Shandong University | Advanced Modern Algebra

Lecture 9 & 10: Field Theory II

Apr. 21, 2023

Lecturer: Bin Guan

This lecture refers to §13.4, §13.5, §14.1 in [1]. All the equation numbers without reference labels are from this book.

1 Splitting fields and algebraic closures

1.1 Splitting fields and normal extensions

Let F be a field. If $f(x)$ is any polynomial in $F[x]$ then there exists a field K (for example $F[x]/(p(x))$ where $p(x) \in F[x]$ is an irreducible factor of $f(x)$) which can (by identifying F with an isomorphic copy of F) be considered an extension of F in which $f(x)$ has a root α. This is equivalent to the statement that $f(x)$ has a linear factor $x - \alpha$ in $K[x]$.

Definition. *The extension field K of F is called a **splitting field** for the polynomial $f(x) \in F[x]$ if*

- *$f(x)$ factors completely into linear factors (or **splits completely**) in $K[x]$, and*
- *$f(x)$ does not factor completely over any proper subfield of K containing F.*

*If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called a **normal extension** of F.*

Recall that if $\deg f(x) = n$, then $f(x)$ has at most n roots in F ([1] §9.5 Proposition 17) and has precisely n roots (counting multiplicities) in F if and only if $f(x)$ splits completely in $F[x]$.

Theorem ([1] §13.4 Theorem 25 & Proposition 31)**.** *For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$, which is unique up to isomorphism.*

Proof of Existence. We first show that there is an extension E of F over which $f(x)$ splits completely into linear factors by induction on the degree n of $f(x)$. If $n = 1$, then take $E = F$.

Suppose now that $n > 1$. If the irreducible factors of $f(x)$ over F are all of degree 1, then F is the splitting field for $f(x)$ and we may take $E = F$. Otherwise, at least one of the irreducible factors, say $p(x)$ of $f(x)$ in $F[x]$ is of degree at least 2. By [1] §13.1 Theorem 3 there is an extension E_1 of F containing a root α of $p(x)$. Over E_1 the polynomial $f(x)$ has the linear factor $x - \alpha$. The degree of the remaining factor $f_1(x)$ of $f(x)$ is $n - 1$, so by induction there is an extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E$, E is an extension of F containing all the roots of $f(x)$.

Now let K be the intersection of all the subfields of E containing F which also contain all the roots of $f(x)$. Then K is a field which is a splitting field for $f(x)$. □

If $f(x) \in F[x]$ is a polynomial of degree n, then adjoining one root of $f(x)$ to F generates an extension F_1 of degree at most n (and equal to n if and only if $f(x)$ is irreducible). Over F_1 the polynomial $f(x)$ now has at least one linear factor, so that any other root of $f(x)$ satisfies an equation of degree at most $n - 1$ over F_1. Adjoining such a root to F_1 we therefore obtain an extension of degree at most $n - 1$ of F_1, etc. Using the multiplicativity of extension degrees, this proves

Proposition ([1] §13.4 Proposition 26)**.** *A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.*

Exercise ([1] §13.4 Exercise 5)**.** *Let K be a finite extension of F. Prove that K/F is a normal extension if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.*

Exercise ([1] §13.4 Exercise 6)**.** *Let K_1 and K_2 be finite normal extensions of F contained in the field K. Show that K_1K_2 and $K_1 \cap K_2$ are both normal over F.*

1.2 Examples

If we already know an extension E/F such that $f(x) \in F[x]$ splits completely in $E[x]$ ($E = \bar{F}$ the algebraic closure, for example), say,

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n) \quad \text{for some } \alpha_1, \ldots, \alpha_n \in E,$$

then $F(\alpha_1, \ldots, \alpha_n)$ (which is a subfield of E) is a splitting field for $f(x)$.

Example. *The splitting field for $x^2 - 2$ over $\mathbb{Q}$ is just $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$. In general any quadratic extension $F(\sqrt{D})$ is normal over F, being a splitting field of $x^2 - D$.*

Example. *The splitting field of $x^4 + 4$ over $\mathbb{Q}$ is smaller than one might at first suspect: in fact it is a quadratic field. This polynomial factors over $\mathbb{Q}$:*

$$\begin{aligned} x^4 + 4 &= x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 \\ &= (x^2 + 2x + 2)(x^2 - 2x + 2), \end{aligned}$$

where these two factors are irreducible (by Eisenstein's Criterion). Solving for the roots of the two factors by the quadratic formula, we find the four roots $\pm 1 \pm i$ so that the splitting field of this polynomial is just the field $\mathbb{Q}(i)$.

Example. *The splitting field of $x^n - 1$ over $\mathbb{Q}$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity, where $\zeta_n = e^{2\pi i/n}$. It is an extension of degree $\varphi(n)$.*

Example (Splitting Field of $x^p - 2$, p a prime)**.** *Let p be a prime and consider the splitting field of $x^p - 2$. If α is a root of this equation, i.e., $\alpha^p = 2$, then $(\zeta\alpha)^p = 2$ where ζ is any p^{th} root of unity. Hence the solutions of this equation are $\zeta\sqrt[p]{2}$, with ζ a p^{th} root of unity, where the symbol $\sqrt[p]{2}$ denotes the positive real p^{th} root of 2 if we wish to view these elements as complex numbers, and denotes any one solution of $x^p = 2$ if we view these roots abstractly.*

Clearly $\mathbb{Q}(\sqrt[p]{2})/\mathbb{Q}$ is not a normal extension (cf. [1] §13.4 Exercise 5).

