Galois structures

Tomasz Maszczyk

Notes by
Paweł Witkowski

January 2008

Contents

Chapter 1

Galois theory

Galois theory is a language to speak about various phenomena in algebra, arithmetic and geometry. It helps to deal with the problems of solving polynomial equations and possibility of geometric constructions.

1.1 Fields

Definition 1.1. A *field* $\mathbb{F}$ is an abelian group (addition) such that the set $\mathbb{F}^* = \{x \in \mathbb{F} \mid x \neq 0\}$ is equipped with a structure of an abelian group (multiplication) which distributes over addition.

Definition 1.2. A **field** $\mathbb{F}$ is a commutative ring without nontrivial ideals.

Definition 1.3. A **field** $\mathbb{F}$ is a commutative division ring.

Examples 1.4.

1. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $\mathbb{Q}(\sqrt{D})$, where D is not a perfect square, that is the equation $x^2 = D$ has no rational solutions. In another words $\mathbb{Q}(\sqrt{D})$ is the smallest field containing $\mathbb{Q}$ and $\sqrt{D} \in \mathbb{R}, \mathbb{C}$. All even powers of $\sqrt{D}$ belong to $\mathbb{Q}$, and all odd powers of $\sqrt{D}$ are nontrivial multiples of $\sqrt{D}$. Thus for every polynomial $f \in \mathbb{Q}[X]$ we have $f(\sqrt{D}) = a + b\sqrt{D}$, where $a, b \in \mathbb{Q}$. The inverse of an element $a + b\sqrt{D}$, $a, b \in \mathbb{Q}$ is given by
$$\frac{1}{a + b\sqrt{D}} = \frac{a}{a^2 - b^2 D} - \frac{b}{a^2 - b^2 D}\sqrt{D},$$
so in fact for every rational function $f \in \mathbb{Q}(X)$ we have $f(\sqrt{D}) = a + b\sqrt{D}$, where $a, b \in \mathbb{Q}$.
3. Rational functions in one variable $\mathbb{Q}(X)$, and in n variables $\mathbb{Q}(X_1, \ldots, X_n)$.
4. $\mathbb{F}_p$ - classes of integers modulo prime p. There exist also a field $\mathbb{F}_{p^n}$ for every $n > 0$, of p^n elements, unique up to isomorphism and all finite fields are of this form.

1.2 Morphisms of fields

Definition 1.5. A *morphism of fields* $\phi\colon \mathbb{F} \to \mathbb{F}'$ is a homomorphism of rings.

Morphism of fields $\phi\colon \mathbb{F} \to \mathbb{F}'$ is always injective, because

$$1_{\mathbb{F}'} = \phi(1_{\mathbb{F}}) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = \phi(x)\phi(x)^{-1},$$

so $\phi(x) \neq 0$ for every $x \in \mathbb{F}$.

There is always a ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{F}$. We have two cases

1. ϕ is injective: then $\phi(\mathbb{Z}) \subset \mathbb{F}$ generates a subfield isomorphic to $\mathbb{Q}$, and we say that $\mathbb{F}$ has characteristic 0, $\mathrm{char}(\mathbb{F}) = 0$.

2. ϕ is not injective: then there exists the smallest positive integer $p > 0$ such that $\phi(p) = 0$. It is a prime number, because if $p = ab$, $1 < a, b < p$ then we would have

$$0 = \phi(p) = \phi(a)\phi(b) \neq 0.$$

   In this case $\phi(\mathbb{Z}) \subset \mathbb{F}$ generates a subfield isomorphic to $\mathbb{F}_p$, and we say that $\mathbb{F}$ has characteristic p, $\mathrm{char}(\mathbb{F}) = p$.

Definition 1.6. A field $\mathbb{E}$ is an *extension* of the field $\mathbb{F}$ if $\mathbb{F}$ is a subfield of $\mathbb{E}$.

We write $\mathbb{E}/\mathbb{F}$ or draw

$$\begin{array}{c} \mathbb{E} \\ | \\ \mathbb{F} \end{array}$$

Corollary 1.7. *If $\mathbb{E}$ is an extension of $\mathbb{F}$ then*

- $\mathrm{char}(\mathbb{E}) = \mathrm{char}(\mathbb{F})$,
- $\mathbb{E}$ *is a vector space over* $\mathbb{F}$*.*

Definition 1.8.

1. The *degree* $[\mathbb{E} : \mathbb{F}]$ of an extension $\mathbb{E}/\mathbb{F}$ is defined as $\dim_{\mathbb{F}}(\mathbb{E})$.

2. $\mathbb{E}$ is a *finite extension* of $\mathbb{F}$ if $[\mathbb{E} : \mathbb{F}] < \infty$.

Examples 1.9. 1. $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$ with $\{1, \sqrt{D}\}$ as basis over $\mathbb{Q}$.

2. $[\mathbb{C} : \mathbb{R}] = 2$ with $\{1, i\}$ as basis over $\mathbb{R}$.

3. $[\mathbb{Q}(x) : \mathbb{Q}] = \infty$ with $\{1, x, x^2, \ldots\}$ being an infinite linearly independent system.

4. $[\mathbb{R} : \mathbb{Q}] = \infty$ with $\{1, e, e^2, \ldots\}$ being an infinite linearly independent system, where $e \approx 2.72\ldots$ is the Euler number.

Linear dependence of powers of $e \in \mathbb{E}$ over $\mathbb{F} \subset \mathbb{E}$ is nothing else but a polynomial equation

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0.$$

Note that in the first two examples the degree is equal to the minimal degree of a polynomial equation satisfied by the adjoint element

$$\sqrt{D}: \quad x^2 - D = 0, \qquad i: \quad x^2 + 1 = 0.$$

1.3 Polynomials

Denote by $\mathbb{F}[X]$ the ring of polynomials in one variable X. It is an *integral domain*, that is if $f(X), g(X) \in \mathbb{F}[X]$ are nonzero polynomials, then $f(X)g(X) \neq 0$. It is also a *Euclidean domain*, that is for all $f(X), g(X) \in \mathbb{F}[X]$ there are unique polynomials $q(X), r(X) \in \mathbb{F}[X]$ such that

$$f(X) = g(X)q(X) + r(X),$$

where either $r(X) = 0$ or $\deg(r(X)) < \deg(g(X))$.

Corollary 1.10. *For any two nonzero polynomials $f(X), g(X) \in \mathbb{F}[X]$ there is their greatest common divisor*

$$\gcd(f(X), g(X)) = a(X)f(X) + b(X)g(X).$$

Corollary 1.11. *Every ideal in $\mathbb{F}[X]$ is principal, that is of the form $(f(X))$.*

Corollary 1.12. *Every nonconstant polynomial $f(X) \in \mathbb{F}[X]$ can be factored as*

$$f(X) = uf_1(X) \dots f_k(X),$$

where $f_i(X)$ are monic, irreducible, and $u \in \mathbb{F}^*$. This factorisation is essentially unique.

There is an important construction of field extensions from irreducible polynomials.

Proposition 1.13. *Let $f(X) \in \mathbb{F}[X]$ be an irreducible of degree d. Then*

$$\mathbb{E} := \mathbb{F}[X]/(f(X))$$

is an extension of degree d.

Proof. First we prove that the classes of $1, x, x^2, \dots, x^{d-1}$ form a basis of $\mathbb{E}$ over $\mathbb{F}$. Every polynomial $g(X) \in \mathbb{F}[X]$ can be presented as

$$g(X) = f(X)q(X) + r(X),$$

where $r(X) = 0$ or $\deg(r(X)) < d$. Thus $g(X)$ is a combination of $1, x, \dots, x^{d-1}$, and classes of $1, x, \dots, x^{d-1}$ generate $\mathbb{E}$.

Every linear combination of classes of $1, x, \dots, x^{d-1}$ is a polynomial of degree less than $d = \deg(f(X))$, so classes of $1, x, \dots, x^{d-1}$ are linearly independent. Observe that $\mathbb{E}$ is an integral domain - it is a consequence of the unique factorisation property for $\mathbb{F}[X]$ and an assumption that f is irreducible.

The proof will be finished if we prove the following lemma

Lemma 1.14. *Every finite dimensional commutative $\mathbb{F}$-algebra $\mathbb{E}$ which is an integral domain is a field.*

Proof. Take $e \in \mathbb{E}^*$. There exists a linear dependence among elements $1, e, e^2, \dots$ since $\mathbb{E}$ is of finite dimension over $\mathbb{F}$. We can divide by the monomial of the lowest degree to obtain

$$1 + f_1 e + f_2 e^2 + \dots + f_n e^n = 0,$$
$$e(-f_1 - f_2 e - \dots - f_n e^{n-1}) = 1,$$

so e has an inverse. $\square$

$\square$

Corollary 1.15 (Kronecker)**.** *Let $f(X) \in \mathbb{F}[X]$ be any nonconstant polynomial. Then there exists an extension $\mathbb{E}/\mathbb{F}$ in which $f(X)$ has a root.*

Proof. We can assume that $f(X)$ is irreducible. Then take

$$\mathbb{E} = \mathbb{F}[X]/(f(X))$$

The root of $f(X)$ in $\mathbb{E}$ is the class of $X \in \mathbb{F}[X]$. □

Definition 1.16. Let $e \in \mathbb{E}$ be algebraic over $\mathbb{F}$. Then the monic irreducible polynomial $f_e(X) \in \mathbb{F}[X]$ such that $f_e(e) = 0$ is determined uniquely (as the monic generator of the ideal $\{f(X) \in \mathbb{F}[X] \mid f(e) = 0\}$) and is called the *minimal polynomial* of e.

Lemma 1.17. *Let $e \in \mathbb{F}$ be algebraic over $\mathbb{F}$. Then the canonical map*

$$\varphi \colon \mathbb{F}[X]/(f_e(X)) \to \mathbb{F}(e) \subset \mathbb{E}, \quad x \mapsto e$$

is an isomorphism.

Proof. Because $f_e(e) = 0$ the map φ is well defined. It is enough to prove that

$$\dim_{\mathbb{F}} \left(\mathbb{F}[X]/(f_e(X))\right) = \dim_{\mathbb{F}} \left(\mathbb{F}(e)\right)$$

By definition

$$\dim_{\mathbb{F}} \left(\mathbb{F}[X]/(f_e(X))\right) = \deg(f_e(X)).$$

Also

$$\dim_{\mathbb{F}} \left(\mathbb{F}(e)\right) = \deg(f_e(X)),$$

because $f_e(x)$ is a monic polynomial of lowest degree vanishing at e. □

1.4 Automorphisms of fields

If $G \subset \mathrm{Aut}(\mathbb{E})$ is a subgroup then $\mathbb{E}^G \subset \mathbb{E}$ is a subfield.

Definition 1.18. Let $G = \{g_1, \ldots, g_n\} \subset \mathrm{Aut}(\mathbb{E})$. We define a *trace*

$$\mathrm{Tr}_G \colon \mathbb{E} \to \mathbb{E}^G, \quad \mathrm{Tr}_G(e) = \sum_{g \in G} g(e).$$

Trace Tr_G is an $\mathbb{E}^G$-linear map.

