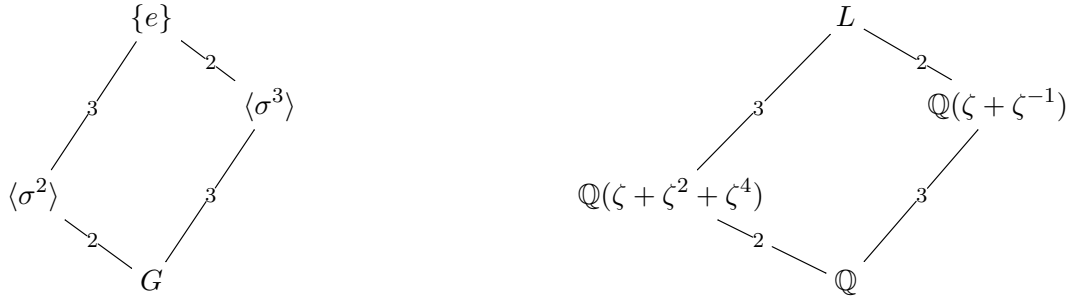
36. Example: Galois extensions of degree 6

W 30 Nov

Example. $f = x^3 - 2 \in \mathbb{Q}[x]$, $F = \mathbb{Q}$, $L = \Sigma_{f/\mathbb{Q}} = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$, with $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. I'll list the roots as $\alpha_1 = \alpha$, $\alpha_2 = \alpha\omega$, $\alpha_3 = \alpha\omega^2$. Then $G = \mathrm{Gal}(L/\mathbb{Q}) \approx S_3$. The following diagram shows subgroups and corresponding subfields.



Example. $f = \Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$, $F = \mathbb{Q}$, $L = \Sigma_{f/\mathbb{Q}} = \mathbb{Q}(\zeta)$, with $\zeta = e^{2\pi i/7}$. I'll list the roots as $\alpha_k = \zeta^k$, $k = 1, \ldots, 6$. Then $G = \mathrm{Gal}(L/Q) \approx C_6$. We can take as a generator the element $\sigma \in G$ which sends $\sigma(\zeta^k) = \zeta^{3k}$, since this has order 6. It corresponds to the permutation (1 3 2 6 4 5) of roots. The following diagram shows subgroups and corresponding subfields.



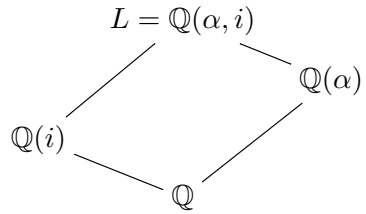
All of the subextensions K/F are normal. Note that σ^3 coincides with complex conjugation, so $L^{\langle\sigma^3\rangle} = L \cap \mathbb{R}$. We have $\beta := \zeta + \zeta^{-1} = 2\cos 2\pi/7$. You can show directly that this has a minimal polynomial of degree 3, namely $x^3 + x^2 - 2x - 1$. The element $\gamma := \zeta + \zeta^2 + \zeta^4$ has minimal polynomial $x^2 + x + 2 = 0$, and that in fact $\gamma = (-1 + i\sqrt{7})/2$.

37. Example: Galois extension of degree 8

Example. $f = x^4 - 2 \in \mathbb{Q}[x]$, $F = \mathbb{Q}$, $L = \Sigma_{f/\mathbb{Q}}$, $G = \mathrm{Gal}(L/\mathbb{Q}) \leq S_4$. The polynomial has roots

$$\alpha_1 = \alpha = \sqrt[4]{2}, \quad \alpha_2 = i\alpha, \quad \alpha_3 = i^2\alpha = -\alpha, \quad \alpha_4 = i^3\alpha = -i\alpha.$$

Consider the following partial diagram of subfields.

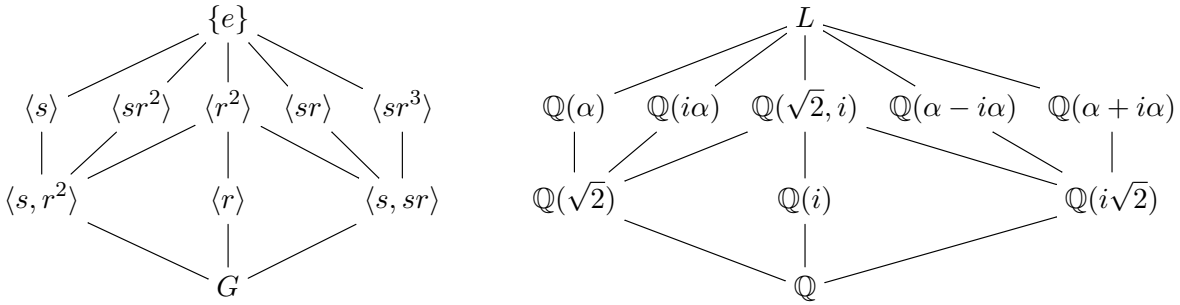


Claim: f is irreducible (e.g., by Eisenstein). Also, $m_{i/\mathbb{Q}} = x^2 + 1$. Therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Also, $i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, so $[L : \mathbb{Q}(\alpha)] \geq 2$. Since $[L : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(i) : \mathbb{Q}] = 2$, we conclude that $[L : \mathbb{Q}(\alpha)] = 2$ and thus $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$, and so $|G| = 8$.

I claim that $G = D_4$. To see this, note that the relations $\alpha_1 = -\alpha_3$ and $\alpha_2 = -\alpha_4$ limit how elements of G can permute the roots, so that only 8 elements of S_4 are possibilities. These include $r = (1\ 2\ 3\ 4)$ and $s = (2\ 4)$.

Here is the full diagram of subgroups and subfields.



Aside from $\{e\}$, the normal subgroups of G are exactly those which contain r^2. Thus, the proper intermediate fields K such that $K/\mathbb{Q}$ is normal are precisely the subfields of $\mathbb{Q}(\sqrt{2}, i)$. The other four extensions $K/\mathbb{Q}$ of degree 4 are not normal over $\mathbb{Q}$. Instead, there are isomorphisms of fields $\mathbb{Q}(\alpha) \approx \mathbb{Q}(i\alpha)$ and $\mathbb{Q}(\alpha - i\alpha) \approx \mathbb{Q}(\alpha + i\alpha)$, because $\langle s \rangle$ and $\langle sr^2 \rangle$ are conjugate subgroups, and likewise $\langle sr \rangle$ and $\langle sr^3 \rangle$.

38. Proof of the lemma on degree of a fixed field

Here is the proof of the "Technical Lemma", that $|L : F| = |G|$ if $F = L^G$ for a finite group of automorphisms G.