Since ζ_p is the ratio of two solutions $\zeta_p\sqrt[p]{2}$ and $\sqrt[p]{2}$ for ζ_p a primitive p^{th} root of unity, the splitting field of $x^p - 2$ over $\mathbb{Q}$ contains $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$. On the other hand, all the roots above lie in this field, so that the splitting field is precisely

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p).$$

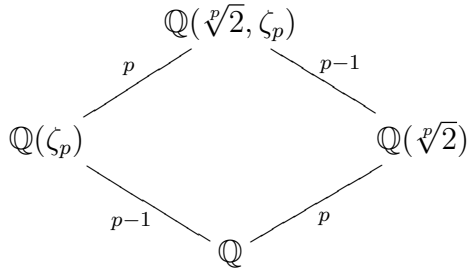
This field is the composite field of $\mathbb{Q}(\sqrt[p]{2})$ and $\mathbb{Q}(\zeta_p)$, with degree $\leq p(p-1)$ over $\mathbb{Q}$. We have

$$p = [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}], \quad p - 1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}].$$

Since p and $p-1$ are relatively prime it follows that the extension degree is divisible by $p(p-1)$ so that we must have

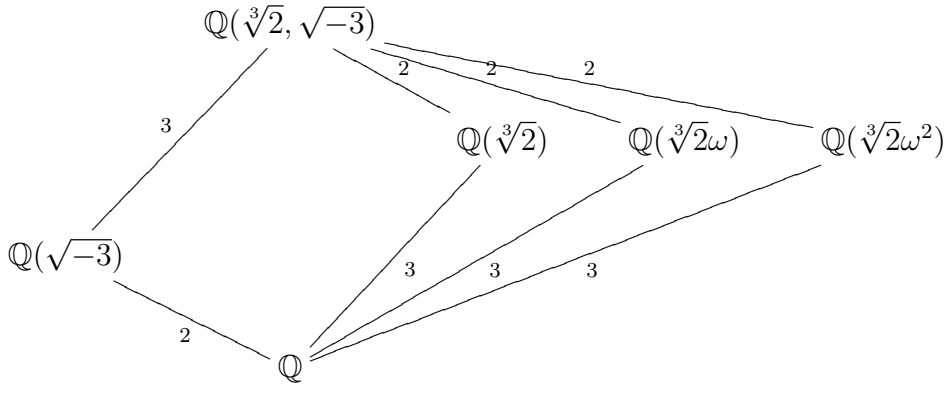
$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1).$$

We have the following diagram of known subfields:



In particular, $x^p - 2$ remains irreducible over $\mathbb{Q}(\zeta_p)$, which is not at all obvious.

When $p = 3$, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a quadratic extension. In fact $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. It follows that $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, and we have the diagram of subfields:



where $\omega = \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$.

Exercise. *Determine the splitting field and its degree over $\mathbb{Q}$ for $x^3 - 3x + 1$.*
(Hint: First verify that $\zeta_9 + {\zeta_9}^{-1}$ is a root, where ζ_9 is any primitive 9^{th} root of unity.)

Exercise. *Determine the splitting field and its degree over $\mathbb{F}_3$ for $x^6 + 2x^3 + 2$.*
(Hint: Read the proof of the existence of splitting fields. Recall that $2^3 = 2$ in $\mathbb{F}_3$, and $a^3 + b^3 = (a+b)^3$ over any integral domain of characteristic 3, cf. [1] §13.5 Proposition 35.)

1.3 Uniqueness of splitting fields

The fact that different roots of the same irreducible polynomial have the same algebraic properties can be extended slightly, as follows:

Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. The map φ induces a ring isomorphism (also denoted φ)

$$\varphi : F[x] \xrightarrow{\sim} F'[x], \qquad \sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} \varphi(a_i) x^i$$

defined by applying φ to the coefficients of a polynomial in $F[x]$.

Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the polynomial obtained by applying the map φ to the coefficients of $p(x)$, i.e., the image of $p(x)$ under φ. The isomorphism φ maps the maximal ideal $(p(x))$ to the ideal $(p'(x))$, so this ideal is also maximal, which shows that $p'(x)$ is also irreducible in $F'[x]$. The following theorem shows that the fields obtained by adjoining a root of $p(x)$ to F and a root of $p'(x)$ to F' have the same algebraic structure (i.e., are isomorphic):

Theorem ([1] §13.1 Theorem 8)**.** *Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism*

$$\begin{array}{rccc} \sigma : & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & \alpha & \longmapsto & \beta \end{array}$$

mapping α to β and extending φ, i.e., such that $\sigma|_F = \varphi$. It can be represented pictorially by the diagram

$$\begin{array}{rccc} \sigma : & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & | & & | \\ \varphi : & F & \xrightarrow{\sim} & F' \end{array}$$

Proof. As noted above, the isomorphism φ induces a natural isomorphism from $F[x]$ to $F'[x]$ which maps the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$. Taking the quotients by these ideals, we obtain an isomorphism of fields

$$F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x)).$$

By [1] §13.1 Theorem 6 the field on the left is isomorphic to $F(\alpha)$ and by the same theorem the field on the right is isomorphic to $F'(\beta)$. Composing these isomorphisms, we obtain the isomorphism σ. It is clear that the restriction of this isomorphism to F is φ, completing the proof. □

We now return to the problem of proving it makes no difference how the splitting field of a polynomial $f(x)$ over a field F is constructed. As in the above theorem it is convenient to state the result for an arbitrary isomorphism $\varphi : F \xrightarrow{\sim} F'$ between two fields.