Theorem 1.19 (Dedekind)**.** *If $g_1, \ldots, g_n$ are pairwise distinct automorphisms of $\mathbb{E}$, they are linearly independent over $\mathbb{E}$ as $\mathbb{E}$-valued functions on $\mathbb{E}$.*

Proof. Induction by n. If $n = 1$ then $g_1 \neq 0$ since it is an automorphism.

Take pairwise distinct automorphisms $g_1, \ldots, g_{n+1}$. If they were linearly dependent then for instance

$$g_{n+1} = e_1 g_1 + \ldots + e_n g_n$$

with at least one $e_i \neq 0$. We would have

$$g_{n+1}(e)(e_1 g_1(e') + \ldots + e_n g_n(e')) = g_{n+1}(e) g_{n+1}(e') = g_{n+1}(ee') =$$

$$= e_1 g_1(ee') + \ldots + e_n g_n(ee') = e_1 g_1(e) g_1(e') + \ldots + e_n g_n(e) g_n(e').$$

Hence

$$e_1 g_{n+1}(e) g_1 + \ldots + e_n g_{n+1}(e) g_n = e_1 g_1(e) g_1 + \ldots e_n g_n(e) g_n.$$

But $g_1, \ldots, g_n$ are linearly independent so

$$g_{n+1}(e) e_1 = e_1 g_1(e), \ldots, g_{n+1}(e) e_n = e_n g_n(e),$$

$$g_1 e_1 = g_{n+1} e_1, \ldots, g_n e_n = g_{n+1} e_n$$

which means that for at least one i we would have $g_i = g_{n+1}$, contradiction. ☐

Corollary 1.20. *If $|G| < \infty$ then $\mathrm{Tr}_G \neq 0$.*

Proof. If $\mathrm{Tr}_G = 0$, that is $\mathrm{Tr}_G(e) = 0$ for all $e \in \mathbb{E}$ then by definition

$$\sum_{g \in G} g(e) = \left(\sum_{g \in G} g \right)(e) = 0$$

that is $\sum_{g \in G} g = 0$, which contradicts linear independence. ☐

Theorem 1.21. *Let G be a group of automorphisms of $\mathbb{E}$. Assume that at least one of numbers $|G|$, $[\mathbb{E} : \mathbb{E}^G]$ is finite. Then they are equal.*

Proof.

1. Assume $|G| < \infty$, $G = \{g_1, \ldots, g_n\}$. Take $e_1, \ldots, e_m \in \mathbb{E}$, where $m > n$. Let $(e'_1, \ldots, e'_m)$ be a nonzero solution of the system

   $$\sum_{j=1}^{n} g_i^{-1}(e_j) e'_j = 0.$$

   We can assume that $\mathrm{Tr}_G(e'_1) \neq 0$. Then

   $$\underbrace{\sum_{i=1}^{n} \sum_{j=1}^{m} e_j g_i(e'_j)}_{= \sum_{j=1}^{n} e_j \mathrm{Tr}_G(e'_j)} = \sum_{i=1}^{n} g_i \left(\sum_{j=1}^{m} g_i^{-1}(e_j) e'_j \right) = 0,$$

   so $e_1, \ldots, e_m$ are linearly dependent over $\mathbb{E}^G$ if $m > n$ which means that $[\mathbb{E} : \mathbb{E}^G] \leq n = |G|$.

2. Assume $[\mathbb{E} : \mathbb{E}^G] < \infty$. Take a basis $e_1, \ldots, e_N$ of $\mathbb{E}$ over $\mathbb{E}^G$. Let $(e'_1, \ldots, e'_M)$, $N < M \leq G$ be a nonzero solution of the system of equations

   $$\sum_{j=1}^{M} e'_j g_j(e_i) = 0.$$

   Then for all $e \in \mathbb{E}$

   $$\sum_{j=1}^{M} e'_j g_j(e) = 0,$$

   $$\sum_{j=1}^{M} e'_j g_j = 0$$

   which contradicts Dedekind theorem (1.19). Thus $[\mathbb{E} : \mathbb{E}^G] \geq |G|$.

Together 1 and 2 give $[\mathbb{E} : \mathbb{E}^G] = |G|$. $\square$

Definition 1.22. An algebraic extension $\mathbb{E}/\mathbb{F}$ is called Galois if there exists a subgroup $G \subset \mathrm{Aut}(\mathbb{E})$ such that $\mathbb{F} = \mathbb{E}^G$.

Theorem 1.23. *Let $\mathbb{E}/\mathbb{F}$ be an algebraic extension. Then it is Galois if and only if $\mathbb{F} = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}$.*

Proof. Assume that there exists group G such that $\mathbb{E}^G = \mathbb{F}$. Then

$$\begin{tikzcd} G \subset \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \arrow[r, Rightarrow] & \mathbb{E}^G \arrow[d, equal] & \supset & \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} \arrow[d, equal] \\ & \mathbb{F} & = & \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} \end{tikzcd}$$

so $\mathbb{E}^G = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}$. $\square$

Remark 1.24. This G may not be equal $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

Corollary 1.25. *If $[\mathbb{E} \colon \mathbb{F}]$ is finite then it is Galois if and only if $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$.*

Proof. If $\mathbb{F} = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}$ then

$$|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = |\mathrm{Gal}(\mathbb{E}/\mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})})| = [\mathbb{E} : \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}] = [\mathbb{E} : \mathbb{F}].$$

If $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$ then $\mathbb{F} \subset \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} \subset \mathbb{E}$.

To finish the proof we need the following:

Lemma 1.26. *Assume $\mathbb{F} \subset \mathbb{E} \subset \mathbb{D}$. Then provided finiteness*

$$[\mathbb{D} : \mathbb{E}] = [\mathbb{D} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$$

Proof. Let $\{d_1, \ldots, d_n\}$ be a basis of $\mathbb{E}/\mathbb{F}$. It is enough to show that $\{d_i e_j\}$ is a basis of $\mathbb{D}/\mathbb{F}$. Let

$$d = \sum_i d_i \tilde{e}_i, \quad \tilde{e}_i = \sum_j e_i f_{ij}.$$

Then

$$d = \sum_{i,j} d_i e_j f_{ij},$$

so $\{d_i e_j\}$ span $\mathbb{D}/\mathbb{F}$. If $\sum_{i,j} d_i e_j f_{ij} = 0$ then

$$\sum_i d_i \underbrace{\left(\sum_j e_j f_{ij} \right)}_{\in \mathbb{E}} = 0$$

which gives a contradiction. $\square$

Now

$$[\mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} : \mathbb{F}] = \frac{[\mathbb{E} : \mathbb{F}]}{[\mathbb{E} : \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}]} = 1,$$

so $\mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} = \mathbb{F}$. $\square$

Definition 1.27. A field extension $\mathbb{E}/\mathbb{F}$ is *normal* if $\mathbb{E}$ contains all roots of minimal polynomials of all elements in $\mathbb{F}$ which are algebraic over $\mathbb{F}$.

Lemma 1.28. *Let $\mathbb{E}/\mathbb{F}$ be algebraic i.e. $\mathbb{F} \subset \mathbb{E} \subset \overline{\mathbb{F}}$, and let $\mathbb{E}/\mathbb{F}$ be normal. Then for every embedding over $\mathbb{F}$*

$$\begin{tikzcd} \mathbb{E} \arrow[rr, "\varphi"] & & \overline{\mathbb{F}}, \\ & \mathbb{F} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

one has $\varphi(\mathbb{E}) = \mathbb{E}$.

Proof. Take $e \in \mathbb{E}$, $f(e) = 0$, so $f(\varphi(e)) = 0$. Hence φ maps the set of roots of every $f(X) \in \mathbb{F}[X]$ in $\mathbb{E}$ into the set of all roots of $f(X)$. Thus $\mathbb{E} = \mathbb{F}(\text{roots}(\text{family of polynomials}))$. The homomorphism φ transforms roots of this family into the roots of its image.

$$\begin{aligned} \varphi(\mathbb{E}) &= \varphi(\mathbb{F}(\text{roots}(\text{family of polynomials}))) \\ &= \mathbb{F}(\varphi(\text{roots}(\text{family of polynomials}))) \\ &= \mathbb{F}(\text{roots}(\text{family of polynomials})) \\ &= \mathbb{E}. \end{aligned}$$

$\square$

Definition 1.29. A field extension $\mathbb{E}/\mathbb{F}$ is *separable* if every $e \in \mathbb{F}$ is a single root of its minimal polynomial.

Definition 1.30. An extension $\mathbb{E}/\mathbb{F}$ is a *splitting field* of $f(X) \in \mathbb{F}[X]$ if

$$f(X) = c(X - e_1)\dots(X - e_n) \in \mathbb{E}[X]$$

and such decomposition is impossible in $\mathbb{F}'[X]$ for any proper subfield $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{E}$.

All splitting fields of a given polynomial are isomorphic over $\mathbb{F}$.

1.5 Extending isomorphisms

Lemma 1.31. *Let $\sigma_0 \colon \mathbb{F}_1 \to \mathbb{F}_2$ be an isomorphism of fields. Let $f_1(X) \in \mathbb{F}_1[X]$ be irreducible and $\mathbb{E}_1 = \mathbb{F}_1(e_1)$, where $f_1(e_1) = 0$. Let $\mathbb{E}_2 = \mathbb{F}_2(e_2)$, where $f_2(e_2) = 0$ for $f_2(X) = \sigma_0(f_1(X))$. Then σ_0 extends to a unique isomorphism $\sigma \colon \mathbb{E}_1 \to \mathbb{E}_2$ with $\sigma(e_1) = e_2$.*

Proof. Extend σ_0 to $\sigma_0 \colon \mathbb{F}_1[X] \to \mathbb{F}_2[X]$. The polynomial $f_1(X)$ is irreducible if and only if $f_2(X)$ is irreducible. By the Kronecker theorem (1.15)

$$\mathbb{F}_i[X]/(f_i)(X) \cong \mathbb{F}_i(e_i) = E_i, \quad i = 1, 2.$$

$\square$

Lemma 1.32. *Let $\sigma_0 \colon \mathbb{F}_1 \to \mathbb{F}_2$ be an isomorphism. Let $f_1(X) \in \mathbb{F}_1[X]$ and $f_2(X) = \sigma_0(f_1(X)) \in \mathbb{F}_2[X]$. Let $\mathbb{E}_i$ be splitting field of $f_i(X)$. Then σ_0 extends to an isomorphism of $\sigma \colon \mathbb{E}_1 \to \mathbb{E}_2$.*

Proof. Factor $f_1(X)$ into k irreducibles in $\mathbb{F}_1[X]$ and consider $d := \deg(f_1(X)) - k$. The proof goes by induction on d. If $d = 0$, then $f_1(X)$ is a product of linear factors, $\mathbb{E}_1 = \mathbb{F}_1$, $\mathbb{E}_2 = \mathbb{F}_2$, and $\sigma = \sigma_0$.