Proof that $[L : F] \geq |G|$. Either $[L : F]$ is infinite in which case the conclusion is immediate, or $[L : F] < \infty$. In that case, we have $G = \mathrm{Emb}_F(L, L)$, and we know that

$$|G| = |\mathrm{Emb}_F(L, L)| \leq [L : F],$$

using the upper bound on the number of embeddings from the embedding theorem. □

For the rest, we are going to need a bit of linear algebra.

Lemma (Linear algebra lemma)**.** *A system of m homegeneous linear equations in n variables always has a non-trivial solution if $n > m$.*

Equivalently, if a system of m homogeneous linear equations in n variables has only one solution, then $n \leq m$.

Proof. This is a theorem of linear algebra. The space of solutions is the nullspace of the $m \times n$ matrix $A = (a_{ij})$, consisting of column vectors in $x \in K^n$ such that $Ax = 0$. The dimension over K of the null space is

$$\text{nullity } A = (\text{number of columns of } A) - (\text{rank of } A) = n - \operatorname{rank} A.$$

If the only solutions are trivial, then nullity $A = 0$ whence $n = \operatorname{rank} A$. But in general $\operatorname{rank} A = \min(m, n)$, so we must have $n \leq m$ as desired. □

Proof that $[L : F] = |G|$. We know that $|G| \leq [L : F]$. Let $m = |G|$, and write $\phi_1, \ldots, \phi_m$ for the distinct elements of G. We suppose there exists a set $v_1, \ldots, v_n$ of F-linearly independent elements of L, with $n = m + 1$, and derive a contradiction. This will show that $\dim_F L \leq n$, and thus completes the proof.

Consider the homogeneous linear system over L of the form

$$\phi_i(v_1)x_1 + \cdots + \phi_i(v_n)x_n = 0, \qquad i = 1, \ldots, m.$$

with m equations and $n = m+1$ variables. This is the matrix equation $Ax = 0$, where $A = (\phi_i(v_j)) \in M_{m\times n}(L)$.

Since $n > m$ there are more variables than equations, so there exists $x = (x_1, \dots, x_n) \in L^n$ with $x \neq 0$ and $Ax = 0$. Choose such a non-trivial solutions with the fewest number of non-zero entries, and relabel the $v_j$ss (and thus the x_js) so that $x_1, \dots, x_r \in L^\times$ and $x_{r+1} = \cdots = x_n = 0$. Thus we have

$$\phi_i(v_1)x_1 + \cdots + \phi_i(v_r)x_r = 0, \qquad x_1, \dots, x_m \in L^\times, \qquad i = 1, \dots, m, \quad r \geq 1.$$

Now let $\psi \in G$ be any element. Applying it to the above equation gives

$$(\psi\phi_i)(v_1)\,\psi(x_1) + \cdots + (\psi\phi_i)(v_r)\,\psi(x_r) = 0, \qquad i = 1, \dots, m.$$

The list $\psi\phi_1, \dots, \psi\phi_m$ just runs through all elements of G in a different order. So we can write this system as

$$\phi_i(v_1)\,\psi(x_1) + \cdots + \phi_i(v_r)\,\psi(x_r) = 0, \qquad i = 1, \dots, m,$$

For each $i = 1, \dots, m$, we form (original equation) $\psi(x_r)$ − (new equation) x_r, and get

$$\phi_i(v_1)\big(x_1\psi(x_r) - \psi(x_1)x_r\big) + \cdots + \phi_i(v_r)\big(x_r\psi(x_r) - \psi(x_r)x_r\big) = 0, \qquad i = 1, \dots, m.$$

The last term drops out, so we really have

$$\phi_i(v_1)y_1 + \cdots + \phi_i(v_{r-1})y_{r-1} = 0, \qquad i = 1, \dots, m,$$

where $y_j = x_j\psi(x_r) - \psi(x_j)x_r$. By minimality of the solution of $Ax = 0$, we must have $y_1 = \cdots = y_{r-1} = 0$, and thus

$$x_j/x_r = \psi(x_j/x_r), \qquad \forall\, \psi \in G, \qquad j = 1, \dots, r-1.$$

Thus $x_j/x_r \in L^G = F$, i.e., $x_j = c_j x_r$ for $c_1, \dots, c_r \in F^\times$, with $c_r = 1$.

Now take the original equations $\sum_j \phi_i(v_j)x_j = 0$ and divide through by x_r to get

$$\phi_i(v_1)c_1 + \cdots + \phi_i(v_r)c_r = 0, \qquad c_1, \dots, c_r \in F^\times, \qquad i = 1, \dots, m, \qquad r \geq 1.$$

In particular, when $\phi_i = \mathrm{id}$, we get $c_1v_1 + \cdots + c_rv_r = 0$ with $c_1, \dots, c_r \in F^\times$, contradicting linear independence of the v_js.

□

39. Minimal polynomials and the Galois correspondence

F 2 Dec

Any finite extension K/F is contained in a finite normal extension L/F. For instance, take $L = \Sigma_{f/K}$, where $f = m_{\alpha_1/F}\cdots m_{\alpha_n/F} \in F[x]$ with $K = F(\alpha_1, \dots, \alpha_n)$. The extension L/F constructed this way is called the **normal closure** of K/F: it is the "smallest" normal extension of K with the property that if $g \in \mathrm{Irred}(F)$ such that g has a root in K, then g splits over L.

normal closure

If the original extension K/F is also separable, then the normal closure is a Galois extension.

Suppose we have finite Galois extension L/F with $G = \mathrm{Gal}(L/F)$. Given $\alpha \in L$, what can we say about: its minimal polynomial $g = m_{\alpha/F}$, the roots of g in L, and the spliting field $\Sigma_{g/F} \subseteq L$?

Given $\alpha \in L$, we write

$$G\alpha := \{\, g(\alpha) \mid g \in G \,\} \subseteq L.$$

This is called the subset of **Galois conjugates** of α in L.

Galois conjugates

Note that the $g(\alpha)$ need not be distinct for distinct g, so $G\alpha$ could have fewer elements than G.

Proposition. *Given L/F finite Galois with $G = \mathrm{Gal}(L/F)$, and $\alpha \in L$, we have the following.*

(1) *For $\alpha \in L$, we have*

$$m = m_{\alpha/F} = \prod_{\beta \in G\alpha} (x - \beta) \in F[x].$$

(2) *We have that $F(\alpha) = L^H$ where $H = \mathrm{Stab}(\alpha) = \{\, g \in G \mid g(\alpha) = \alpha \,\}$. Thus*

$$\deg m = |G\alpha| = [F(\alpha) : F] = |G : H|.$$

(3) *We have that* $\Sigma_{m/F} = F(g(\alpha),\ g \in G) = L^N$, *where* $N = \bigcap_{g\in G} gHg^{-1} \trianglelefteq G$ *is the largest normal subgroup of* G *which is contained in* H. *Thus* $\mathrm{Gal}(\Sigma_{m/F}/F) \approx G/N$.