Theorem ([1] §13.4 Theorem 27)**.** *Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying the map φ to the coefficients of $f(x)$. Let E be the splitting field for $f(x)$ over F, and let E' be the splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., $\sigma|_F = \varphi$:*

$$\begin{array}{rccc} \sigma : & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \varphi : & F & \xrightarrow{\sim} & F' \end{array}$$

Proof. By induction on the degree n of $f(x)$. □

1.4 Algebraic closures

The field $\overline{F}$ is called an **algebraic closure** of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$ (so that $\overline{F}$ can be said to contain all the elements algebraic over F). A field K is said to be **algebraically closed** if every polynomial with coefficients in K has a root in K.

Note that if K is algebraically closed, then in fact every $f(x) \in K[x]$ has all its roots in K, since by definition $f(x)$ has a root $\alpha \in K$, hence has a factor $(x-\alpha)$ in $K[x]$. The remaining factor of $f(x)$ then is a polynomial in $K[x]$, hence has a root, so has a linear factor etc., so that $f(x)$ must split completely. Hence if K is algebraically closed, then K itself is an algebraic closure of K and the converse is obvious, so that $\overline{K} = K$ if and only if K is algebraically closed.

The next result shows that the process of "taking the algebraic closure" actually stops after one step — taking the algebraic closure of an algebraic closure does not give a larger field: the field is already algebraically closed (notationally: $\overline{\overline{F}} = F$).

Proposition ([1] §13.4 Proposition 29)**.** *Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.*

Proof. Let $f(x)$ be a polynomial in $\overline{F}[x]$ and let α be a root of $f(x)$. Then α generates an algebraic extension $\overline{F}(\alpha)$ of $\overline{F}$, and $\overline{F}$ is algebraic over F. By [1] §13.2 Theorem 20, $\overline{F}(\alpha)$ is algebraic over F so in particular its element α is algebraic over F. But then $\alpha \in \overline{F}$, showing $\overline{F}$ is algebraically closed. □

Proposition ([1] §13.4 Propositions 30 & 31)**.** *For any field F there exists an algebraically closed field K containing F; the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.*

2 Separable and inseparable extensions

2.1 Separable polynomials

Let F be a field and let $f(x) \in F[x]$ be a polynomial. Over a splitting field for $f(x)$ we have the factorization

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct elements of the splitting field and $n_i \geq 1$ for all i. Here α_i is called a **multiple root** if $n_i > 1$ and is called a **simple root** if $n_i = 1$. The integer n_i is called the **multiplicity** of the root α_i.

A polynomial over F is called **separable** if it has no multiple roots (i.e., all its roots are distinct). A polynomial which is not separable is called **inseparable**. (Remark that in some textbooks a polynomial over F is called separable if all its irreducible factors have no multiple roots.)

The next proposition shows that the separability of $f(x)$ can be determined by the Euclidean Algorithm in the field where the coefficients of $f(x)$ lie, without passing to a splitting field and factoring $f(x)$.

Proposition ([1] §13.5 Proposition 33)**.** *Define the **(formal) derivative** of a polynomial $f(x) = \sum_{k=0}^{n} a_k x^k \in F[x]$ to be the polynomial*

$$f'(x) = D_x f(x) \coloneqq \sum_{k=1}^{n} k a_k x^{k-1} \in F[x].$$

Then $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$, i.e., $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $GCD(f(x), D_x f(x)) = 1$.

The formal derivative of a polynomial is purely algebraic and so can be applied to a polynomial over an arbitrary field F, where the analytic notion of derivative (involving limits — a *continuous* operation) may not exist.

Exercise ([1] §13.5 Exercise 1)**.** *Show that the formal derivative D_x of a polynomial satisfies*

$$D_x(f(x)+g(x)) = D_x f(x) + D_x g(x) \quad \textit{and} \quad D_x(f(x)g(x)) = D_x f(x) g(x) + f(x) D_x g(x)$$

for any two polynomials $f(x)$ and $g(x)$. And prove the above proposition.

Example. *The polynomial $x^{p^n} - x$ over $\mathbb{F}_p$ has derivative $p^n x^{p^n-1} - 1 = -1$ since the field has characteristic p. Since in this case the derivative has no roots at all, it follows that the polynomial has no multiple roots, hence is separable.*

Example. *The polynomial $x^n - 1$ has derivative nx^{n-1}. Over any field of characteristic not dividing n (including characteristic 0) this polynomial has only the root 0 (of multiplicity $n-1$), which is not a root of $x^n - 1$. Hence $x^n - 1$ is separable and there are n distinct n^{th} roots of unity. We saw this directly over $\mathbb{Q}$ by exhibiting n distinct solutions over $\mathbb{C}$.*

If F is of characteristic p and p divides n, then there are fewer than n distinct n^{th} roots of unity over F: in this case the derivative is identically 0 since $n = 0$ in F. In fact every root of $x^n - 1$ is multiple in this case. For example, $x^p - 1 = (x-1)^p$ in $\mathbb{F}_p[x]$ (cf. [1] §13.5 Proposition 35).

Corollary ([1] §13.5 Corollary 34)**.** *Every irreducible polynomial over a field of characteristic 0 (for example, $\mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.*

Proof. Suppose F is a field of characteristic 0 and $p(x) \in F[x]$ is irreducible of degree n. Then the derivative $D_x p(x)$ is a polynomial of degree $n-1$. Up to constant factors the only factors of $p(x)$ in $F[x]$ are 1 and $p(x)$, so $D_x p(x)$ must be relatively prime to $p(x)$. This shows that any irreducible polynomial over a field of characteristic 0 is separable.