Suppose $d > 0$. Then $f_1(X)$ has an irreducible factor of degree > 1. Take a root $e_1 \in \mathbb{E}_1$ of $g_1(X) \in \mathbb{F}_1[X]$, and a root $e_2 \in \mathbb{E}_2$ of $\sigma_0(g_1(X)) \in \mathbb{F}_2[X]$. Then $\mathbb{F}_i(e_i) \in \mathbb{E}_i$, $i = 1, 2$, and by the previous lemma (1.31) there is an isomorphism

$$\tilde{\sigma}_0 \colon \mathbb{F}_1(e_1) \to \mathbb{F}_2(e_2)$$

with $\tilde{\sigma}_0\big|_{\mathbb{F}_1} = \sigma_0$ and $\tilde{\sigma}_0(e_1) = e_2$. Take now $\tilde{\mathbb{F}}_1 := \mathbb{F}_1(e_1)$ instead of $\mathbb{F}_1$. Consider $\tilde{f}_i(X) = f_i(X) \in \tilde{\mathbb{F}}_i[X]$. Now $g_1(X) \in \mathbb{F}_1[X]$ has a linear factor $(X - e_1)$. Thus $\tilde{f}_1(X)$ has $\tilde{k} > k$ irreducible factors in $\tilde{\mathbb{F}}_1[X]$. Thus $\tilde{d} = \deg \tilde{f}_1(X) - \tilde{k} < d$. Now $\mathbb{E}_i$ is still a splitting field of a polynomial $\tilde{f}_i(X) \in \tilde{\mathbb{F}}_i[X]$, so $\tilde{\sigma}_0$ extends to some $\sigma \colon \mathbb{E}_1 \cong \mathbb{E}_2$. ☐

Theorem 1.33. *An algebraic extension $\mathbb{E}/\mathbb{F}$ is Galois if and only if it is normal and separable.*

Proof.

- Assume that $\mathbb{E}/\mathbb{F}$ is Galois, that is there exists group $G < \mathrm{Aut}(\mathbb{E})$ such that $\mathbb{F} = \mathbb{E}^G$. It is enough to prove that the minimal polynomial $f_e(X) \in \mathbb{F}[X]$ of any $e \in \mathbb{E}$ splits into pairwise distinct linear factors in $\mathbb{E}[X]$.

  Because $f_e(e) = 0$ we have for all $g \in G$ that $f_e(g(e)) = gf_e(e) = 0$, so $|Ge| < \infty$ as the number of roots is finite. Say $Ge = \{g_1(e), \ldots, g_r(e)\}$. Define $f(X) := (X - g_1(e)) \ldots (X - g_r(e))$. For all $g \in G$ we have $g(f(X)) = f(X)$, so $f(X) \in \mathbb{F}[X]$. Since all roots of f are pairwise distinct roots of f_e we have that $f | f_e$. But f_e is monic irreducible, so $f = f_e$. This implies that f_e splits as desired.

- Assume now that $\mathbb{E}/\mathbb{F}$ is separable and normal. Take $e \in \mathbb{E} \setminus \mathbb{F}$ and its minimal polynomial $f_e(X)$. In $\mathbb{E}$ $f_e(X)$ splits as $f_e(X) = (X - e_1) \ldots (X - e_r)$. Assume that $e_1 := e \notin \mathbb{F}$, so $\deg(f_e(X)) > 0$. There must be another root $e_2 \neq e_1$ of $f_e(X)$. There is an isomorphism $\mathbb{F}(e_1) \to \mathbb{F}(e_2)$ which is id on $\mathbb{F}$ and sends e_1 to e_2. It extends to $\overline{\mathbb{F}(e_1)} = \overline{\mathbb{F}} \to \overline{\mathbb{F}} = \overline{\mathbb{F}(e_2)}$ (nonconstructive axiom of choice). Since $\mathbb{E}/\mathbb{F}$ is normal this isomorphism restricts to $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ such that $g(e_1) = e_2 \neq e_1$. There are no elements of $\mathbb{E} \setminus \mathbb{F}$ which are fixed by $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, so $\mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})} = \mathbb{F}$ and $\mathbb{E}/\mathbb{F}$ is a Galois extension.

☐

Corollary 1.34. *Extension $\mathbb{E}/\mathbb{F}$ is finite Galois if and only if it is a splitting field of a separable polynomial $f(X) \in \mathbb{F}[X]$.*

Proof. We know that $\mathbb{E}/\mathbb{F}$ is finite Galois if and only if it is finite, normal, and separable. In fact $\mathbb{E}/\mathbb{F}$ is finite and normal if and only if $\mathbb{E}$ is a splitting field of some $f(X) \in \mathbb{F}[X]$. Indeed, if $\mathbb{E}/\mathbb{F}$ is finite and normal, then we can take all roots of a family of polynomials and choose a linearly independent (finite) subset of roots generating $\mathbb{E}/\mathbb{F}$. They are roots of some finite number of polynomials $f_1(X), \ldots, f_n(X) \in \mathbb{F}[X]$. Then $\mathbb{E}$ is a splitting field of $f(X) = f_1(X) \cdot \ldots \cdot f_n(X)$. The reverse implication is obvious from the definition of normality. Finally $\mathbb{E}/\mathbb{F}$ is separable if and only if $f(X) = f_1(X) \cdot \ldots \cdot f_n(X)$ is separable. ☐

1.6 The fundamental theorem of Galois theory

Theorem 1.35. *Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension, $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Then*

1. *There is a one-to-one correspondence between intermediate fields $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{E}$ and subgroups $G \supset G' \supset \{1\}$ given by*
$$\mathbb{F}' := \mathbb{E}^{G'}$$
2. *Extension $\mathbb{F}'/\mathbb{F}$ is normal if and only if G' is a normal subgroup of G. This is the case if and only if $\mathbb{F}'/\mathbb{F}$ is Galois. In this case $\mathrm{Gal}(\mathbb{F}'/\mathbb{F}) \cong G/G'$.*
3. *For each $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{E}$*
$$[\mathbb{F}' : \mathbb{F}] = [G : G']$$
$$[\mathbb{E} : \mathbb{F}'] = |G'|$$

Remark 1.36.

1. If $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{F}'' \subset \mathbb{E}$ then $G' \supset G''$.
2. Extension $\mathbb{E}/\mathbb{F}'$ is always Galois with $\mathrm{Gal}(\mathbb{E}/\mathbb{F}') = G'$.
3. If an extension $\mathbb{E}/\mathbb{F}$ is separable then $\mathbb{F}'/\mathbb{F}$ is separable. Thus $\mathbb{F}'/\mathbb{F}$ is normal if and only if it is Galois.
4. From the proof we will get that if $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$, then $G/G' = \mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ in the case $\mathbb{F}'/\mathbb{F}$ is Galois.

Proof.

1. Define a map
$$\phi\colon \{\text{subgroups of } G\} \to \{\text{intermediate fields}\}$$
$$G' \mapsto \mathbb{E}^{G'}$$

- ϕ is injective: $G' \neq G'' \implies \mathbb{E}^{G'} \neq \mathbb{E}^{G''}$

  Lemma 1.37. $\mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'}) = G'$.

  Proof. $\mathbb{E}^{G'} = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'})}$ because $\mathbb{E}/\mathbb{E}^{G'}$ is Galois. Furthermore
$$|G'| = [\mathbb{E} : \mathbb{E}^{G'}] = [\mathbb{E} : \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'})}] = |\,\mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'})|$$
  and $G' \subset \mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'})$, so $G' = \mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'})$. □

  By lemma if $\mathbb{E}^{G'} \subset \mathbb{E}^{G''}$ then $G'' = \mathrm{Gal}(\mathbb{E}/\mathbb{E}^{G'}) \subset G'$. Hence if $\mathbb{E}^{G'} = \mathbb{E}^{G''}$ then $G' = G''$.

- ϕ is surjective. Indeed, let $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{E}$, $G' = \mathrm{Gal}(\mathbb{E}/\mathbb{F}') \subset \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$. If $\mathbb{E}/\mathbb{F}$ is Galois then $\mathbb{E}$ is a splitting field of a separable polynomial with coefficients in $\mathbb{F}$, $f(X) \in \mathbb{F}[X] \subset \mathbb{F}'[X]$. Thus $\mathbb{E}$ is a splitting field of $f(X) \in \mathbb{F}'[X]$, so $\mathbb{E}/\mathbb{F}'$ is Galois and $\mathbb{F}' = \mathbb{E}^{G'}$.

2. Suppose $G' \triangleleft G$, $\mathbb{F}' := \mathbb{E}^{G'}$. Then $\mathbb{E}/\mathbb{F}'$ is a Galois extension. Take $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Then $g(\mathbb{F}') = \mathbb{E}^{gGg^{-1}} = \mathbb{E}^{G'} = \mathbb{F}'$. This gives the restriction map

$$\begin{aligned} \mathrm{Res}\colon\ \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G &\to \mathrm{Gal}(\mathbb{F}'/\mathbb{F}) \\ g &\mapsto g|_{\mathbb{F}'} \\ \ker(\mathrm{Res}) &= \mathrm{Gal}(\mathbb{E}/\mathbb{F}') = G \\ \mathrm{im}(\mathrm{Res}) &= G/G' \end{aligned}$$

   We want to prove that Res is onto. Let $\tilde{g} \in \mathrm{Gal}(\mathbb{F}'/\mathbb{F})$. We know that $\mathbb{E}$ is a splitting field of some polynomial $f(X) \in \mathbb{F}'[X]$, so $\tilde{g}\colon \mathbb{F}' \to \mathbb{F}'$ extends to $g\colon \mathbb{E} \xrightarrow{\simeq} \mathbb{E}$, $g|_{\mathbb{F}} = \mathrm{id}$. Thus $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $g|_{\mathbb{F}'} = \tilde{g}$ and Res is onto. Hence $\mathrm{Gal}(\mathbb{F}'/\mathbb{F}) \simeq G/G'$.

   Suppose the converse, that is $\mathbb{F}'/\mathbb{F}$ is Galois. Then $\mathbb{F}'$ is a splitting field of some separable polynomial $f(X) \in \mathbb{F}[X]$ with roots (distinct by separability) $e_1, \dots, e_n \in \mathbb{F}' \subset \mathbb{E}$ and $\mathbb{F}' = \mathbb{F}(e_1, \dots, e_n) \subset \mathbb{E}$. Take $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$. We have $g(f(X)) = f(X)$, so g permutes the set of roots $\{e_1, \dots, e_n\}$. Hence $\mathbb{E}^{G'} = \mathbb{F}' = g(\mathbb{F}') = \mathbb{E}^{gG'g^{-1}}$. By 1, $G' = gG'g^{-1}$, so $G' \triangleleft G$.

3. If $\mathbb{E}/\mathbb{F}'$ is Galois extension, then

$$[\mathbb{E} : \mathbb{F}'] = |\,\mathrm{Gal}(\mathbb{E}/\mathbb{F}')| = |G'|,$$

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}] \cdot [\mathbb{F}' : \mathbb{F}], \quad |G| = |G'| \cdot [G : G'].$$

   Hence $[\mathbb{F}' : \mathbb{F}] = [G : G']$ and $[\mathbb{E} : \mathbb{F}'] = |G'|$.

$\square$

Corollary 1.38. *If*

$$\begin{tikzcd} & \mathbb{F}' \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{F} \arrow[dr, dash] & & \mathbb{E} \arrow[dl, dash] \\ & \mathbb{F}'' & \end{tikzcd}$$

are field extensions, then the following are equivalent

1. $g(\mathbb{F}') = \mathbb{F}''$ *for some* $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$
2. $g\,\mathrm{Gal}(\mathbb{E}/\mathbb{F}')g^{-1} = \mathrm{Gal}(\mathbb{E}/\mathbb{F}'')$

Definition 1.39. An abstract group G acts transitively on a set S if for all elements $s, s' \in S$ there is $g \in G$ such that $s' = g(s)$.