Proof. For (1), note that any $g \in G$ applied to $f = \prod_{\beta\in G\alpha}(x-\beta)$ just permutes the factors, so in fact $f \in (L[x])^G = L^G[x] = F[x]$. It must be irreducible over F, since G acts transitively on the set of roots of f, so it cannot factor over F non-trivially.

For (2), clearly $F(\alpha) \subseteq L^H$, so equality holds since $\deg m = |G\alpha| = |G/H| = [L^H : F]$ using the orbit/stabilizer theorem.

For (3), clearly the splitting field of m is generated by its roots, which are exactly the the Galois conjugates of m. We know from the Galois correspondence that

- $g(F(\alpha)) = F(g(\alpha))$ corresponds to gHg^{-1}, and
- $\Sigma_{m/F}$ is the composite field of the $F(g(\alpha))$s, and composite fields correspond to intersection of subgroups.

□

We can say this in terms of the action of the Galois group G on the *set* L of elements in the Galois extension: there is a bijective correspondence

$$\big\{\text{orbits of action of } G \text{ on } L\big\} \longleftrightarrow \big\{f \in \mathrm{Irred}(F) \text{ which have a root in } L\big\},$$

where the orbit corresponding to f is the set of roots of f. Furthermore, the size of the orbit is the degree of the corresponding irreducble.

Example. Consider $\mathbb{C}/\mathbb{R}$ with $|G| = 2$. Then orbits of G acting on $\mathbb{C}$ have the form (i) $\{c\}$, $c \in \mathbb{R}$, or (i) $\{\lambda, \overline{\lambda}\}$, $\lambda \in \mathbb{C} \smallsetminus \mathbb{R}$. These correspond to polynomials in $\mathbb{R}[x]$ of the form (i) $f = x - c$, or (ii) $f = x^2 + bx + c$ with $b^2 < 4c$. In particular, all $f \in \mathrm{Irred}(\mathbb{R})$ have degree 1 or 2.

Example. Fix a prime p. Then every finite field of characteristic p is isomorphic to $\mathbb{F}_{p^n}$ for some $n \geq 1$. Note that each $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension with cyclic Galois group $G = \langle\phi\rangle \approx C_n$ generated by Frobenius. The intermediate fields of this are exactly the $\mathbb{F}_{p^d}$ for all divisors $d \mid n$, and note that since G is abelian there is only one subfield of $\mathbb{F}_{p^n}$ which is isomorphic to a given $\mathbb{F}_{p^d}$.

We can use this to count the number of irreducible polynomials of degree n in $\mathbb{F}_p[x]$. In fact, if we write $m_d :=$ number of monic irreducibles in $\mathbb{F}_p[x]$ of degree d, we have the formula

$$p^n = \sum_{d|n} d m_d, \qquad \text{for all } n \geq 1.$$

Using this we can inductively compute m_d:

$$\begin{aligned} m_1 &= (p)/1, & m_5 &= (p^5 - p)/5, \\ m_2 &= (p^2 - p)/2, & m_6 &= (p^6 - p^3 - p^2 + p)/6, \\ m_3 &= (p^3 - p)/3, & m_7 &= (p^7 - p)/7, \\ m_4 &= (p^4 - p^2)/4, & m_8 &= (p^8 - p^4)/8. \end{aligned}$$

To see this, note that if $f \in \mathrm{Irred}(\mathbb{F}_p)$ with $\deg f = d$, then its splitting field must be isomorphic $\mathbb{F}_{p^d}$. In fact, f has a root in $\mathbb{F}_p[x]/(f) \approx \mathbb{F}_{p^d}$, and therefore splits since this is a Galois extension over $\mathbb{F}_p$. Since $\mathbb{F}_{p^n}$ contains a subfield isomorphic to $\mathbb{F}_{p^d}$ if and only if $d \mid n$, we see that: *f has a root over $\mathbb{F}_{p^n}$ iff f splits over $\mathbb{F}_{p^n}$ iff $d \mid n$.*

Now consider the orbits of the action by $G \approx C_n$ on $\mathbb{F}_{p^n}$, so that

$$|\mathbb{F}_{p^n}| = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}| = \sum_{d|n} d \cdot (\text{number of orbits of size } d) = \sum_{d|n} d m_d,$$

because an orbits of size d is exactly the set of roots of a monic irreducible of degree d, and all of these split over $\mathbb{F}_{p^n}$.

40. Primitive element theorem

Lemma. *Suppose F is an* infinite *field. Let V be a finite dimensional F-vector space, and suppose that $W_1, \dots, W_k$ is a finite collection of subspaces. If $V = W_1 \cup \cdots \cup W_k$, then $V = W_i$ for some i.*

Proof. Let $n = \dim V$; we argue by induction on n, noting that the cases of $n = 0$ and $n = 1$ are obvious. Consider $V' \subsetneq V$ any proper subspace, and let $W_i' := V' \cap W_i$. Then $V' = W_1' \cup \cdots \cup W_k'$, and so by the inductive argument $V' = W_i'$ for some i, i.e., $V' \subseteq W_i$.

Note that if V' has codimension 1 in V, the statement $V' \subseteq W_i$ implies either $V' = W_i$ or $W_i = V$. So there are two possibilities: either

(1) every codimension 1 subspace of V is an element of the set $\{W_1, \dots, W_k\}$, or
(2) there exists an i such that $W_i = V$.

So we can finish the proof by showing that for $n \geq 2$ there are infinitely many distinct codimension 1 subspaces of V, which without loss of generality we can take to be F^n. Given $a \in F$, let

$$V_a = \{\, (x_1, \dots, x_n) \in F^n \mid x_1 = a x_2 \,\}.$$

Each V_a is the kernel of a surjective linear map $F^n \to F$ and so has codimension 1 in F^n. If $a \neq b$, then $v = (a, 1, 0, \dots, 0)$ is in V_a but not in V_b, whence $V_a \neq V_b$. Since F is infinite, this gives infinitely many such subspaces.

□

The primitive element theorem says that all finite separable field extensions are simple extensions.

Theorem (Primitive element theorem)**.** *Let K/F be a finite separable field extension. Then there exists $\gamma \in K$ such that $K = F(\gamma)$.*

Proof. The case of finite fields is easy: if F is finite then so is K, and if $|K| = p^k$ any primitive $(p^k - 1)$st root of unity in K is certainly a primitive element. Thus we are left with the case of infinite fields.

Let L be a normal closure of K/F. Then L/F is a finite Galois extension, and hence by the Galois correspondence there exist only finitely many intermediate extensions (corresponding to the finitely many subgroups of the Galois group). Therefore K/F also has only finitely many intermediate extensions.