The second statement of the corollary is then clear since distinct irreducibles never have zeros in common (otherwise they are both divisible by the minimal polynomial of a common zero by [1] §13.2 Proposition 9). □

2.2 Perfect fields

The point in the proof of the corollary that can fail in characteristic p is the statement that the derivative $D_x p(x)$ is of degree $n-1$. In characteristic p the derivative of any power x^{pm} of x^p is identically 0:

$$D_x(x^{pm}) = pmx^{pm-1} = 0,$$

so it is possible for the degree of the derivative to decrease by more than one. If the derivative $D_x p(x)$ of the *irreducible* polynomial $p(x)$ is nonzero, however, then just as before we conclude that $p(x)$ must be separable.

It is clear from the definition of the derivative that if $p(x)$ is a polynomial whose derivative is 0, then every exponent of x in $p(x)$ must be a multiple of the characteristic $p = \operatorname{char} F$ of F:

$$p(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \cdots + a_1 x^p + a_0,$$

i.e., $p(x)$ is a polynomial in x^p, namely $p(x) = p_1(x^p)$ with

$$p_1(x) \coloneqq a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

We recall a simple but important result about raising to the p^{th} power in a field of characteristic p.

Proposition ([1] §13.5 Proposition 35)**.** *Let F be a field of characteristic p. Then for any $a, b \in F$,*

$$1^p = 1, \quad (a+b)^p = a^p + b^p, \quad \textit{and} \quad (ab)^p = a^p b^p.$$

*Put another way, the p^{th}-power map defined by $\mathrm{Frob}_p(a) \coloneqq a^p$ is an injective field homomorphism from F to F, called the **Frobenius endomorphism** of F.*

Corollary ([1] §13.5 Corollary 36)**.** *Suppose that $\mathbb{F}$ is a finite field of characteristic p. Then every element of $\mathbb{F}$ is a p^{th} power in $\mathbb{F}$ (notationally, $\mathbb{F} = \mathbb{F}^p$).*

Proof. The injectivity of the Frobenius endomorphism of $\mathbb{F}$ implies that it is also surjective when $\mathbb{F}$ is finite, which is the statement of the corollary. □

A field K is called **perfect** if it is of characteristic 0, or is of characteristic p and every element of K is a p^{th} power in K, i.e., $K = K^p$.

Proposition ([1] §13.5 Proposition 37)**.** *Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.*

Proof. Suppose that $p(x) \in \mathbb{F}[x]$ is an irreducible polynomial with coefficients in a finite field $\mathbb{F}$. If $p(x)$ were inseparable then we have seen that $p(x) = q(x^p)$ for some polynomial $q(x) \in \mathbb{F}[x]$. Let

$$q(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

By [1] §13.5 Corollary 36, each a_i, $i = 1, 2, \ldots, m$ is a p^{th} power in $\mathbb{F}$, say $a_i = b_i^p$. Then by [1] §13.5 Proposition 35 we have

$$\begin{aligned} p(x) = q(x^p) &= a_m (x^p)^m + a_{m-1}(x^p)^{m-1} + \cdots + a_1 x^p + a_0 \\ &= (b_m x^m)^p + (b_{m-1}x^{m-1})^p + \cdots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0)^p, \end{aligned}$$

which shows that $p(x)$ is the p^{th} power of a polynomial in $\mathbb{F}[x]$, a contradiction to the irreducibility of $p(x)$. □

The notion of separability carries over to the fields generated by the roots of these polynomials. The field K is said to be **separable** (or **separably algebraic**) over F if every element of K is the root of a separable polynomial over F (equivalently, the minimal polynomial over F of every element of K is separable). A field which is not separable is **inseparable**.

We have seen that the issue of separability is straightforward for finite extensions of perfect fields since for these fields the minimal polynomial of an algebraic element is irreducible hence separable.

Corollary ([1] §13.5 Corollary 39)**.** *Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.*

Example (Existence and Uniqueness of Finite Fields)**.** *Let $n > 0$ be any positive integer and consider the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. We have already seen that this polynomial is separable, hence has precisely p^n roots. Let α and β be any two roots of this polynomial, so that $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$. Then $(\alpha\beta)^{p^n} = \alpha\beta$, $(\alpha^{-1})^{p^n} = \alpha^{-1}$ and (by [1] §13.5 Proposition 35) $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Hence* ***the set $\mathbb{F}$ consisting of the p^n distinct roots of $x^{p^n} - x$ over $\mathbb{F}_p$ is closed under addition, multiplication and inverses*** *in its splitting field. It follows that $\mathbb{F}$ is a subfield, hence in fact must be the splitting field. Since the number of elements is p^n, we have $[\mathbb{F} : \mathbb{F}_p] = n$, which shows that there exist finite fields of degree n over $\mathbb{F}_p$ for any $n > 0$.*

Let now $\mathbb{F}$ be any finite field of characteristic p. If $\mathbb{F}$ is of dimension n over its prime subfield $\mathbb{F}_p$, then $\mathbb{F}$ has precisely p^n elements. Since the multiplicative group $\mathbb{F}^\times$ is (in fact cyclic) of order $p^n - 1$, we have $\alpha^{p^n-1} = 1$ for every $\alpha \neq 0$ in $\mathbb{F}$, so that $\alpha^{p^n} = \alpha$ for every $\alpha \in \mathbb{F}$. But this means α is a root of $x^{p^n} - x$, hence $\mathbb{F}$ is contained in a splitting field for this polynomial. Since we have seen that the splitting field has order p^n, this shows that $\mathbb{F}$ ***is a splitting field for $x^{p^n} - x$ over $\mathbb{F}_p$.*** *Since splitting fields are unique up to isomorphism, this proves that* ***finite fields of any order p^n exist and are unique up to isomorphism****. We shall denote the finite field of order p^n by $\mathbb{F}_{p^n}$.*