Proposition 1.40. *Let* $\mathbb{E}/\mathbb{F}$ *be finite Galois extension, so* $\mathbb{E}$ *is a splitting field of a separable polynomial* $f(X) \in \mathbb{F}[X]$. *Then* $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ *is isomorphic to a subgroup of the permutation group on the roots of* $f(X)$. *If* $f(X)$ *is irreducible then this action is transitive.*

Proof. Take the set of roots of $f(X)$, $S := \{e_1, \dots, e_n\}$. Let $g \in G$ such that $g(f(X)) = f(X)$, so g permutes S. We have $\mathbb{E} = \mathbb{F}(e_1, \dots, e_n)$, and if for all i $g(e_i) = e_i$, then $g = \mathrm{id}$. This means that G embeds in the group of permutations of S.

Take now $e_i \neq e_j$. If $f(X)$ is irreducible then there exists an isomorphism $\sigma_0\colon \mathbb{F}(e_i) \xrightarrow{\simeq} \mathbb{F}(e_j)$, such that $\sigma_0|_{\mathbb{F}} = \mathrm{id}$, $\sigma_0(e_i) = e_j$. Hence σ_0 extends to $g\colon \mathbb{E} \to \mathbb{E}$, $g|_{\mathbb{F}} = \mathrm{id}$, so there exists an element $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ such that $g(e_i) = e_j$. $\square$

1.7 The normal basis theorem

We know that if $\mathbb{E}/\mathbb{F}$ is finite Galois then $[\mathbb{E}:\mathbb{F}] = |\operatorname{Gal}(\mathbb{E}/\mathbb{F})|$.

Definition 1.41. If $\mathbb{E}/\mathbb{F}$ is finite Galois then a basis $\{e_1,\dots,e_n\}$ is called *normal* if there exists $e \in \mathbb{E}$ such that $e_i = g_i(e)$ for $\{g_1,\dots,g_n\} = \operatorname{Gal}(\mathbb{E}/\mathbb{F})$.

Theorem 1.42 (Normal Basis theorem)**.** *If $\mathbb{F}$ is infinite and $\mathbb{E}/\mathbb{F}$ is finite Galois then $\mathbb{E}$ has a normal basis over $\mathbb{F}$.*

The proof uses some additional results.

Lemma 1.43. *If $\mathbb{E}/\mathbb{F}$ is a Galois extension of degree n, $\operatorname{Gal}(\mathbb{E}/\mathbb{F}) = \{g_1,\dots,g_n\}$, then $\{e_1,\dots,e_n\} \subset \mathbb{E}$ is a basis over $\mathbb{F}$ if and only if the matrix $\{g_i(e_j)\}$ is nonsingular.*

Proof. If $\{e_1,\dots,e_n\}$ is a basis of $\mathbb{E}/\mathbb{F}$, then if for some $(c_1,\dots,c_n) \neq 0 \in \mathbb{F}^n$ and all $j = 1,\dots,n$

$$\sum_{i=1}^{n} c_i g_i(e_j) = 0$$

we get that for all $e \in E$

$$\sum_{i=1}^{n} c_i g_i(e) = 0,$$

which contradicts Dedekind theorem (1.19).

On the other hand if $\sum_{j=1}^{n} c_j e_j = 0$ is a nontrivial linear dependence then for all i

$$\sum_{i=1}^{n} c_j g_i(e_j) = 0$$

which means that $\{g_i(e_j)\}$ is singular. □

Lemma 1.44. *Let $\mathbb{F}$ be infinite, $\mathbb{E}/\mathbb{F}$ an extension. If $f(c_1,\dots,c_n) = 0$ for all $(c_1,\dots,c_n) \in \mathbb{F}^n$ and $f(X_1,\dots,X_n) \in \mathbb{E}[X_1,\dots,X_n]$, then $f(X_1,\dots,X_n) = 0$.*

Proof. Induction by n. If $f(e_1) = 0$ for infinitely many e_1, then $f(X_1) = 0$.

Let $n > 1$. Then we can write

$$f(X_1,\dots,X_n) = \sum_{k=0}^{n} f_k(X_1,\dots,X_{n-1}) X_n^k.$$

Take $(c_1,\dots,c_{n-1})$ such that $f(c_1,\dots,c_{n-1},X_n) = 0$. Then for all k we have $f_k(c_1,\dots,c_{n-1}) = 0$, and by the inductive step $f_k(X_1,\dots,X_{n-1}) = 0$, so $f(X_1,\dots,X_n) = 0$. □

The next result we need is a generalization of the Dedekind theorem, provided $\mathbb{F}$ is infinite.

Theorem 1.45. *Let $\mathbb{F}$ be infinite, $\mathbb{E}/\mathbb{F}$ finite extension, $\operatorname{Gal}(\mathbb{E}/\mathbb{F}) = \{g_1,\dots,g_n\}$. Then $g_1,\dots,g_n$ are algebraically independent i.e. for all $e \in \mathbb{E}$ if for some $f(X_1,\dots,X_n) \in \mathbb{E}[X_1,\dots,X_n]$ we have $f(g_1(e),\dots,g_n(e))$, then $f(X_1,\dots,X_n) = 0$.*

Proof. Let $\{e_1, \dots, e_n\}$ be a basis of $\mathbb{E}$ over $\mathbb{F}$. By the first lemma $\{g_i(e_j)\}$ is nonsingular. Let $e = \sum_{j=1}^n c_j e_j$, so $g_i(e) = \sum_{j=1}^n c_j g_i(e_j)$. Suppose $f(g_1(e), \dots, g_n(e)) = 0$ for all $e \in \mathbb{E}$. After substitution

$$f(\dots, \sum_{j=1}^n c_j g_i(e_j), \dots) = 0,$$

for all $e \in \mathbb{E}$, so from the second lemma

$$f(\dots, \sum_{j=1}^n X_j g_i(e_j), \dots) = 0.$$

Since $X_i \mapsto \sum_{j=1}^n X_j g_i(e_j)$ is an automorphism of $\mathbb{E}[X_1, \dots, X_n]$ we get that $f(\dots, X_i, \dots) = 0$. □

Proof. (of the Normal Basis Theorem (1.42)) Let $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \{g_1, \dots, g_n\}$. Take a matrix

$$A_{ij} = X_k \quad \text{if} \quad g_i g_j = g_k.$$

Denote its determinant by $d(X_1, \dots, X_n) := \det(A_{ij}) \in \mathbb{E}[X_1, \dots, X_n]$. Then $d(1, \dots, 1) = \pm 1 \neq 0$ because each X_k appears only once in every row and every column. Hence $d(X_1, \dots, X_n) \neq 0$.

Let $e_j := g_j(e)$, $A^e_{ij} := g_k(e)$ if $g_i g_j = g_k$. Then $A^e_{ij} = g_i g_j(e) = g_i(e_j)$, and $\det(A^e_{ij}) = d(g_1(e), \dots, g_n(e))$. By the previous theorem there exists $e \in \mathbb{E}$ such that

$$d(g_1(e), \dots, g_n(e)) \neq 0.$$

By the first lemma $\{e_1, \dots, e_n\}$ is a normal basis. □

1.8 Hilbert's 90 theorem

Definition 1.46. Let $\mathbb{E}/\mathbb{F}$ be finite Galois, $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

- The *norm* $\mathrm{N}_{\mathbb{E}/\mathbb{F}} \colon \mathbb{E} \to \mathbb{F}$ is given by

$$\mathrm{N}_{\mathbb{E}/\mathbb{F}}(e) := \prod_{g \in G} g(e).$$

- The *trace* $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}} \colon \mathbb{E} \to \mathbb{F}$ is given by

$$\mathrm{Tr}_{\mathbb{E}/\mathbb{F}} := \sum_{g \in G} g(e).$$

Theorem 1.47. *Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension with cyclic Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ generated by $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Then the following sequences of abelian groups*

1.
$$\mathbb{E}^* \xrightarrow{\partial} \mathbb{E}^* \xrightarrow{\mathrm{N}_{\mathbb{E}/\mathbb{F}}} \mathbb{F}, \quad \partial(e) = \frac{e}{g(e)}$$

2.
$$\mathbb{E} \xrightarrow{\partial} \mathbb{E} \xrightarrow{\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}} \mathbb{F}, \quad \partial(e) = e - g(e)$$

are exact.

Proof.

1. By the Dedekind theorem $\{g, g^2, \ldots, g^{n-1}, g^n = 1\}$ are linearly independent over $\mathbb{E}$. For every $(e_1, \ldots, e_n) \in \mathbb{E}^n$ there exists $\tilde{\tilde{e}} \in \mathbb{E}$ such that

$$\tilde{e} := \sum_{i=1}^{n} e_i g^i(\tilde{\tilde{e}}) \neq 0.$$

Take

$$\begin{cases} e_i & := \; eg(e)\ldots g^{i-1}(e), \; i = 1, \ldots n-1, \\ e_n & := \; 1 = \mathrm{N}_{\mathbb{E}/\mathbb{F}}(e) \end{cases}$$

We have

$$\begin{aligned}
eg(e_i) &= eg(e)\ldots g^i(e) = e_{i+1}, \; i = 1, \ldots, n-1 \\
eg(e_n) &= e = e_1 \\
eg(\tilde{e}) &= \sum_{i=1}^{n} eg(e_i) g^{i+1}(\tilde{\tilde{e}}) \\
&= \sum_{i=1}^{n-1} \underbrace{eg(e_i)}_{e_{i+1}} g^{i+1}(\tilde{\tilde{e}}) + \underbrace{eg(e_n)}_{e_1} \underbrace{g^{n+1}}_{g}(\tilde{\tilde{e}}) \\
&= \sum_{i=1}^{n-1} e_{i+1} g^{i+1}(\tilde{\tilde{e}}) + e_1 g(\tilde{\tilde{e}}) \\
&= \sum_{i=2}^{n} e_i g^i(\tilde{\tilde{e}}) + e_1 g(\tilde{\tilde{e}}) \\
&= \sum_{i=1}^{n} e_i g^i(\tilde{\tilde{e}}) \\
&= \tilde{e}.
\end{aligned}$$

Hence $e = \frac{\tilde{e}}{g(\tilde{e})}$.

2. By the Dedekind theorem (1.19) there is $\tilde{\tilde{e}} \in \mathbb{E}$ such that $\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(\tilde{\tilde{e}}) = 1$.

$$\begin{aligned}
\tilde{e} &:= eg(\tilde{\tilde{e}}) + (e + g(e))g^2(\tilde{\tilde{e}}) + \ldots + (e + g(e) + \ldots + g^{n-2}(e))g^{n-1}(\tilde{\tilde{e}}) \\
\tilde{e} - g(\tilde{e}) &= e(\underbrace{\tilde{\tilde{e}} + g(\tilde{\tilde{e}}) + \ldots + g^{n-1}(\tilde{\tilde{e}})}_{=\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(\tilde{\tilde{e}})=1}) - (\underbrace{e + g(e) + \ldots + g^{n-1}(e)}_{=\mathrm{Tr}_{\mathbb{E}/\mathbb{F}}(e)=0})\tilde{\tilde{e}} \\
&= e.
\end{aligned}$$

$\square$

Chapter 2

Hopf-Galois extensions

2.1 Canonical map

Theorem 2.1. *Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension, $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Then*

$$\begin{aligned} \mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} &\to \mathrm{Map}(G, \mathbb{E}), \\ e_1 \otimes e_2 &\mapsto (g \mapsto e_1 g(e_2)) \end{aligned}$$

is bijective.