Let $K_1, \dots, K_r$ be the list of *proper* intermediate extensions of K/F. Then by the above lemma, there exists $\gamma \in K \smallsetminus (K_1 \cup \cdots \cup K_r)$, which necessarily satisfies $F(\gamma) = K$. □

41. Cyclotomic extensions

Let K be a field, let $n \geq 1$, and suppose there exists a primitive nth root of unity $\zeta = \zeta_n \in K$. This is equivalent to saying there is a cyclic subgroup of order n in $K^\times$, with ζ_n as its generator.

This ζ_n is a root of $f = x^n - 1$, which is defined over the prime subfield of K. Note that every ζ^k must be a root of f, so f must be a separable polynomial, since the elements in the list $1, \zeta, \dots, \zeta^{n-1}$ are pairwise distinct because ζ is a *primitive* nth root of unity. Clearly, f and $Df = nx^{n-1}$ are relatively prime iff $n \neq 0$ in the field.

Therefore: a primitive nth root of unity can exist in K only if $\operatorname{char} K = 0$ or $\operatorname{char} K = p > 0$ with $p \nmid n$. Conversely, if either $\operatorname{char} K = 0$ or $\operatorname{char} K = p > 0$ with $p \nmid n$, then K has a finite extension field which has a primitive nth root of unity.

Now let's assume $\operatorname{char} K = 0$ or $\operatorname{char} K = p > 0$ and $p \nmid n$, and consider an extension $K = F(\zeta_n)/F$. This is a Galois extension. What can we say about $G = \operatorname{Gal}(F)$?

For any $g \in G$, we have that $g(\zeta_n) = \zeta_n^k$ for some $k \in \mathbb{Z}$. This k is well-defined modulo n. Since g restricts to an automorphism of the group $\langle \zeta_n \rangle \subseteq K^\times$, it must take ζ_n to a another generator of this group. Thus we must have $\gcd(k, n) = 1$.

Thus we have a function

$$\pi\colon \operatorname{Gal}(K/F) \to (\mathbb{Z}/n)^\times, \qquad g(\zeta_n) = \zeta_n^{\phi(g)}.$$

This is a group homomorphism:

$$(gh)(\zeta_n) = g(h(\zeta_n)) = g(\zeta^{\phi(h)}) = (\zeta^{\phi(g)})^{\phi(h)} = \zeta^{\phi(g)\phi(h)}, \qquad \Longrightarrow \qquad \phi(gh) = \phi(g)\phi(h).$$

This is injective: $g \in \operatorname{Ker}\pi$ iff $\phi(g) = 1$ iff $g(\zeta_n) = \zeta_n$.

Thus, for any F (with characteristic not dividing n) we have that $G = \operatorname{Gal}(F(\zeta)/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n)^\times$.

Remark. If used a different primitive nth root of unity $\epsilon = \zeta_n^a$ instead of ζ_n, we actually get the same formula:

$$g(\epsilon) = g(\zeta^a) = (\zeta^{\phi(g)})^a = (\zeta^a)^{\phi(g)} = \epsilon^{\phi(g)}.$$

Thus G is *naturally* isomorphic to a subgroup of $(\mathbb{Z}/n)^\times$.

One case when the image of π is surjective is when $F = \mathbb{Q}$.

Proposition. *We have that* $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx (\mathbb{Z}/n)^\times$.

Proof. Since $\Phi_n \in \operatorname{Irred}(\mathbb{Q})$, we have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n)^\times|$. □

Remark. The structure of these groups is understood. Suppose $n = p_1^{k_1} \cdots p_r^{k_r}$ is a prime factorization. The Chinese Remainder Theorem gives

$$(\mathbb{Z}/n)^\times \approx (\mathbb{Z}/p_1^{k_1})^\times \cdots \times (\mathbb{Z}/p_r^{k_r}).$$

Then you can show that for p odd,

$$(\mathbb{Z}/p^k)^\times \approx C_{p^{k-1}} \times C_{p-1} = \langle 1+p \rangle \times \langle a \rangle, \qquad k \geq 1,$$

where $a = b^{p^{k-1}}$ and a projects to a generator of $(\mathbb{Z}/p)^\times$. When $p = 2$ this is slightly different:

$$(\mathbb{Z}/p^k)^\times \approx C_{2^{k-2}} \times C_2 = \langle 1 + 2^2 \rangle \times \langle -1 \rangle, \qquad k \geq 2.$$

Example (Cyclotomic extensions of $\mathbb{F}_p$). Suppose $p \nmid n$. Then $\operatorname{Gal}(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p)$ is a cyclic group of order d, generated by the Frobenius automorphism $\phi(a) = a^p$, where $d =$ the order of p in $(\mathbb{Z}/n)^\times$

Thus, $\mathbb{F}_p(\zeta_n) \approx \mathbb{F}_{p^d}$, where $d =$ the smallest power of p which is congruent to 1 modulo n.

An extension L/F is **abelian** if L/F is Galois and $\operatorname{Gal}(L/F)$ is abelian. The cyclotomic extensions provide a large class of abelian extensions, and in fact supply all abelian extensions of $\mathbb{Q}$. **abelian extension**

Theorem (Kronecker-Weber)**.** *Every finite abelian extension $L/\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*

This is a non-trivial theorem, the subject for a course in algebraic number theory.

42. Extensions by nth roots

Let F be a field. Let $n \geq 1$, and suppose either $\operatorname{char} F = 0$ or $\operatorname{char} F = p > 0$ with $p \nmid n$.

Then for any $c \in F$, the polynomial $f = x^n - c \in F[x]$ is separable. Form its splitting field L/K. If $\alpha, \beta \in L$ are two roots of f, then

$$(\beta/\alpha)^n = \beta^n/\alpha^n = c/c = 1,$$

an nth root of unity. Since there are n distinct roots, a primitive nth root of unity must appear as such a ratio. Thus

$$L = F(\alpha, \zeta), \qquad \alpha^n = c, \quad \zeta \in L^\times, \ \ |\zeta| = n,$$

where $\alpha = \sqrt[n]{c}$ is a chosen nth root of c, and ζ a chosen nth root of unity. The roots of f in L are $\{\alpha, \alpha\zeta, \ldots, \alpha\zeta^{n-1}\}$.

Let $K = F(\zeta)$. We have a chain of extensions $F \subseteq K \subseteq L$, all of which are normal and separable.

Let $G = \mathrm{Gal}(L/F)$, and let $H = \mathrm{Gal}(L/K)$, so $\mathrm{Gal}(K/F) \approx G/H$. Since K/F is a cyclotomic extension, we can identify G/H with a subgroup of $(\mathbb{Z}/n)^\times$ via $\phi\colon G/H \rightarrowtail (\mathbb{Z}/n)^\times$ by $g(\zeta) = \zeta^{\phi(g)}$.