Note also that since the finite field $\mathbb{F}_{p^n}$ is unique up to isomorphism, the quotients of $\mathbb{F}_p[x]$ by any of the irreducible polynomials of degree n are all isomorphic. If $f_1(x)$ and $f_2(x)$ are irreducible of degree n, then $f_2(x)$ splits completely in the field $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f_1(x))$. If we denote a root of $f_2(x)$ by $\alpha(x)$ (to emphasize that it is a polynomial of degree $< n$ in x in $\mathbb{F}_p[x]/(f_1(x))$), then the isomorphism is given by

$$\mathbb{F}_p[x]/(f_2(x)) \cong \mathbb{F}_p[x]/(f_1(x)) \qquad x \mapsto \alpha(x)$$

(we have mapped a root of $f_2(x)$ in the first field to a root of $f_2(x)$ in the second field). For example, if $f_1(x) = x^4 + x^3 + 1$, $f_2(x) = x^4 + x + 1$ are two of the irreducible quartics over $\mathbb{F}_2$, then a simple computation verifies that

$$\alpha(x) = x^3 + x^2$$

is a root of $f_2(x)$ in $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$. Then we have

$$\mathbb{F}_2[x]/(x^4 + x + 1) \cong \mathbb{F}_2[x]/(x^4 + x^3 + 1) \quad (\cong \mathbb{F}_{16}) \qquad x \mapsto x^3 + x^2.$$

Exercise ([1] §14.3 Exercise 5)**.** *Find two irreducible polynomials of degree 3 over $\mathbb{F}_3$. Directly verify that the quotients of $\mathbb{F}_3[x]$ by these two irreducible polynomials are isomorphic.*

We end this part by introducing an important result of finite separable extension. Recall that, for any finite field $\mathbb{F}$, the multiplicative group $\mathbb{F}^\times$ is cyclic (cf. [1] §9.5 Proposition 18). Assume that α is a generator, then $\mathbb{F} = \mathbb{F}_p(\alpha)$ is a simple extension of its prime field $\mathbb{F}_p$.

Theorem ([1] §14.4 Theorem 25, the Primitive Element Theorem)**.** *If K/F is finite and separable, then K/F is simple, i.e., $K = F(\theta)$ for some $\theta \in K$. In particular, any finite extension of fields of characteristic 0 is simple; any finite field is a simple extension of its prime field.*

2.3 Inseparable polynomials

It is not hard to see that if K is not perfect then there are inseparable irreducible polynomials.

Proposition ([1] §13.5 Proposition 38)**.** *Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ such that $p(x) = p_{sep}(x^{p^k})$.*

Example. *The polynomial $p(x) = x^p - t$ over $F = \mathbb{F}_p(t)$ has derivative 0, hence is not separable. Here $p_{sep}(x) = x - t$.*

The degree of $p_{sep}(x)$ is called the **separable degree** of $p(x)$, denoted $\deg_s p(x)$. The integer p^k in the proposition is called the **inseparable degree** of $p(x)$, denoted $\deg_i p(x)$. Computing degrees in the relation $p(x) = p_{sep}(x^{p^k})$ we see that $\deg p(x) = \deg_s p(x) \deg_i p(x)$.

Proof. We have seen above that if $p(x)$ is an irreducible polynomial which is not separable, then its derivative $D_x p(x)$ is identically 0, so that $p(x) = p_1(x^p)$ for some polynomial $p_1(x)$.

The polynomial $p_1(x)$ may or may not itself be separable. If not, then it too is a polynomial in x^p, $p_1(x) = p_2(x^p)$, so that $p(x)$ is a polynomial in x^{p^2}: $p(x) = p_2(x^{p^2})$. Continuing in this fashion we see that there is a uniquely defined power p^k of p such that $p(x) = p_k(x^{p^k})$ where $p_k(x)$ has nonzero derivative (and $p^k \leq \deg p(x)$; in fact $\deg p(x) = p^k \deg p_k(x)$).

It is clear that $p_k(x)$ is irreducible since any factorization of $p_k(x)$ would, after replacing x by x^{p^k}, immediately imply a factorization of the irreducible $p(x)$. It follows that $p_k(x)$ is separable. □

2.4 Purely inseparable extension

An algebraic extension E/F is called **purely inseparable** if for each $\alpha \in E$ the minimal polynomial $m_{\alpha,F}(x)$ of α over F has only one distinct root.

It is easy to see that the following are equivalent:
(1) E/F is purely inseparable;
(2) if $\alpha \in E$ is separable over F, then $\alpha \in F$;
(3) if $\alpha \in E$, then $\alpha^{p^n} \in F$ for some n (depending on α), and $m_{\alpha,F}(x) = x^{p^n} - \alpha^{p^n}$.

Proposition ([1] §14.9)**.** *Let E/F be an algebraic extension. Then there is a unique field E_{sep} with $F \subseteq E_{sep} \subseteq E$ such that E_{sep} is separable over F and E is purely inseparable over E_{sep}. The field E_{sep} is the set of elements of E which are separable over F.*

The degree of E_{sep}/F is called the **separable degree** of E/F and the degree of E/E_{sep} is called the **inseparable degree** of E/F (often denoted as $[E : F]_s$ and $[E : F]_i$ respectively).