Proof. Let $G = \{g_1, \ldots, g_n\}$. Observe that can is left $\mathbb{E}$-linear and

$$\dim_{\mathbb{E}}(\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) = \dim_{\mathbb{F}}(\mathbb{E}) = [\mathbb{E} : \mathbb{F}],$$

$$\dim_{\mathbb{E}}(\mathrm{Map}(G, \mathbb{E})) = |G|.$$

By Galois theory these dimensions are equal. It is enough to prove that can is injective. Let $\sum \tilde{e}_i \otimes e_i \in \ker(\mathrm{can})$, where $\{e_1, \ldots, e_n\}$ is a basis of $\mathbb{E}/\mathbb{F}$. After applying the canonical map we get that for all $g_j \in G$

$$\sum_{i=1}^{n} \tilde{e}_i g_j(e_i) = 0.$$

By the Dedekind theorem (1.19) $g_j(e_i)$ are nonsingular, so all $\tilde{e}_i$ are zero, and $\ker(\mathrm{can}) = \{0\}$. ☐

Theorem 2.2. *If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension, $G < \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then*

$$\mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \mathrm{Map}(G, \mathbb{E}),$$

$$e_1 \otimes e_2 \to (g \mapsto e_1 g(e_2))$$

is well defined, and the following implication holds:

$$\mathrm{can} \ \textit{is bijective} \implies \mathbb{F} = \mathbb{E}^G.$$

Proof. We have

$$\underbrace{\dim_{\mathbb{F}}(\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E})}_{[\mathbb{E}:\mathbb{F}]^2} = \underbrace{\dim_{\mathbb{F}}(\mathrm{Map}(G, \mathbb{E}))}_{|G|[\mathbb{E}:\mathbb{F}]}$$

Hence $[\mathbb{E} : \mathbb{F}] = |G| = [\mathbb{E} : \mathbb{E}^G]$. If $\mathbb{F} \subset \mathbb{E}^G$, then $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{E}^G][\mathbb{E}^G : \mathbb{F}]$, so $[\mathbb{E}^G : \mathbb{F}] = 1$, that is $\mathbb{F} = \mathbb{E}^G$. ☐

Corollary 2.3. *If $\mathbb{E}/\mathbb{F}$ is a finite extension, $G < \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then $\mathbb{E}/\mathbb{F}$ is Galois if and only if* can *is bijective.*

What algebraic structures are involved in can?
On $\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}$ there is a structure of a bimodule over $\mathbb{E}$

$$\begin{aligned} e(e_1 \otimes e_2) &= ee_1 \otimes e_2 \\ (e_1 \otimes e_2)e &= e_1 \otimes e_2 e \end{aligned}$$

If one wants can to be a bimodule map, then $\mathrm{Map}(G, \mathbb{E})$ has to be equipped with the following bimodule structure

$$\begin{aligned} (e\varphi)(g) &= e\varphi(g) \\ (\varphi e)(g) &= \varphi(g)g(e) \end{aligned}$$

2.2 Coring structure

Definition 2.4. (C, Δ, ε) is called a *coring* over $\mathbb{E}$ if C is a bimodule over $\mathbb{E}$ equipped with bimodule maps $\Delta\colon C \to C \otimes_{\mathbb{E}} C$ (a *comultiplication*), and $\varepsilon\colon C \to \mathbb{E}$ (a *counit*) such that the following diagrams commute

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"] & C \otimes_{\mathbb{E}} C \arrow[d, "\mathrm{id}\otimes\Delta"] \\ C \otimes_{\mathbb{E}} C \arrow[r, "\Delta\otimes\mathrm{id}"] & C \otimes_{\mathbb{E}} C \otimes_{\mathbb{E}} C \end{tikzcd}$$

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"] \arrow[dr, "\mathrm{id}"] & C \otimes_{\mathbb{E}} C \arrow[d, "\mathrm{id}\otimes\varepsilon"] \\ C \otimes_{\mathbb{E}} C \arrow[r, "\varepsilon\otimes\mathrm{id}"] & C \end{tikzcd}$$

On $\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}$ there is a coring structure given by

$$\begin{aligned} &\Delta(e_1 \otimes e_2) := (e_1 \otimes 1) \otimes (1 \otimes e_2) \in (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}), \\ &\varepsilon(e_1 \otimes e_2) := e_1 e_2. \end{aligned}$$

The following diagrams commute

$$\begin{tikzcd} \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \arrow[r, "\Delta"] \arrow[d, "\Delta"] & (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \arrow[d, "\mathrm{id}\otimes\Delta"] \\ (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \arrow[r, "\Delta\otimes\mathrm{id}"] & (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \arrow[r, "\Delta"] \arrow[d, "\Delta"] \arrow[dr, "\mathrm{id}"] & (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \arrow[d, "\mathrm{id}\otimes\varepsilon"] \\ (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \arrow[r, "\varepsilon\otimes\mathrm{id}"] & \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \end{tikzcd}$$

so $(\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}, \Delta, \varepsilon)$ is a coring.

On $\mathrm{Map}(G, \mathbb{E})$ there is also a canonical comultiplication Δ induced by the group law $G \times G \to G$.

$$\begin{tikzcd}
\mathrm{Map}(G,\mathbb{E}) \arrow[rr, dashed, "\Delta"] \arrow[dr] & & \mathrm{Map}(G,\mathbb{E}) \otimes_{\mathbb{E}} \mathrm{Map}(G,\mathbb{E}) \arrow[dl, "\simeq"] \\
& \mathrm{Map}(G \times G, \mathbb{E}) &
\end{tikzcd}$$

The isomorphism $\mathrm{Map}(G,\mathbb{E}) \otimes_{\mathbb{E}} \mathrm{Map}(G,\mathbb{E}) \to \mathrm{Map}(G \times G, \mathbb{E})$ is given by

$$\varphi_1 \otimes \varphi_2 \mapsto ((g_1, g_2) \mapsto \varphi_1(g_1) g_1(\varphi_2(g_2))).$$

The counit is induced by the neutral element $g_0 \in G$

$$\varepsilon\colon \mathrm{Map}(G,\mathbb{E}) \to \mathbb{E}, \quad \varphi \mapsto \varphi(g_0).$$

Altogether these give a coring structure on $\mathrm{Map}(G,\mathbb{E})$.

Proposition 2.5. *The canonical map* $\mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \mathrm{Map}(G,\mathbb{E})$ *is a homomorphism of corings over* $\mathbb{E}$*.*

Proof. We have to check compatibility with comultiplication, that is commutativity of the diagram

$$\begin{tikzcd}
\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \arrow[r, "\mathrm{can}"] \arrow[dd, "\Delta"'] & \mathrm{Map}(G,\mathbb{E}) \arrow[d] \\
& \mathrm{Map}(G \times G, \mathbb{E}) \arrow[d] \\
(\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}) \arrow[r, "\mathrm{can} \otimes \mathrm{can}"] & \mathrm{Map}(G,\mathbb{E}) \otimes_{\mathbb{E}} \mathrm{Map}(G,\mathbb{E})
\end{tikzcd}$$

We have

$$\begin{tikzcd}
e_1 \otimes e_2 \arrow[r, mapsto] \arrow[ddd, mapsto] & (g \mapsto e_1 g(e_2)) \arrow[d, mapsto] \\
& ((g_1, g_2) \mapsto e_1 g_1 g_2(e_2)) \arrow[d, equal] \\
& ((g_1, g_2) \mapsto e_1 g_1(g_2(e_2))) \\
(e_1 \otimes 1) \otimes (1 \otimes e_2) \arrow[r, mapsto] & (g_1 \mapsto e_1) \otimes (g_2 \mapsto g_2(e_2)) \arrow[u, mapsto]
\end{tikzcd}$$

Next we check the compatibility with the counit that is commutativity of the diagram

$$\begin{tikzcd}
\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \arrow[r, "\mathrm{can}"] \arrow[d, "\varepsilon"'] & \mathrm{Map}(G,\mathbb{E}) \arrow[d, "\varepsilon"] \\
\mathbb{E} \arrow[r] & \mathbb{E}
\end{tikzcd}$$

We have

$$\begin{tikzcd}
e_1 \otimes e_2 \arrow[r, mapsto] \arrow[d, mapsto] & (g \mapsto e_1 g(e_2)) \arrow[d, mapsto] \\
e_1 e_2 \arrow[r, mapsto] & e_1 e_2 = e_1 g_0(e_2)
\end{tikzcd}$$

□

We will use the Sweedler notation for comultiplication $\Delta \colon C \to C \otimes_{\mathbb{E}} C$

$$\Delta(c) = \sum_i c_{1i} \otimes c_{2i} =: c_{(1)} \otimes c_{(2)}.$$

Proposition 2.6. *Let* (C, Δ, ε) *be a coring over* $\mathbb{E}$*. Then* $\operatorname{Hom}_{\mathbb{E}}(C, \mathbb{E})$ *is a ring with multiplication given by*

$$(\varphi_1 \varphi_2)(c) := \varphi_1(c_{(1)} \varphi_2(c_{(2)}))$$

and unit ε*.*

Examples 2.7.

1. $\operatorname{Hom}_{\mathbb{E}}(\mathbb{E} \otimes_{\mathbb{F}} \mathbb{E}, \mathbb{E}) = \operatorname{Hom}_{\mathbb{F}}(\mathbb{E}, \mathbb{E}) = \operatorname{End}_{\mathbb{F}}(\mathbb{E})$ with composition of morphisms as multiplication, and identity as the unit.

2. For finite G

$$E \rtimes G \xrightarrow{\simeq} \operatorname{Hom}_{\mathbb{E}}(\operatorname{Map}(G, \mathbb{E}), \mathbb{E})$$

$$\sum_{g \in G} e_g x_g \mapsto (\varphi \mapsto \sum_i e_i \varphi(g_i)), \quad x_g e = g(e) x_g$$

Corollary 2.8. *The canonical map of corings* $\operatorname{can} \colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \operatorname{Map}(G, \mathbb{E})$ *induces a ring homomorphism*

$$\operatorname{Hom}_{\mathbb{E}}(\operatorname{can}, \mathbb{E}) \colon E \rtimes G \to \operatorname{End}_{\mathbb{F}}(\mathbb{E}).$$

Proposition 2.9. *Let* $\mathbb{E}/\mathbb{F}$ *be a finite extension,* $G \subset \operatorname{Gal}(\mathbb{E}/\mathbb{F})$*. Then* $\mathbb{E}/\mathbb{F}$ *is Galois if and only if* $\operatorname{Hom}_{\mathbb{E}}(\operatorname{can}, \mathbb{E})$ *is bijective.*

Proof. If $\mathbb{E}/\mathbb{F}$ is Galois, then can is bijective, so $\operatorname{Hom}(\operatorname{can}, \mathbb{E})$ is bijective.