If $h \in H$, then $h(\zeta) = \zeta$. Thus $h(\alpha) = \alpha\zeta^a$ for some integer a, which is unique modulo n. We thus define a function

$$\psi\colon H \to \mathbb{Z}/n, \qquad h(\alpha) = \alpha\zeta^{\psi(h)}.$$

This is a group homomorphism:

$$hh'(\alpha) = h(\alpha\zeta^{\psi(h')}) = \alpha\zeta^{\psi(h)}\zeta^{\psi(h')} = \alpha\zeta^{\psi(h)+\psi(h')}.$$

Furthermore, it is injective, since $L = K(\alpha)$. Therefore H isomorphic to a subgroup of $\mathbb{Z}/n$.

Recall that a group G is *solvable* if there exists a chain of subgroups

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G,$$

each normal in the next, so that the quotionts G_k/G_{k-1} are abelian.

Proposition. *Let L/F be a splitting field of $x^n - c \in F[x]$, where $\mathrm{char}\, F$ does not divide n. Then $G = \mathrm{Gal}(L/F)$ is a solvable group, of order dividing $n\phi(n)$*

Proof. We have $H \leq \mathbb{Z}/n$ and $G/H \leq (\mathbb{Z}/n)^\times$, which are both abelian. □

Remark. In general, the action of a particular element $g \in G$ on L/F is determined by formulas of the form

$$g(\alpha) = \alpha\zeta^a, \qquad g(\zeta) = \zeta^b,$$

for some $a \in \mathbb{Z}/n$ and $b \in (\mathbb{Z}/n)^\times$ depending on g. Using this, you can see that G will be isomorphic to some *subgroup* of the semi-direct product group $G' = (\mathbb{Z}/n) \rtimes_\alpha (\mathbb{Z}/n)^\times$, where $\alpha\colon (\mathbb{Z}/n)^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n)$ is the standard isomorphism, defined by $b \mapsto (a \mapsto ab)$. Thus the group structure of G' is given by

$$(a, b) \cdot (a', b') = (a + ba', bb').$$

Exercise. Show that if p is prime, then the Galois group of the splitting field of $f = x^p - 2$ over $\mathbb{Q}$ is the largest possible, i.e., of order $p(p-1)$.

43. Solvability by radicals

M 5 Dec

Assume $\mathrm{char}\, F = 0$. Recall a **radical extension** K/F is an extension such that there exists a chain of extensions **radical extension**

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K, \qquad K_j = K_{j-1}(\sqrt[n_j]{c_j}), \quad n_j \geq 1, \quad c_j \in K_{j-1},$$

where we use the symbol "$\sqrt[n]{c}$" to denote any root of the polynomial $x^n - c$.

We say that $f \in F[x]$ is **solvable by radicals** if its splitting field Σ/F is contained in some radical extension L/F. **solvable by radicals**

Lemma. *If $K, K' \subseteq L/F$ such that K/F and K'/F are radical extensions, then KK'/F is a radical extension.*

Proof. A straightforward induction, based on the case of $K' = F(\sqrt[n]{c})$, in which case $KK' = K(\sqrt[n]{c})$. □

Lemma. *If K/F is a radical extension, then it is contained in some Galois radical extension.*

Proof. Given K/F, form a normal closure L/F, which is Galois with Galois group G. Then L is the composite subfield of the collection of subfields $\{\, g(K) \mid g \in G \,\}$. Since each $g(K)/F$ is isomorphic to K/F it is radical, and thus L/F is radical and Galois. □

Proposition. *If K/F is contained in a radical extension, then $\mathrm{Aut}(K/F)$ is solvable.*

Proof. Choose a radical extension R/F containing K, and then choose a Galois closure L/F of R/F, which is also radical. We have that $\mathrm{Aut}(K/F) \approx N_G(H)/H$ where $H = \mathrm{Aut}(L/K) \leq N_G(H) \leq G$. We know that any subgroup and quotient group of a solvable group are solvable. Thus it suffices to show that G is solvable.

Since L/F is radical, there is a chain $F = K_0 \subseteq \cdots \subseteq K_r = L$ with $K_j = K_{j-1}(\sqrt[n_j]{c_j})$. Inductively define L_j so that $L_0 = K_0 = F$, and $L_j =$ the normal closure of $L_{j-1}(\sqrt[n_j]{c_j})$, (i.e., the splitting field of $x^{n_j} - c_j$ over L_{j-1}) which is contained in L since L/F is normal. Thus $L_r = L$.

We thus have a chain of extensions

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{r-1} \subseteq L_r = L,$$

such that each L_j/L_{j-1} is normal. Thus the associated chain of Galois groups $G_j = \mathrm{Gal}(L/L_j)$ has the form

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{r-1} \trianglerighteq G_r = \{e\},$$

with each $G_{j-1}/G_j = \mathrm{Gal}(L_j/L_{j-1})$ a solvable group, since L_j/L_{j-1} is a splitting field for $x^{n_j} - c_j \in L_{j-1}[x]$. Thus G is solvable. □

44. A polynomial which is not solvable by radicals

Proposition. *Let p be a prime number. Let $f \in \mathrm{Irred}(\mathbb{Q})$ with $\deg f = p$, such that f has exactly two non-real roots in $\mathbb{C}$. Then the Galois group of the splitting field of f is isomorphic to S_p.*

Proof. Let $L \subseteq \mathbb{C}$ be the splitting field. Since f is irreducible it is separable, by labelling the roots we can identify $G = \mathrm{Gal}(L/\mathbb{Q})$ with a subgroup of S_p.

We have that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p$, so p divides $[L : F] = |G|$. By Cauchy's theorem there exists an element of order p in G, which must therefore be a p-cycle $\sigma \in S_p$.

Let $\tau \in G$ be the automorphism induced by complex conjugation (defined because $\mathbb{Q} \subseteq \mathbb{R}$). Then τ corresponds to a 2-cycle in S_p, since there are only two non-real roots.

The statement now follows from the following. □

Proposition. *For p prime, we have $S_p = \langle \sigma, \tau \rangle$, where σ is any p-cycle and τ is any 2-cycle.*

Proof. WLOG we can assume $\tau = (1\ 2)$. Replace σ with a power of it which sends 1 to 2, which will also be a p-cycle since p is prime. Thus we can assume WLOG that $\sigma = (1\ 2\ \cdots\ p)$. (More precisely: there is an inner automoprhism of S_p which sends the original σ and τ to these new cycles.)

Then $\sigma^{k-1}\tau\sigma^{-(k-1)} = (k\ k+1)$, and the set of such transpositions with $k = 1, \ldots, p-1$ generate S_p. □

Example. Let $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$. This is irreducible over $\mathbb{Q}$ by Eisenstein, using $p = 3$.