Proposition ([1] §14.9)**.** *If E/F is normal with $[E : F]_s < \infty$, then $E = E_{sep}E_{pi}$, where E_{pi} is a purely inseparable extension of F (E_{pi} consists of all purely inseparable elements of E over F) and $E_{sep} \cap E_{pi} = F$.*

The largest separable algebraic extension of F is called the **separable closure** of F.

3 Galois extensions

3.1 Automorphism groups and fixed fields

Let K be a field. An isomorphism σ of K with itself is called an **automorphism** of K. The collection of automorphisms of K is denoted $\mathrm{Aut}(K)$. If $\sigma \in K$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.

An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to **fix** an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is a subset of K (for example, a subfield), then an automorphism σ is said to **fix** F if it fixes all the elements of F, i.e., $\sigma a = a$ for all $a \in F$.

Note that any field has at least one automorphism, the identity map, denoted by $\mathbf{1}$ and sometimes called the **trivial automorphism**.

The prime field of K is generated by $1 \in K$, and since any automorphism σ takes 1 to 1 (and 0 to 0), i.e., $\sigma(1) = 1$, it follows that $\sigma a = a$ for all a in the prime field. Hence any automorphism of a field K fixes its prime subfield. In particular we see that $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism: $\mathrm{Aut}(\mathbb{Q}) = \{\mathbf{1}\}$ and $\mathrm{Aut}(\mathbb{F}_p) = \{\mathbf{1}\}$.

Let K/F be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collection of automorphisms of K which fix F. Note that if F is the prime subfield of K then $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$ since every automorphism of K automatically fixes F.

The following proposition is extremely useful for determining the automorphisms of algebraic extensions.

Proposition ([1] §14.1 Proposition 2)**.** *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F, i.e., $\mathrm{Aut}(K/F)$ permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.*

Proof. Suppose α satisfies the equation

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

where $a_0, a_1, \ldots, a_{n-1}$ are elements of F. Applying the automorphism σ to the equation (and using the fact that σ is a homomorphism) we obtain

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

By assumption, σ fixes all the elements of F, so $\sigma(a_i) = a_i$, $i = 0, 1, \ldots, n-1$. Hence

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

This precisely shows $\sigma\alpha$ is a root of the same polynomial over F as α. This proves the proposition. □

Example. *Let $K = \mathbb{Q}(\sqrt{D})$ where D is not a square in $\mathbb{Q}$. If $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{D})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$, then $\tau(\sqrt{D}) = \pm\sqrt{D}$ since these are the two roots of the minimal polynomial for $\sqrt{D}$. Since τ fixes $\mathbb{Q}$, this determines τ completely:*

$$\tau(a + b\sqrt{D}) = a \pm b\sqrt{D}.$$

The map $\sqrt{D} \mapsto \sqrt{D}$ is just the identity automorphism $\mathbf{1}$ of $\mathbb{Q}(\sqrt{D})$; the map $\sigma : \sqrt{D} \mapsto -\sqrt{D}$ is the isomorphism $\mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}[x]/(x^2 - D) \cong \mathbb{Q}(-\sqrt{D})$ given by [1] §13.1 Theorem 13.6. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt{D})) = \mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) = \{\mathbf{1}, \sigma\}$ is a cyclic group of order 2 generated by σ.

Example. *Let $K = \mathbb{Q}(\sqrt[3]{2})$. As before, if $\tau \in \mathrm{Aut}(K/\mathbb{Q})$, then τ is completely determined by its action on $\sqrt[3]{2}$ since*

$$\tau(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\tau\sqrt[3]{2} + c(\tau\sqrt[3]{2})^2.$$

Since $\tau\sqrt[3]{2}$ must be a root of $x^3 - 2$ and the other two roots of this equation are not elements of K (recall the splitting field of this polynomial is degree 6 over $\mathbb{Q}$), the only possibility is $\tau\sqrt[3]{2} = \sqrt[3]{2}$ i.e., $\tau = \mathbf{1}$. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathbf{1}\}$ is the trivial group.

In general, if K is generated over F by some collection of elements, then any automorphism $\sigma \in \mathrm{Aut}(K/F)$ is completely determined by what it does to the generators. If K/F is finite then K is finitely generated over F by algebraic elements, so by the above proposition the number of automorphisms of K fixing F is finite. In particular, the automorphisms of a finite extension can be considered as permutations of the roots of a finite number of equations (not every permutation gives rise to an automorphism, however, as the example above illustrates). It was the investigation of permutations of the roots of equations that led Galois to the theory we are describing.

Example. *Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$, where $\omega = \zeta_3 = \frac{1}{2}(-1+\sqrt{-3})$. Any $\varphi \in \mathrm{Aut}(K/\mathbb{Q})$ maps $\sqrt[3]{2}$ to one of $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, and maps ω to ω or $\omega^2 = \frac{1}{2}(-1-\sqrt{-3})$ (since these are the roots of the cyclotomic polynomial $\Phi_3(x) = x^2 + x + 1$). Since φ is completely determined by its action on these two elements, this gives only 6 possibilities and each of these possibilities is actually an automorphism.*

To give these automorphisms explicitly, let σ and τ be the automorphisms defined by

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega \\ \omega & \mapsto & \omega \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ \omega & \mapsto & \omega^2 = -\omega - 1. \end{cases}$$

As before, these can be given explicitly on the elements of $\mathbb{Q}(\sqrt[3]{2}, \omega)$, which are linear combinations of the basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \sqrt[3]{2}\omega, (\sqrt[3]{2})^2\omega\}$. For example,

$$\sigma(\sqrt[3]{2}\omega) = \sigma(\sqrt[3]{2})\sigma(\omega) = \sqrt[3]{2}\omega \cdot \omega = \sqrt[3]{2}\omega^2 = \sqrt[3]{2} \cdot (-1 - \omega) = -\sqrt[3]{2} - \sqrt[3]{2}\omega.$$

The other elements of the automorphism group are as follows. (Exercise: Complete the table.)

Elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega))$	**Images of** ω	ω^2	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\mathbf{1}$	ω	ω^2	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
σ	ω	ω^2	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$
σ^2	ω		$\sqrt[3]{2}\omega^2$		
τ	ω^2	ω	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\tau\sigma$					
$\tau\sigma^2$	ω^2		$\sqrt[3]{2}\omega$		

One can compute that $\sigma^3 = \tau^2 = \mathbf{1}$ and $\sigma\tau = \tau\sigma^2$. Hence

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)) = \langle \sigma, \tau \rangle \cong S_3$$

is the symmetric group on 3 letters. Alternatively (and less computationally), since $G = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)) = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ acts as permutations of the 3 roots of $x^3 - 2$, G is a subgroup of S_3, hence must be S_3 since it is of order 6 (cf. [1] §14.1 Proposition 5). The computations above explicitly identify the automorphisms in G and give an explicit isomorphism of G with S_3.

One can also write the splitting field as $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega)$. Note that not every map taking $\sqrt[3]{2}$ and $\sqrt[3]{2}\omega$ to roots of $x^3 - 2$ gives rise to an automorphism of the field (for example, the map $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega$ clearly cannot be an automorphism since it is evidently not an injection). The point is that there may be (sometimes very subtle) algebraic relations among the generators and these relations must be respected by an automorphism. For example, the quotient of the generators here is ω, which is mapped to 1 and not to a root of the minimal polynomial for ω. Put another way, the quotient of these generators satisfies a quadratic equation and this map does not respect that property.

It is an easy exercise to verify the following properties by definition.

Proposition ([1] §14.1 Propositions 1, 3, 4)**.** *Let K/F be an extension of fields. Then*

- $\mathrm{Aut}(K)$ *is a group under composition and* $\mathrm{Aut}(K/F)$ *is a subgroup.*
- *Let $H \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K, and $\mathrm{Inv}(H)$ be the collection of elements of K fixed by all the elements of H:*

$$\mathrm{Inv}(H) \coloneqq \{\alpha \in K \mid \sigma\alpha = \alpha \quad \textit{for any } \sigma \in H\}.$$

Then $\mathrm{Inv}(H)$ is a subfield of K, called the ***fixed field*** *of H.*

The association of groups to fields and fields to groups defined above is inclusion reversing, namely

- *if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\mathrm{Aut}(K/F_1) \geq \mathrm{Aut}(K/F_2)$; and*
- *if $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ are two subgroups of automorphisms, then $\mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2)$.*

Given a subfield F of K, the associated group is the collection of automorphisms of K which fix F. Given a group of automorphisms of K, the associated extension is defined by taking F to be the fixed field of the automorphisms.

Example. *It is obvious that, for $\mathbf{1} \in \mathrm{Aut}(K/F)$, $\mathrm{Inv}(\{\mathbf{1}\}) = K$; but the fixed field $\mathrm{Inv}(\mathrm{Aut}(K/F))$ of the whole group may not be F. For example,*

$$\mathrm{Inv}(\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) = \mathbb{Q}, \quad \textit{but} \quad \mathrm{Inv}(\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

There is a "duality" between the subfields of $\mathbb{Q}(\sqrt{2})$ and the subgroups of $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$:

$$\left\{ \begin{array}{ll} \textit{subfields } F \subseteq \mathbb{Q}(\sqrt{2}) & \mathbb{Q}(\sqrt{2}) \\ & | \\ & \mathbb{Q} \end{array} \right\} \underset{\mathrm{Inv}(\cdot)}{\overset{\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\cdot)}{\rightleftarrows}} \left\{ \begin{array}{ll} \textit{subgroups } H \leq \mathrm{Aut}(\mathbb{Q}(\sqrt{2})) & \{\mathbf{1}\} \\ & | \\ & \{\mathbf{1}, \sigma\} \end{array} \right\}.$$

But there are "not enough" automorphisms in $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ to force the fixed field to be $\mathbb{Q}$ rather than the full $\mathbb{Q}(\sqrt[3]{2})$. This in turn seems to be due to the fact that the other roots of $x^3 - 2$, which are the only possible images of $\sqrt[3]{2}$ under an automorphism, are not elements of $\mathbb{Q}(\sqrt[3]{2})$. (Although even if they were we would need to check that the additional maps we could define were automorphisms.)