Apllying $\operatorname{Hom}(-, \mathbb{E})$ to $\operatorname{Hom}(\operatorname{can}, \mathbb{E})$ we obtain can again by finite dimension over $\mathbb{F}$. □

Remark 2.10. $\operatorname{End}_{\mathbb{F}}(\mathbb{E})$ is a matrix algebra with entries in $\mathbb{F}$. If $\mathbb{E}/\mathbb{F}$ is Galois then $\mathbb{E} \rtimes G$ is Morita equivalent to $\mathbb{F} = \mathbb{E}^G$ (i.e. the category $\mathbb{E}^G-\mathbf{Mod}$ is equivalent to $\mathbb{E} \rtimes G-\mathbf{Mod}$). It is the cornerstone of noncommutative geometry. If G is not finite, then $\mathbb{E}^G$ can be pathological and then one can take its noncommutative replacement $\mathbb{E} \rtimes G$.

Example 2.11. Let $\mathbb{E} = \mathbb{C}((X))$ be the field of rational complex functions. Take $G = \mathbb{Z}$ generated by $g(X) := 2X$. Each $e \in \mathbb{E}$ can be written as

$$e = \frac{a_{-n}}{x^n} + \frac{a_{-n+1}}{x^{n-1}} + \ldots + a_0 + a_1 x + \ldots$$

If g fixes e, then $a_i = 0$ for $i \neq 0$, so $\mathbb{E}^G = \mathbb{C}$. On the other hand $\mathbb{E} \rtimes G = \mathbb{C}((X)) \rtimes G$.

2.3 Hopf-Galois field extensions

Assume $[\mathbb{E} : \mathbb{F}] < \infty$, $G < \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Then

$$\mathrm{Map}(G, \mathbb{E}) = \mathbb{E} \otimes_{\mathbb{F}} \mathrm{Map}(G, \mathbb{F}).$$

$\mathrm{Map}(G, \mathbb{F})$ is an $\mathbb{F}$-algebra with pointwise multiplication and it is also a coalgebra with comultiplication

$$\begin{tikzcd}
\mathrm{Map}(G,\mathbb{F}) \arrow[rr, dashed, "\Delta"] \arrow[dr] & & \mathrm{Map}(G,\mathbb{F}) \otimes_{\mathbb{F}} \mathrm{Map}(G,\mathbb{F}) \arrow[dl, "\simeq"] \\
& \mathrm{Map}(G \times G, \mathbb{F}) &
\end{tikzcd}$$

$$\varphi_1 \otimes \varphi_2 \mapsto ((g_1, g_2) \mapsto \varphi_1(g_1)\varphi_2(g_2))$$
$$\varepsilon \colon \mathrm{Map}(G, \mathbb{F}) \to \mathbb{F}, \quad \varphi \mapsto \varphi(g_0).$$

There is also a coinverse map

$$S \colon \mathrm{Map}(G, \mathbb{F}) \to \mathrm{Map}(G, \mathbb{F}), \quad \varphi \mapsto (g \mapsto \varphi(g^{-1}))$$

Fact 2.12. *The comultiplication, counit, and coinverse are homomorphisms of (commutative) $\mathbb{F}$-algebras.*

This fact motivates the following definition:

Definition 2.13. An $\mathbb{F}$-algebra $\mathcal{H}$ is called *Hopf algebra* if it has a coassociative counital comultiplication Δ, and the coinverse S such that the following diagram is commutative

$$\begin{tikzcd}
& \mathcal{H} \arrow[dl, "\Delta"'] \arrow[d] \arrow[dr, "\Delta"] & \\
\mathcal{H} \otimes \mathcal{H} \arrow[d, "S\otimes\mathrm{id}"'] & \mathbb{F} \arrow[dd] & \mathcal{H} \otimes \mathcal{H} \arrow[d, "\mathrm{id}\otimes S"] \\
\mathcal{H} \otimes \mathcal{H} \arrow[dr, "m"'] & & \mathcal{H} \otimes \mathcal{H} \arrow[dl, "m"] \\
& \mathcal{H} &
\end{tikzcd}$$

The action of G in $\mathbb{E}$ defines the coaction of $\mathrm{Map}(G, \mathbb{F})$ on $\mathbb{E}$, i.e.

$$\mathbb{E} \mapsto \mathbb{E} \otimes_{\mathbb{F}} \mathrm{Map}(G, \mathbb{F}) = \mathrm{Map}(G, \mathbb{E})$$
$$e \mapsto (g \mapsto g(e))$$

compatible as follows with the comultiplication Δ

$$\begin{tikzcd}
\mathbb{E} \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & \mathbb{E} \otimes_{\mathbb{F}} \mathrm{Map}(G,\mathbb{F}) \arrow[d, "\mathrm{id}\otimes\Delta"] \\
\mathbb{E} \otimes_{\mathbb{F}} \mathrm{Map}(G,\mathbb{F}) \arrow[r] & \mathbb{E} \otimes_{\mathbb{F}} \mathrm{Map}(G,\mathbb{F}) \otimes_{\mathbb{F}} \mathrm{Map}(G,\mathbb{F})
\end{tikzcd}$$

Remark 2.14. For any $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$, $\mathbb{F}/\mathbb{K}$ finite, one can take another Hopf algebra $\mathrm{Map}(G, \mathbb{K})$ and obtain

$$\mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} \to \mathbb{E} \otimes_{\mathbb{K}} \mathrm{Map}(G, \mathbb{K}).$$

In the coring approach there is one canonical coring $\mathrm{Map}(G, \mathbb{E})$ related to the action of G on $\mathbb{E}$, which in the Hopf approach can be realized by many Hopf algebras $\mathrm{Map}(G, \mathbb{K})$ defined over subfields $\mathbb{F} \subset \mathbb{F}$. Even when we fix $\mathbb{K} = \mathbb{F}$ after replacing $\mathrm{Map}(G, \mathbb{F})$ by an arbitrary abstract Hopf algebra over $\mathbb{F}$ theory is not as complete as in the group case.

For every group G

$$\mathrm{Map}(G, \mathbb{F}) = \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}G, \mathbb{F}),$$

where $\mathbb{F}G$ is the group algebra of G. $\mathbb{F}G$ is also a Hopf algebra with comultiplication obtained from the diagonal map $G \mapsto G \times G$, $g \mapsto (g, g)$,

$$\Delta\colon \mathbb{F}G \to \mathbb{F}G \otimes \mathbb{F}G, \quad g \mapsto g \otimes g,$$

counit $\varepsilon\colon \mathbb{F}G \to \mathbb{F}$ sending all group elements to $1 \in \mathbb{F}$, and coinverse obtained from group inverse $g \mapsto g^{-1}$.

Dualization $\mathrm{Hom}(-, \mathbb{F})$ transforms the coalgebra structure of $\mathbb{F}G$ into the algebra structure of $\mathrm{Map}(G, \mathbb{F})$. If $|G| < \infty$ then

$$\mathbb{F}G \cong \mathrm{Hom}_{\mathbb{F}}(\mathrm{Map}(G, \mathbb{F}), \mathbb{F})$$

transforms the coalgebra structure of $\mathrm{Map}(G, \mathbb{E})$ into the algebra structure of $\mathbb{F}G$. From the point of view of $\mathbb{F}G$ the canonical map looks like

$$\begin{aligned} \mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} &\to \mathrm{Hom}_{\mathbb{F}}(\mathbb{F}G, \mathbb{E}) \\ e_1 \otimes e_2 &\mapsto (h \mapsto e_1 h e_2), \end{aligned}$$

where $\mathbb{F}G$ acts on $\mathbb{E}$ in the following way

$$h(e_1 e_2) := h_{(1)}(e_1) h_{(2)}(e_2).$$

Fixed subfield can also be defined in terms of this action

$$\mathbb{E}^{\mathbb{F}G} := \{e \in \mathbb{E} \mid \forall\, h \in \mathbb{F}G he = \varepsilon(h)e\} = \mathbb{E}^G$$

Replacing $\mathbb{F}G$ by an arbitrary Hopf algebra $\mathcal{H}$ we obtain

$$\begin{aligned} \mathrm{can}\colon \mathbb{E} \otimes_{\mathbb{F}} \mathbb{E} &\to \mathrm{Hom}_{\mathbb{F}}(\mathcal{H}, \mathbb{E}) \\ e_1 \otimes e_2 &\mapsto (h \mapsto e_1 h e_2). \end{aligned}$$

where $\mathcal{H}$ acts on $\mathbb{E}$ in the same manner

$$h(e_1 e_2) := h_{(1)}(e_1) h_{(2)}(e_2).$$

To extend the Galois theory to this case we need a notion of a Hopf subalgebra of $\mathcal{H}$.

Definition 2.15. $\mathcal{H}' \subset \mathcal{H}$ is a Hopf subalgebra of $\mathcal{H}$ if the inclusion is a homomorphism of Hopf algebras.

Theorem 2.16 (Chase-Sweedler)**.** *Let $\mathbb{E}/\mathbb{F}$ be Hopf-Galois with respect to the action of a cocommutative Hopf algebra $\mathcal{H}$. Then*

$$\phi\colon \{\mathcal{H}' \subset \mathcal{H} \mid \mathcal{H}' \text{ is Hopf subalgebra of } \mathcal{H}\} \to \{\mathbb{F}' \mid \mathbb{F} \subset \mathbb{F}' \subset \mathbb{E} \text{ subfield}\}$$

$$\mathcal{H}' \mapsto \mathbb{E}^{\mathcal{H}'}$$

is injective and inclusion reversing.

Note that the claim is about injectivity only. Another distinction comparing with classical Galois theory is that the Hopf algebra making a given extension Hopf-Galois is not unique.

Example 2.17 (Greither-Pareigis)*.* Let $\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(^4\sqrt{2})$, $\omega :=^4 \sqrt{2}$

$$\mathcal{H} := \mathbb{Q}[c, s]/(c^2 + s^2 - 1,\ cs)$$

with the comultiplication

$$\begin{aligned} \Delta\colon \mathcal{H} &\to \mathcal{H} \otimes_{\mathbb{F}} \mathcal{H} \\ c &\mapsto c \otimes c - s \otimes s \\ s &\mapsto c \otimes s + s \otimes c, \end{aligned}$$

counit

$$\begin{aligned} \varepsilon\colon \mathcal{H} &\to \mathbb{F} \\ c &\mapsto 1 \\ s &\mapsto 0, \end{aligned}$$

and coinverse

$$\begin{aligned} S\colon \mathcal{H} &\to \mathcal{H} \\ c &\mapsto c \\ s &\mapsto -s. \end{aligned}$$

The action $\mathcal{H} \otimes_{\mathbb{F}} \mathbb{E} \to \mathbb{E}$ is given in a table

	1	ω	ω^2	ω^4
c	1	0	$-\omega^2$	0
s	0	$-\omega$	0	ω^3

Then $\mathbb{E}/\mathbb{F}$ is $\mathcal{H}$-Galois.