Furthermore, f has exactly 3 real roots. To show this, note that $D(f) = 5x^4 - 6$ has exactly two real roots (at $\pm\sqrt[4]{6/5}$), neither of which is repeated. Thus the derivative of f changes sign exactly twice over $\mathbb{R}$. We have

$$\lim_{x\to-\infty} f(x) = -\infty, \qquad f(0) = 3 > 0, \qquad f(1) = -2 < 0, \qquad \lim_{x\to+\infty} f(x) = +\infty,$$

and since $-\sqrt[4]{6/5} < 0 < 1 < \sqrt[4]{6/5}$, we can deduce using the intermediate value theorem that f has exactly 3 real roots.

Thus, by the preceding proposition, the Galois group of the splitting field is isomorphic to S_5, which is not solvable. Therefore f is not solvable by radicals.

45. Linear independence of characters

For any field L, and any set S, the set of all functions $\mathcal{F}(S, L)$ is itself a vector space over L, by "pointwise" addition and scalar multiplication.

Proposition (Linear independence of "characters")**.** *Let G be a group, L a field, and let $\chi_1, \dots, \chi_n$ be distinct homomorphisms $G \to L^\times$. Then, viewed as functions $G \to L$, they form a linearly independent subset of $\mathcal{F}(G, L)$.*

Proof. We show that if $a_1, \dots, a_n \in L$ are such that $\sum_j a_j \chi_j = 0$, then all $a_j = 0$. This amounts to showing: if $\sum_j a_j \chi_j(g) = 0$ for all $g \in G$, then all $a_j = 0$.

Key observation: for any non-trivial linear dependence $\sum_j a_j \chi_j = 0$ and $h \in G$, we can produce a new linear dependence $\sum_j a_j \chi_j(h) \chi_j = 0$, since

$$0 = a_1\chi_1(hg) + \cdots + a_n\chi_n(hg) = a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g).$$

Then, by subtracting $\phi_n(h) \sum_j a_j \phi_j = 0$ from this new dependence, we get

$$a_1\big(\phi_1(h) - \phi_n(h)\big)\phi_1 + \cdots + a_{n-1}\big(\phi_{n-1}(h) - \phi_n(h)\big)\phi_{n-1}.$$

We argue by contradiction, i.e., suppose there exists a non-trivial linear dependence $\sum_{j=1}^n a_j \chi_j = 0$. Choose among these one with shortest length m, i.e., smallest (positive) number of non-zero coefficients. By relabelling this has the form $\sum_{j=1}^m a_j \chi_j$ with $a_1, \dots, a_m$ non-zero.

- If $m = 1$, then $a_1\chi_1 = 0$, whence $a_1\chi(1) = a_1$ (where $1 \in G$ is the identity element), contradicting $a_1 \neq 0$.
- If $m \geq 2$, then since $\chi_1 \neq \chi_m$ we can find $h \in H$ such that $\chi_1(h) \neq \chi_m(h)$. Then using the argument above we get a new linear dependence

$$a_1\big(\chi_1(h) - \chi_m(h)\big)\chi_1 + \cdots + a_{n-1}\big(\chi_{m-1}(h) - \chi_m(h)\big)\chi_{m-1}, \qquad a_1\big(\chi_1(h) - \chi_m(h)\big) \neq 0.$$

  This contradicts the minimality.

□

Consider fields K and L. The set $\mathrm{Emb}(K, L)$ of embeddings is a subset of the set of all functions $\mathcal{F}(K, L)$.

Corollary (Linear independence of embeddings)**.** *The subset $\mathrm{Emb}(K, L)$ of $\mathcal{F}(K, L)$ is linearly independent over L.*

Proof. Restriction along $K^\times \subset K$ defines a surjective L-linear map $\mathcal{F}(K, L) \twoheadrightarrow \mathcal{F}(K^\times, L)$. To show $\mathrm{Emb}_F(K, L) \subseteq \mathcal{F}(K, L)$ is linearly independent, it suffices to show that its image in $\mathcal{F}(K^\times, L)$ is linearly independent. (Note that distinct embeddings still differ as functions $K^\times \to L$, since they all send $0 \mapsto 0$.)

But a field homomorphism $\phi\colon K \to L$ restricts to a "character", i.e., a group homomorphism $\phi\colon K^\times \to L^\times$. Thus the claim results from linear independence of characters applied to $G = K^\times$. □

46. Kummer theory

A **cyclic extension** is a finite Galois extension with cyclic Galois group. It turns out we can completely classify cyclic extensions over fields which have "enough" roots of unity: in this case they are exactly the root-extensions. **cyclic extension**

Theorem (Kummer theory)**.** *Let F be a field which contains a primitive nth root of unity ζ. Consider a finite Galois extension L/F with $[L : F] = n$. The following are equivalent.*

(1) *$G = \mathrm{Gal}(L/F)$ is a cyclic group.*
(2) *There exists $c \in F$ such that $f = x^n - c \in \mathrm{Irred}(F)$ and $L = F(\sqrt[n]{c})$.*

Proof. (2) $\implies$ (1). We have basically already done this: Since F contains a primitive nth root of unity, we have an injective homomorphism $\rho\colon G \rightarrowtail \mathbb{Z}/n$ defined by $g(\sqrt[n]{c}) = \zeta^{\rho(g)}\sqrt[n]{c}$. Since f is irreducible, we have $[L : F] = |G| = n$, so this is an isomorphism.

(1) $\implies$ (2). Fix a primitive nth root of unity $\zeta \in F$, and a generator $\sigma \in G$ of the cyclic group. For $\alpha \in L$, we define a function $\lambda\colon L \to L$ by

$$\lambda(\alpha) := \sum_{k=0}^{n-1} \zeta^{-k}\, \sigma^k(\alpha) = \alpha + \zeta^{-1}\sigma(\alpha) + \zeta^{-2}\sigma^2(\alpha) + \cdots + \zeta^{-(n-2)}\sigma^{n-2}(\alpha) + \zeta^{-(n-1)}\sigma^{n-1}(\alpha) \in L.$$

We can compute that

$$\begin{aligned}\sigma(L\lambda(\alpha)) &= \sigma(\alpha) + \zeta^{-1}\sigma^2(\alpha) + \zeta^{-2}\sigma^3(\alpha) + \cdots + \zeta^{-(n-2)}\sigma^{n-1}(\alpha) + \zeta^{-(n-1)}\alpha \\ &= \zeta\lambda(\alpha).\end{aligned}$$

Therefore

$$\big(\sigma(\lambda(\alpha)\big)^n = \zeta^n\lambda(\alpha)^n = \lambda(\alpha)^n,$$

so $\lambda(\alpha)^n \in L^G = F$.