*In the next section we make precise the notion of fields with "enough" automorphisms (leading to the definition of a **Galois** extension). As one might suspect even from these two examples (and we prove in the next lecture) these are related to splitting fields.*

Example. *We can determine the fixed fields for any of the subgroups of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \langle \sigma, \tau \rangle$. For example, consider the fixed field of the subgroup $\{1, \sigma, \sigma^2\}$ generated by σ. These are just the elements fixed by σ, since if an element is fixed by σ then it is also fixed by σ^2. (In general, the fixed field of some subgroup is the field fixed by a set of generators for the subgroup.)*

Recall that $\sigma : \left\{ \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega \\ \omega & \mapsto & \omega \end{array} \right.$ can be given explicitly on the elements of $\mathbb{Q}(\sqrt[3]{2}, \omega)$, which are linear combinations of the basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \sqrt[3]{2}\omega, (\sqrt[3]{2})^2\omega\}$. Explicitly,

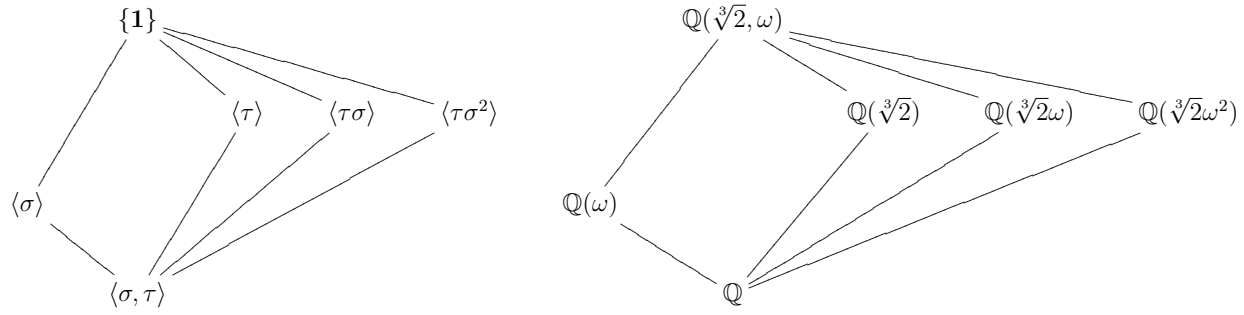
$$\begin{aligned} &\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega) \\ &\qquad = a - e\sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\omega + (b - e)\sqrt[3]{2}\omega - c\sqrt[3]{4}\omega. \end{aligned}$$

The elements fixed by σ are those with

$$a = a, \quad b = -e, \quad c = f - c, \quad d = d, \quad e = b - e, \quad f = -c,$$

which is equivalent to $b = c = f = e = 0$. Hence the fixed field of $\{1, \sigma, \sigma^2\}$ is the field $\mathbb{Q}(\omega)$.

There is a strong similarity between the diagram of subgroups of $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ and the diagram of known subfields for the splitting field of $x^3 - 2$:



where the subfields in the second diagram are precisely the fixed fields of the subgroups in the first diagram.

Exercise ([1] §14.1 p.563-564, §14.2 p.567-568)**.** *Compute* $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ *and the fixed fields of all its subgroups. Compare the diagram of subgroups of* $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ *and the diagram of known subfields for* $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Exercise ([1] §14.2 p.577-581)**.** *Compute the Galois group of the splitting field of* x^8-2 *over* $\mathbb{Q}$ *and the fixed fields of all its subgroups. Compare the diagram of subgroups and that of subfields.*

3.2 Galois extensions

An extension E/F is called **Galois** if it is algebraic, normal and separable. In this case $\mathrm{Aut}(E/F)$ is called the **Galois group** of the extension and is denoted by $\mathrm{Gal}(E/F)$.

Proposition ([1] §14.2 Corollary 10 & Theorem 13)**.** *Let* K/F *be a finite extension. Then*

$$|\mathrm{Aut}(K/F)| \leq [K:F],$$

with equality if and only if K *is Galois over* F*, i.e.,* K *is the splitting field over* F *of a separable polynomial* $f(x)$.

Example. *The extension* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *is Galois with Galois group* $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathbf{1},\sigma\} \cong \mathbb{Z}/2\mathbb{Z}$*, where* σ *is the automorphism* $a+b\sqrt{2} \mapsto a-b\sqrt{2}$*. More generally, any quadratic extension* K *of any field* F *of characteristic different from* 2 *is Galois.*

Example. *The extension* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *is not Galois since it is not normal. Its group of automorphlsms is only of order* 1.

The extension $\mathbb{Q}(\sqrt[3]{2},\omega)$ *is Galois over* $\mathbb{Q}$ *since it is the splitting field of the polynomial* x^3-2*. We have seen that* $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) \cong S_3$ *is of order* $6 = [\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}]$.

Example. *The field* $\mathbb{Q}(\sqrt[4]{2})$ *is not Galois over* $\mathbb{Q}$ *since any automorphism is determined by where it sends* $\sqrt[4]{2}$ *and of the four possibilities* $\{\pm\sqrt[4]{2},\pm\sqrt[4]{2}\}$*, only two are elements of the field (the two real roots). But* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *and* $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ *are both Galois extensions since both are quadratic extensions. This shows that* ***a Galois extension of a Galois extension is not necessarily Galois****.*

Exercise ([1] §14.1 p.566)**.** *We already know the extension of finite fields* $\mathbb{F}_{p^n}/\mathbb{F}_p$ *is Galois since* $\mathbb{F}_{p^n}$ *is the splitting field over* $\mathbb{F}_p$ *of separable polynomial* $x^{p^n}-x$*. Show that* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *is a cyclic group of order* n*, with the Frobenius automorphism* Frob_p *as generator.*

Exercise ([1] §14.1 p.566)**.** *We already know* $\mathbb{F}_p(\sqrt[p]{t}) := \mathbb{F}_p(t)[x]/(x^p-t)$ *is an inseparable extension over* $\mathbb{F}_p(t)$*. Calculate* $\mathrm{Aut}(\mathbb{F}_p(\sqrt[p]{t})/\mathbb{F}_p(t))$.

Other related exercises in [1]

§13.4 2 3 4
§13.5 4 5 6 8 9 11
§14.1 5 6 7 8 9 10

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.