Example 2.18*.* Let $\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(\sqrt[4]{2})$, $\omega := \sqrt[4]{2}$

$$\tilde{\mathcal{H}} := \mathbb{Q}[\tilde{c}, \tilde{s}]/(\tilde{c}^2 + \tilde{s}^2 - 1,\ \tilde{c}\tilde{s})$$

with the comultiplication

$$\begin{aligned} \Delta\colon \tilde{\mathcal{H}} &\to \tilde{\mathcal{H}} \otimes_{\mathbb{F}} \tilde{\mathcal{H}} \\ \tilde{c} &\mapsto \tilde{c} \otimes \tilde{c} - \tfrac{1}{2}\tilde{s} \otimes \tilde{s} \\ \tilde{s} &\mapsto \tilde{c} \otimes \tilde{s} + \tilde{s} \otimes \tilde{c}, \end{aligned}$$

counit

$$\begin{aligned}\varepsilon\colon \mathcal{H} &\to \mathbb{F}\\ \tilde{c} &\mapsto 1\\ \tilde{s} &\mapsto 0,\end{aligned}$$

and coinverse

$$\begin{aligned}S\colon \mathcal{H} &\to \mathcal{H}\\ \tilde{c} &\mapsto \tilde{c}\\ \tilde{s} &\mapsto -\tilde{s}.\end{aligned}$$

The action $\tilde{\mathcal{H}} \otimes_{\mathbb{F}} \mathbb{E} \to \mathbb{E}$ is given in a table

	1	ω	ω^2	ω^4
$\tilde{c}$	1	0	$-\omega^2$	0
$\tilde{s}$	0	ω^3	0	-2ω

Then $\mathbb{E}/\mathbb{F}$ is $\tilde{\mathcal{H}}$-Galois.

Example 2.19. Note that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, because the minimal polynomial of $\sqrt[4]{2}$ is $X^4 - 2$, and it has imaginary roots $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. Hence it is not Galois in a classical sense. However it is Hopf-Galois.

Example 2.20. There are separable field extensions which are not Hopf-Galois at all. For example no field extension $\mathbb{E}/\mathbb{F}$, $[\mathbb{E}/\mathbb{F}] = 5$ with $\operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F}) = 5$ (where $\widetilde{\mathbb{E}}$ denotes the normal closure of $\mathbb{F} \subset \mathbb{E} \subset \overline{\mathbb{F}}$) can be Hopf-Galois.

What can be said about separable Hopf-Galois extensions?

Definition 2.21. If S is a set, then a subgroup of $\operatorname{Perm}(S)$ is called *regular* if it is transitive with trivial stabilizers.

Let $\widetilde{\mathbb{E}}$ be a normal closure of $\mathbb{E}$ in $\overline{\mathbb{F}}$, so $\operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{E}) \subset \operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F})$. Denote

$$S := \operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{E})/\operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F}) \quad \text{(left cosets)}$$

Theorem 2.22. *The following conditions are equivalent:*

1. *There is a Hopf $\mathbb{F}$-algebra $\mathcal{H}$ such that $\mathbb{E}/\mathbb{F}$ is $\mathcal{H}$-Hopf-Galois.*
2. *There is a regular subgroup $N \subset \operatorname{Perm}(S)$ such that $\operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F}) = \operatorname{Perm}(S)$ normalizes N.*

Proposition 2.23. *The following conditions are equivalent:*

1. *There exists a Galois extension $\mathbb{F}'/\mathbb{F}$ such that $\mathbb{F}' \otimes_{\mathbb{F}} \mathbb{E}$ is a field containing $\widetilde{\mathbb{E}}$.*
2. *There exists a Galois extension $\mathbb{F}'/\mathbb{F}$ such thae $\mathbb{F}' \otimes_{\mathbb{F}} \mathbb{E} = \widetilde{\mathbb{E}}$.*
3. $\operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{E})$ *has a normal complement $N \subset \operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F})$.*
4. *There exists a normal subgroup $N \subset \operatorname{Gal}(\widetilde{\mathbb{E}}/\mathbb{F})$ which is regular in $\operatorname{Perm}(S)$.*

Definition 2.24. If $\mathbb{E}/\mathbb{F}$ is finite and one of the conditions (1)-(4) is fulfilled then this extension is called *almost classical*.

Theorem 2.25 (Greither-Pareigis)**.** *If $\mathbb{E}/\mathbb{F}$ is almost classicaly Galois, then there is a Hopf algebra $\mathcal{H}$ such that $\mathbb{E}/\mathbb{F}$ is $\mathcal{H}$-Hopf-Galois and the map*

$$\phi\colon \{\mathcal{H}' \subset \mathcal{H} \mid \mathcal{H}' \textit{ is Hopf subalgebra of } \mathcal{H}\} \to \{\mathbb{F}' \mid \mathbb{F} \subset \mathbb{F}' \subset \mathbb{E} \textit{ subfield}\}, \quad \mathcal{H}' \mapsto \mathbb{E}^{\mathcal{H}'}$$

is bijective.

However, even for classical Galois extensions one cannot expect that for such $\mathcal{H}$, making this extension Hopf-Galois, the image of ϕ contains all intermediate subfield.

Theorem 2.26 (Greither-Pareigis)**.** *Any classical Galois extension $\mathbb{E}/\mathbb{F}$ can be endowed with an $\mathcal{H}$-Galois structure such that the image of ϕ consists of normal intermediate extensions $\mathbb{F} \subset \mathbb{F}' \subset \mathbb{E}$.*

Example 2.27. Let $\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(\omega, \xi)$, where $\omega = \sqrt[3]{2}$ and $\xi = \frac{\sqrt{3}+i}{2}$. It is known that the extension $\mathbb{E}/\mathbb{F}$ is Galois with $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = S_3$. But there exists a Hopf algebra

$$\mathcal{H} := \underbrace{\mathbb{Q}\langle c, s, t\rangle}_{\text{noncommutative variables}} /(c(c-1)(c+1),\ 2c^2 + st + ts - 2,\ cs,\ sc,\ ct,\ tc,\ s^2,\ t^2)$$

The comultiplication is given by

$$\begin{aligned}\Delta\colon \mathcal{H} &\to \mathcal{H} \otimes_{\mathbb{F}} \mathcal{H}\\ c &\mapsto c \otimes c + \tfrac{1}{2}(s \otimes t + t \otimes s)\\ s &\mapsto c \otimes s + s \otimes c + \tfrac{1}{2} t \otimes t\\ t &\mapsto c \otimes t + t \otimes c + s \otimes s\end{aligned}$$

$\mathcal{H}$ is a Hopf algebra making $\mathbb{E}/\mathbb{F}$ Hopf-Galois, where action $\mathcal{H} \otimes_{\mathbb{F}} \mathbb{E} \to \mathbb{E}$ is given in the table

	1	ω	ξ
c	1	0	ξ^2
s	0	ω^2	0
t	0	0	0

In the image of ϕ one obtains only normal intermediate extensions.

2.4 Torsors

Let G be a group, X a set, $X \times G \to X$ right action $(x, g) \mapsto xg$. We assume that neutral element acts trivially $xg_0 = x$, and that $x(g_1 g_2) = (xg_1)g_2$.

Example 2.28.

1. $X = \emptyset$ or $X = *$, a one element set.
2. $X = G$, $G \times G \to G$ group composition.
3. $X = \{1, 2, \ldots, n\}$, $G = S_n$ acting by permutations.

Definition 2.29. A G-torsor is a G-set which is isomorphic to G in the category of G-sets.

Theorem 2.30. *The following conditions are equivalent*

1. *X is a G-torsor.*

2. *For all $x, y \in X$ there is a unique $g \in G$ such that $xg = y$.*

3. *For all $x \in X$ the map $g \mapsto xg$ gives an isomorphism $G \cong X$ of G-sets.*

4. *The map $X \times G \to X \times X$, $(x, g) \mapsto (x, xg)$ is bijective.*

We are mainly interested in algebraic sets.

Definition 2.31. If $I = \sqrt{I} \triangleleft \mathbb{F}[X_1, \ldots, X_n]$ is a radical ideal of an algebraic set $X \subset \overline{\mathbb{F}}^n$, then we form a *coordinate ring* of X

$$\mathcal{O}(X) = \mathbb{F}[X_1, \ldots, X_n]/I$$

Definition 2.32. If $\mathbb{F} \subset \mathbb{E}$ is an algebraic field extension then $X(\mathbb{E})$ is the set of $\mathbb{E}$-*points* of X.

Fact 2.33. *If X, Y are algebraic sets corresponding to $\mathbb{F}$-algebras $\mathcal{O}(X)$, $\mathcal{O}(Y)$ respectively then*

$$\mathcal{O}(X \times_{\mathbb{F}} Y) = \mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(Y)$$

$$(X \times_{\mathbb{F}} Y)(\mathbb{E}) = X(\mathbb{E}) \times Y(\mathbb{E})$$

Example 2.34. Let $\mathcal{O}(X) := \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$. The real points $X(\mathbb{R})$ form a circle in $\mathbb{R}^2$. But an algebraic set can have complex points, which are the complex solutions of $X^2 + Y^2 = 1$.

Definition 2.35. A *morphism of algebraic sets* $X \to Y$ over $\mathbb{F}$ is a homomoprhism of $\mathbb{F}$-algebras $\mathcal{O}(Y) \to \mathcal{O}(X)$.

This gives a map $X(\mathbb{E}) \to Y(\mathbb{E})$ for every algebraic extension $\mathbb{E}/\mathbb{F}$.

Example 2.36. $\mathrm{GL}_n(\mathbb{E})$ - set of $\mathbb{E}$-points of general linear group over $\mathbb{F}$.

$$\mathcal{O}(\mathrm{GL}_n) = \mathbb{F}[X_{11}, \ldots, X_{ij}, \ldots, X_{nn}; \det([X_{ij}]_{i,j=1}^n)^{-1}]$$

A linear algebraic group $G \subset \mathrm{GL}_n$ is defined by polynomial relations $f_1(X), \ldots, f_r(X)$, $X = [X_{ij}]_{i,j=1}^n$. A matrix $A \in G(\mathbb{E})$ if and only if $f_1(A) = 0, \ldots, f_r(A) = 0$. Here are the examples of linear algebraic groups:

1. GL_n, $f_1(X) = 0$.

2. SL_n, $f_1(X) = \det(X) - 1$.

3. O_n, $\{A^T A = I\}$.

4. UT_n, $f_{ij}(X) = X_{ij}$ for $i > j$.

If G is an algebraic group, then $\mathcal{H} = \mathcal{O}(G)$ is a Hopf algebra with the pointwise multiplication and comultiplication induced by the composition in G,

$$\Delta\colon \mathcal{O}(G) \to \mathcal{O}(G) \otimes_{\mathbb{F}} \mathcal{O}(G) \simeq \mathcal{O}(G \times_{\mathbb{F}} G).$$

If $\mathbb{E}/\mathbb{F}$ is any field extension then an $\mathbb{F}$-homomorphism $\mathcal{O}(G) \to \mathbb{E}$ is determined by a subgroup $G(\mathbb{E}) \subset \mathrm{GL}_n(\mathbb{E})$.