Suppose we find $\alpha \in L$ such that $\beta := L(\alpha) \neq 0$. Then $c := \beta^n \in F$, and also $\sigma^k(\beta) = \zeta^k\beta$, which means that β is not fixed by any non-identity element of G, so $L = F(\beta)$. This exhibits $L = F(\sqrt[n]{c})$ as desired.

The existence of such an α is given by linear independence of embeddings. If no such α exists, then $\lambda(\alpha) = 0$ for all $\alpha \in L$, whence we have a non-trivial linear dependence

$$\mathrm{id} + \zeta^{-1}\sigma + \cdots + \cdots + \zeta^{-(n-1)}\sigma^{n-1} = 0$$

of elements of G. But $G \subseteq \mathrm{Emb}(L, L) \subseteq \mathcal{F}(L, L)$, which is an L-linearly indpendent subset, so this is impossible. □

Remark. The hypothesis about having a primitive root of unity in F is necessary. In particular, if L/F is a cyclic Galois extension of *prime* degree p such that F does *not* contain a primitive pth root of unity, then there is no $\alpha \in L \smallsetminus F$ such that $\alpha^p \in F$. (Exercise: prove this.)

An example is the splitting field L of $f = x^3 + x^2 - 2x - 1 \in \mathrm{Irred}(\mathbb{Q})$. As we have seen, $G = \mathrm{Aut}(L/\mathbb{Q})$ is cyclic of order 3. In fact, $L \subseteq \mathbb{Q}(\zeta_7)$, where $\zeta_7^k + \zeta_7^{-k}$ for $k = 1, 2, 3$ are the roots of f. However, there is no $\alpha \in L \smallsetminus \mathbb{Q}$ such that $\alpha^3 \in \mathbb{Q}$. (Exercise: why is there no such α?)

47. Classification of solvable polynomials

We can use Kummer theory to give a criterion for radical extensions, as long as the base field has "enough" roots of unity. **W 7 Dec**

Proposition. *Let L/F be a Galois extension with solvable Galois group G, with $n = |G|$. If F contains a primitive nth root of unity, then L/F is a radical extension.*

Proof. Since G is solvable, there exists a chain of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{e\}$$

with each $G_j \trianglelefteq G_{j-1}$ and G_{j-1}/G_j is finite cyclic. Note that $|G_{j-1} : G_j|$ divides n.

We have a corresponding chain of fixed fields

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r = L,$$

where $L_j = L^{G_j}$. We have that each L_j/L_{j-1} is finite Galois with cyclic Galois group of order n_j dividing n. By hypothesis, F contains a primitive n_jth root of unity, so by Kummer theory we have $L_j = L_{j-1}(\sqrt[n_j]{c_j})$. □

We can now give a complete classification of which polynomials $f \in F[x]$ are solvable over radicals.

Proposition. *Let F be a field of characteristic 0, and let L/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/F)$. Then TFAE.*

(1) *There exists a finite extension R/L such that R/F is a radical extension.*

(2) *G is a solvable group.*

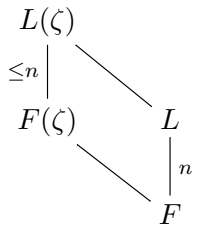
Corollary. *A polynomal $f \in F[x]$ over a field of characteristic 0 is solvable by radicals iff the Galois group of its splitting field is solvable.*

Proof of proposition. (1) $\implies$ (2). We can replace R/F by its normal closure, which will be a radical Galois extension. Then $G' := \mathrm{Gal}(R/F)$ is solvable, as we have seen. Since L/F is Galois, $G \approx G'/N$ where $N = \mathrm{Gal}(R/F)$, so G is solvable.

(2) $\implies$ (1). Let $n = [L : F]$.

We suppose G is solvable. Write $n = [L : F] = |G|$, and form an extension $L \subseteq L(\zeta)$ where ζ is a primitive $(n!)$th root of unity. Thus, $F(\zeta)$ contains a primitive kth root of unity for all $1 \leq k \leq n$. We are going to show $L(\zeta)/F$ is a radical extension.

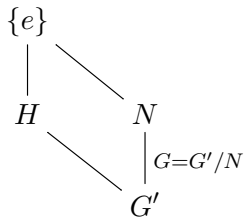
We have the following diagram of fields.



We know L/F and $F(\zeta)/F$ are normal, and so are splitting fields of polynomials f and $x^n - 1$ in $F[x]$. Therefore $L(\zeta)/F$ is also a splitting field of $(x^n - 1)f$ in $F[x]$ and so is also normal. Thus all extensions pictured are Galois.

The cyclotomic extenion $F(\zeta)/F$ is certainly radical, so it suffices to show $L(\zeta)/F(\zeta)$ is radical.

We have a corresponding diagram of Galois groups.



Since $L(\zeta) = F(\zeta)L$ is a composite extension, from the Galois correspondence we have $H \cap N = \{e\}$, and thus the homomorphism $H \to G'/N \approx G$ by $h \mapsto hN$ is injective. Since $H = \mathrm{Gal}(L(\zeta)/F(\zeta))$ is isomorphic to a subgroup of the solvable group G it is also solvable.

Also, since $L(\zeta) = F(\zeta)L$, we have that $k = [L(\zeta) : F(\zeta)] \leq n = [L : F]$. By construction F contains a primitive kth root of unity, so the previous proposition applies to show $L(\zeta)/F(\zeta)$ is solvable. □

Exercise. The theorem requires that L/F be a *Galois* extension. This is necessary. Give an example of a finite extension $L/\mathbb{Q}$ such that $\mathrm{Aut}(L/\mathbb{Q})$ is solvable, but $L/\mathbb{Q}$ is not contained in any radical extension of $\mathbb{Q}$.

48. Ordered fields and square roots

Recall that an *ordered* field F is a pair $(F, F_{>0})$, where $F_{>0}$ is a subset of F for which:

- $1 \in F_{>0}$, and $a, b \in F_{>0}$ imply $a + b, ab \in F_{>0}$, and
- for all $a \in F$, exactly one of the following hold: (i) $a \in F_{>0}$, (ii) $-a \in F_{>0}$, (iii) $a = 0$.

The subset $F_{>0}$ is thus the subset of **positive elements**. This implies that that F must have characteristic 0, since $1 + \cdots + 1 \in F_{>0}$. Given this you can define an order relation $a < b$ (equivalent

positive elements

to $b - a \in F_{>0}$), and show it has the usual properties. In particular, you have that $(F^\times)^2 \subseteq F_{>0}$, i.e., non-zero squares are always positive.

In some cases (e.g., $\mathbb{R}$, but not $\mathbb{Q}$), all positive elements are squares.

Proposition. *Let F be a field, and form $L = F(i)$ where i is a root of $x^2 + 1 \in F[x]$. TFAE.*

(1) *F has the structure of an ordered field with $F_{>0} = (F^\times)^2$.*
(2) *$i \notin F$ and $L^\times = (L^\times)^2$.*

If these are true, L has no quadratic extensions.

Proof. (1) $\implies$ (2). Since $-1 \notin F_{>0}$, clearly $i \notin F$. Every element of F has a squareroot in L: by hypothesis if $a \geq 0$, while if $a < 0$ then $a = (bi)^2$ with $b^2 = -a$, $b \in F$.

For $u = a + bi \in L$, $a, b \in F$, $b \neq 0$, we can choose a square root $r = \sqrt{a^2 + b^2} \in F_{>0}$. Then

$$\sqrt{\frac{a+r}{2}} + \sqrt{\frac{a-r}{2}} \in L$$

is a squareroot of u, where the signs on the squareroots are chosen so that

$$\sqrt{\frac{a+r}{2}}\,\sqrt{\frac{a-r}{2}} = \sqrt{\frac{-b^2}{4}} = +\frac{bi}{2}.$$

(This is basically the same thing as the "half-angle formula" from trigonometry: $\cos^2(\theta/2) = (1 + \cos\theta)/2$ and $\sin^2(\theta/2) = (1 - \cos\theta)/2$, so $e^{i\theta/2} = \sqrt{(1+\cos\theta)/2} + i\sqrt{(1-\cos\theta)/2}$ if $-\pi \leq \theta \leq \pi$.)

(2) $\implies$ (1). Note that since $i \notin F$, we have $x^2 + 1 \in \mathrm{Irred}(F)$. Therefore $\mathrm{char}\, F \neq 2$, since otherwise $x^2 + 1 = (x+1)^2$. Also, $[L : F] = 2$.

We set $F_{>0} := (F^\times)^2$ and show it has the properties of a set of positive elements.

- Clearly $1 \in F_{>0}$, and $F_{>0}$ is closed under multiplication since $a^2b^2 = (ab)^2$.
- Suppose $a, b \in F$. Then $a + bi = (c + di)^2$ for some $c, d \in F$, so

  $$a^2 + b^2 = (a + bi)(a - bi) = (c + di)^2(c - di)^2 = \big[(c + di)(c - di)\big]^2 = (c^2 + d^2)^2,$$

  so $F_{>0}$ is closed under addition.
- Suppose $a \in F^\times$. Then

  $$a = (c + di)^2 = (c^2 - d^2) + (2cd)i$$

  for some $c, d \in F$ not both 0. Since $i \notin F$ we have $2cd = 0$, whence (since $\mathrm{char}\, F \neq 2$) either (i) $a = c^2$ or (ii) $a = -d^2$. If $a, -a \in F_{>0} = (F^\times)^2$ then $-1 = (-a)/a \in (F^\times)^2$, but this is impossible since $i \notin F$. Thus if $a \neq 0$ then either a or $-a$ is in $F_{>0}$ but not both.

  The final statement about quadratic extensions is clear: every degree 2 polynomial over L has a root in L, because L has squareroots and $\mathrm{char}\, L \neq 2$, so the quadratic formula applies.

□

49. Real closed fields

A **real closed field** is an *ordered* field R such that (i) every positive element of R has a square root in R, and (ii) every polynomial of odd degree over R has a root in R. **real closed field**

Thus in this case we have we have $R_{>0} = (R^\times)^2$, i.e., positive elements are exactly the non-zero squares in R.

Example. The real numbers are a real closed field. The proofs of (i) and (ii) use the intermediate value theorem: $f(x) = x^2 - a$ with $a > 0$ has $\lim_{x\to\pm\infty} f(x) = +\infty$, and $f(0) < 0$, whence f has roots, while $g(x)$ of odd degree is such that $\lim_{x\to+\infty} g(x)$ and $\lim_{x\to-\infty} g(x)$ are infinite with opposite signs.

Example. The field $F = \mathbb{Q}^{\mathrm{alg}} \cap \mathbb{R}$ consisting of real numbers which are algebraic is real closed.

Example. A **Puiseux series** over F in some variable x is an expression of the form **Puiseux series**

$$f = \sum_{k \geq k_0}^{\infty} c_k x^{k/n}, \qquad n \geq 1, \quad k_0 \in \mathbb{Z}, \qquad c_k \in F.$$

Let $F\{x\}$ denote the set of Puiseux series. This set natually a commutative ring, via the "obvious" operations. In fact, it is a field.

If R is real closed, then so is $R\{x\}$. Positive elements of $R\{x\}$ are non-zero series $f = \sum_{k \geq k_0} c_k x^{k/n}$ such that the smallest non-zero c_{k_0} is positive.

50. Proof of the fundamental theorem of algebra

Proposition. *A field R is a real closed field iff $C := R(i)$ is algebraically closed and $i \notin R$.*

Corollary. *The complex numbers are algebraically closed.*

Proof. $\Longleftarrow$: Since C is algebraically closed it has all squareroots, and thus since $i \notin R$, as we have shown R has the structure of an ordered field with $R_{>0} = (R^\times)^2$.

So all positive elements of R have a squareroot by definition. Finally, all $f \in \mathrm{Irred}(R)$ must have degree 1 or 2 since $[C : R] = 2$, so any odd degree $f \in R[x]$ must have a linear factor.

(1) $\Longrightarrow$ (2). Now we suppose R is real closed. We already have showed that $i \notin C$ and that C has no degree 2 extenions. We need to show C is algebraically closed.

Recall that a **p-group** is a finite group with order p^k for some k. We use the following facts. **p-group**

- For every prime p, every finite group G has a subgroup $P \leq G$ which is a p-group, and such that $p \nmid |G : P|$. (First Sylow theorem.)
- Every non-trivial p-group has a subgroup of index p.

In fact, I only need these facts for $p = 2$.

We suppose K/C is a finite extension. This will be contained in a finite Galois extenion L/R. We will show $[L : R] = 2$, whence $C = K$ and thus C is algebraically closed. Let $G = \mathrm{Aut}(L : R)$ and $H = \mathrm{Aut}(L : C)$, so $|G : H| = 2$.

Every non-trivial simple extension $R(\alpha)/R$ has even degree, since there are no $f \in \mathrm{Irred}(R)$ with odd degree > 1. Therefore every *proper* subgroup of G has even index. In particular, consider a 2-Sylow subgroup $P \leq G$. Since $|G : P|$ is odd, we must have $G = P$, i.e., $|G| = 2^k$ for some $k \geq 1$, whence $|H| = 2^{k-1}$.

If $|H| > 1$, then there exists a subgroup $A \leq H$ with $|H : A| = 2$, and hence a degree 2 extension $C = L^H \subseteq L^K$. But this is impossible because every quadratic polynomial in C splits. $\square$

Since the reals are clearly a real closed field, this gives another proof of the algebraic closure of $\mathbb{C}$.

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL
Email address: rezk@illinois.edu