Consider a group action of G on X. The compatibility conditions can be shown using diagrams

$$\begin{tikzcd}
X \times_{\mathbb{F}} G \times_{\mathbb{F}} G \arrow[r] \arrow[d] & X \times_{\mathbb{F}} G \arrow[d] \\
X \times_{\mathbb{F}} G \arrow[r] & X
\end{tikzcd}
\qquad
\begin{tikzcd}
X \times * \arrow[d] \arrow[dr] & \\
X \times_{\mathbb{F}} G \arrow[r] & X
\end{tikzcd}$$

These diagrams can be dualized

$$\begin{tikzcd}
\mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(G) \otimes_{\mathbb{F}} \mathcal{O}(G) & \mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(G) \arrow[l] \\
\mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(G) \arrow[u] & \mathcal{O}(X) \arrow[l] \arrow[u]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{O}(X) \otimes * \arrow[d, leftrightarrow] \arrow[dr, leftrightarrow] & \\
\mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(G) & \mathcal{O}(X) \arrow[l]
\end{tikzcd}$$

Algebraic G-action on an algebraic set induces a coaction of the Hopf algebra $\mathcal{O}(G)$ on an algebra $\mathcal{O}(X)$. Then X is a G-torsor if the map

$$\begin{tikzcd}
\mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(X) \arrow[r] \arrow[d, equal] & \mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(X) \arrow[d, equal] \\
\mathcal{O}(X \times_{\mathbb{F}} X) & \mathcal{O}(X \times_{\mathbb{F}} G)
\end{tikzcd}$$

is induced by the canonical map

$$X \times_{\mathbb{F}} X \leftarrow X \times_{\mathbb{F}} G$$

On $\mathbb{E}$-points it is given by

$$\begin{tikzcd}
(X \times_{\mathbb{F}} X)(\mathbb{E}) \arrow[d, equal] & (X \times_{\mathbb{F}} G)(\mathbb{E}) \arrow[l] \arrow[d, equal] \\
X(\mathbb{E}) \times X(\mathbb{E}) & X(\mathbb{E}) \times G(\mathbb{E})
\end{tikzcd}$$

$$(x, xg) \longleftarrow\!\!\shortmid (x, g)$$

Example 2.37. If $\mathbb{E}/\mathbb{F}$ is a finite Galois extension then the algebraic set X over $\mathbb{F}$ corresponding to an $\mathbb{F}$-algebra $\mathbb{E} = \mathcal{O}(X)$ is a G-torsor where G is a linear algebraic group corresponding to an $\mathbb{F}$-algebra $\mathcal{O}(G) = \mathrm{Map}(\mathrm{Gal}(\mathbb{E}/\mathbb{F}), \mathbb{F})$. Note that $X(\mathbb{F}) = \emptyset$, $X(\mathbb{E})$ is a finite set of cardinality equal to the degree of the extension $[\mathbb{E} : \mathbb{F}]$. If $\mathbb{E}$ is a splitting field of $f(X) \in \mathbb{F}[X]$, then $X(\mathbb{E})$ is the set of roots of f.

2.5 Crossed homomorphisms and G-torsors

Let $\mathbb{E}/\mathbb{F}$ be a finite Galoios extension, and G linear algebraic group over $\mathbb{F}$.

Definition 2.38. A crossed homomorphism is a map

$$\varphi\colon \operatorname{Gal}(\mathbb{E}/\mathbb{F}) \to G(\mathbb{E})$$

satisfying $\varphi(g_1g_2) = \varphi(g_1)g_1(\varphi(g_2))$. Two crossed morphisms φ, φ' are said to be *equivalent* if $\varphi'(g) = \psi\varphi(g)\psi^{-1}$ for some $\psi \in G(\mathbb{E})$.

A crossed homomorphism φ gives rise to a torsor as follows. On $\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G)$ we have an obvious $\operatorname{Gal}(\mathbb{E}/\mathbb{F})$-action, and we define a φ-twisted action by

$$g \cdot (e \otimes h) := g(e) \otimes \varphi(g^{-1})^* h \in \mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G)$$

Then the fixed $\mathbb{F}$-subalgebra $(\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G))^{\operatorname{Gal}(\mathbb{E}/\mathbb{F})}$ is a coordinate ring $\mathcal{O}(X)$ for a G-torsor X with the G-action induced by the restriction $\mathcal{O}(X) \to \mathcal{O}(X) \otimes_{\mathbb{F}} \mathcal{O}(G)$ of the comultiplication

$$\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G) \to (\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G)) \otimes_{\mathbb{E}} (\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G)).$$

Definition 2.39. W say that the extension $\mathbb{E}/\mathbb{F}$ trivializes a G-torsor X if after the base extension $\mathbb{E}/\mathbb{F}$ we have an isomorphism.

$$\mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(X) \simeq \mathbb{E} \otimes_{\mathbb{F}} \mathcal{O}(G).$$

Theorem 2.40. *The isomorphism classes of G-torsors over $\mathbb{F}$ trivializable by the extension $\mathbb{E}/\mathbb{F}$ correspond bijectively to the equivalence classes of crossed homomorphisms* $\operatorname{Gal}(\mathbb{E}/\mathbb{F}) \to G(\mathbb{E})$.

Example 2.41. Let $G = \mathrm{GL}_1 = \overline{\mathbb{F}}^*$ (invertible elements). Then the set of nonzero vectors in any one dimensional vector space over $\mathbb{F}$ is a G-torsor X over $\mathbb{F}$. Then the set of isomorphism classes of such torsors correspond bijectively to the set of isomorphism classes of one dimensional vector spaces over $\mathbb{F}$.

The set of equivalence classes of crossed homomorphisms $\operatorname{Gal}(\mathbb{E}/\mathbb{F}) \to G(\mathbb{E})$ is $\mathrm{H}^1(\operatorname{Gal}(\mathbb{E}/\mathbb{F}); \mathbb{E}^*)$, which is 0 by the Hilbert's 90'th theorem (1.47).

Example 2.42. Let $\mathbb{F} = \mathbb{C}$, $\mathcal{O}(G) = \mathbb{C}[g, h, g^{-1}, h^{-1}]$,

$$\mathcal{O}(X) = \mathbb{C}\langle x, y, x^{-1}, y^{-1}\rangle/(xy = qyx), \quad q \in \mathbb{C}^*.$$

2.6 Descent theory

Let $\mathbb{E}/\mathbb{F}$ be a field extension. Given an algebraic object A defined over $\mathbb{F}$ (vector space, quadratic space, algebra, coalgebra, Hopf algebra etc.) one can construct an algebraic object $\mathbb{E} \otimes_{\mathbb{F}} A$ defined over $\mathbb{E}$. The aim of descent theory is to say something about what happens when we go in the opposite direction. For example given $a_{\mathbb{E}} \in A_{\mathbb{E}} := \mathbb{E} \otimes_{\mathbb{F}} A$ we can ask what conditions guarantee that $a_{\mathbb{E}} = 1 \otimes a_{\mathbb{F}}$.

Example 2.43. If $\mathbb{E}/\mathbb{F}$ is finite Galois extension then taking $A_{\mathbb{F}} = \mathbb{F}$ we obtain $A_{\mathbb{E}} = \mathbb{E} \otimes_{\mathbb{F}} \mathbb{F} = \mathbb{E}$. The answer in this case is: this happens if and only if $g(a) = a$ for all $g \in \operatorname{Gal}(\mathbb{E}/\mathbb{F})$.

Another problem consists in the question when a given $A_{\mathbb{E}}$ defined over $\mathbb{E}$ is of the form $A_{\mathbb{E}} = \mathbb{E} \otimes_{\mathbb{F}} A_{\mathbb{F}}$. This is called a problem of forms of algebraic structures.

Definition 2.44. $A'_{\mathbb{F}}$ is called $\mathbb{E}$-form of $A_{\mathbb{F}}$ if $\mathbb{E} \otimes_{\mathbb{F}} A'_{\mathbb{F}} \simeq \mathbb{E} \otimes_{\mathbb{F}} A_{\mathbb{F}}$.

Example 2.45. Let $\mathbb{F} = \mathbb{R}$, $\mathbb{E} = \mathbb{C}$, $\mathcal{H} = \mathbb{R}\mathbb{Z}$ (group algebra). Define

$$\begin{aligned} \mathcal{H}' &:= \mathbb{R}[c,s]/(c^2+s^2-1) \\ \Delta(c) &= c \otimes c - s \otimes s \\ \Delta(s) &= c \otimes s + s \otimes c \end{aligned}$$

Then

$$a := 1 \otimes c + i \otimes s = c + is \in \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}'$$

is invertible with inverse $a^{-1} = c - is \in \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}'$. Hence $c, s \in \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}'$, and

$$\mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}' = \mathbb{C}[a, a^{-1}] \cong \mathbb{C}\mathbb{Z} \cong \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}$$

Note that $\mathcal{H}$ and $\mathcal{H}'$ are not isomorphic over $\mathbb{R}$, because their groups of real points are different:

$$\mathrm{Hom}(\mathcal{H}, \mathbb{R}) \cong \mathbb{R}^*$$

with only two elements of finite order $\{1, -1\}$, and

$$\mathrm{Hom}(\mathcal{H}', \mathbb{R}) \cong \mathrm{U}(1)$$

with infinitely many elements of finite order.

Theorem 2.46 (Haggenmüller-Pereigis)**.** *Let Γ be a finitely generated group with finite isomorphism group G. Then there is a bijection between the set of isomorphism classes of G-Galois extensions of $\mathbb{F}$ and the set of Hopf algebra forms of $\mathcal{H} = \mathbb{F}\Gamma$. This associates with each G-Galois extension $\mathbb{E}$ of $\mathbb{F}$ the Hopf algebra*

$$\mathcal{H}' := \left\{ \sum_{\gamma \in \Gamma} c_\gamma \gamma \in \mathbb{E}\Gamma \mid \forall\, g \in G \ \sum_{\gamma \in \Gamma} g(c_\gamma) g(\gamma) = \sum_{\gamma \in \Gamma} c_\gamma \gamma \right\}$$

which is an $\mathbb{E}$-form of $\mathbb{E}\Gamma$ by the isomorphism

$$\begin{aligned} \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H}' &\to \mathbb{E} \otimes_{\mathbb{F}} \mathcal{H} = \mathbb{E}\Gamma \\ e \otimes \sum_{\gamma \in \Gamma} c_\gamma \gamma &\mapsto \sum_{\gamma \in \Gamma} e c_\gamma \otimes \gamma \end{aligned}$$

Example 2.47. Let $G = \mathbb{Z}/2$, g-generator, $\mathbb{C} \hookrightarrow \mathbb{H} = \{z_0 + z_1 j \mid jz = \bar{z}j,\ j^2 = -1\}$.

$$g(z_0 + z_1 j) := z_0 - z_1 j = i(z_0 + z_1 j) i^{-1}$$

Then $\mathbb{H}^G = \mathbb{C} \subset \mathbb{H}$, and

$$\begin{aligned} \mathrm{can}\colon \mathcal{H} \otimes_{\mathbb{C}} \mathcal{H} &\cong \mathrm{Map}(G, \mathcal{H}) \\ q_1 \otimes q_2 &\mapsto (g \mapsto q_1 g(q_2)) \end{aligned}$$