

# Fields and Galois Theory

File name: `ktt.tex`

Utkan Utkaner

April 29, 2020

## 1 Basic Definitions and Results

### 1.1 Symmetry

### 1.2 Rings

### 1.3 Domains and Fields

### 1.4 Homomorphisms and Ideals

### 1.5 Quotient Rings

### 1.6 Polynomial Rings over Fields

### 1.7 Prime Ideals and Maximal Ideals

## 2 Algebraic Extensions of Fields

### 2.1 Factoring Polynomials

**Proposition 2.1** (Gauss's Lemma (Primitivity)). *The product of two primitive polynomials  $f(x)$  and  $g(x)$  is itself primitive.*

*Proof.* Assume that the product  $f(x)g(x)$  is not primitive, so there is some prime  $p$  dividing each of its coefficients. Let  $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}_p$  be the natural map, and consider the ring map  $\sigma^* : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$  reducing coefficients mod  $p$ . Now

$$\sigma^*(fg) = \sigma^*(f)\sigma^*(g).$$

But  $\sigma^*(fg) = 0$  in  $\mathbb{Z}_p[x]$  while  $\sigma^*(f) \neq 0$  and  $\sigma^*(g) \neq 0$ , and this contradicts the fact that  $\mathbb{Z}[x]$  is a domain.  $\square$

**Proposition 2.2** (Gauss's Lemma (Irreducibility)). *Let  $f(x) \in \mathbb{Z}[x]$ . If  $f(x)$  is reducible over  $\mathbb{Q}$ , then it is also reducible over  $\mathbb{Z}$ .*

*Proof.* Suppose  $f(x)$  is reducible over  $\mathbb{Q}$ . Without loss of generality we may assume that  $f(x)$  is primitive. Let  $f(x) = u(x)v(x)$  with  $u(x), v(x) \in \mathbb{Q}[x]$  and  $u(x), v(x) \notin \mathbb{Q}$ . Then  $f(x) = (a/b)u'(x)v'(x)$ , where  $u'(x)$  and  $v'(x)$  are primitive polynomials in  $\mathbb{Z}[x]$ . Then  $bf(x) = au'(x)v'(x)$ . The gcd of the coefficients of  $bf(x)$  is  $b$ , and the gcd of the coefficients of  $au'(x)v'(x)$  is  $a$ , by xxx. Hence,  $b = \pm a$ , so  $f(x) = \pm u'(x)v'(x)$ . Therefore,  $f(x)$  is reducible over  $\mathbb{Z}$ .  $\square$

**Proposition 2.3.** *Let  $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$  be a monic polynomial, i.e., a polynomial with leading coefficient one. If  $f(x)$  has a root  $a \in \mathbb{Q}$ , then  $a \in \mathbb{Z}$  and  $a|a_0$ .*

*Proof.* Write  $a = \alpha/\beta$ , where  $\alpha, \beta \in \mathbb{Z}$  and  $(\alpha, \beta) = 1$ . Then

$$a_0 + a_1\left(\frac{\alpha}{\beta}\right) + \cdots + a_{n-1}\left(\frac{\alpha^{n-1}}{\beta^{n-1}}\right) + \frac{\alpha^n}{\beta^n} = 0.$$

Multiply the above equation by  $\beta^{n-1}$  to obtain

$$a_0\beta^{n-1} + a_1\alpha\beta^{n-2} + \cdots + a_{n-1}\alpha^{n-1} = -\frac{\alpha^n}{\beta}.$$

Because  $\alpha, \beta \in \mathbb{Z}$ , it follows that  $\alpha^n/\beta \in \mathbb{Z}$ , so  $\beta$  must be  $\pm 1$ . The last equation also shows  $\alpha|a_0$ . Hence,  $a = \pm\alpha \in \mathbb{Z}$  and  $a|a_0$ .  $\square$

**Proposition 2.4** (Eisenstein's Criterion). *Let  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$  for  $n \geq 1$ . If there is a prime  $p$  such that  $p^2 \nmid a_0$ ,  $p|a_1, \dots, p|a_{n-1}$ ,  $p \nmid a_n$ , then  $f(x)$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* Suppose

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),$$

with  $b_i, c_i \in \mathbb{Z}$ ,  $b_r \neq 0$ ,  $c_s \neq 0$ ,  $r < n$ , and  $s < n$ . Then  $a_0 = b_0c_0$  and  $a_n = b_rc_s$ . Then since  $p|a_0$  and  $p^2 \nmid a_0$ , either  $p|b_0$  and  $p \nmid c_0$  or  $p|c_0$  and  $p \nmid b_0$ . Consider the case  $p|c_0$  and  $p \nmid b_0$ . Because  $p \nmid a_n$ , it follows that  $p \nmid b_r$  and  $p \nmid c_s$ . Let  $c_m$  be the first coefficient in  $c_0 + \cdots + c_sx^s$  such that  $p \nmid c_m$ . Then note that  $a_m = b_0c_m + b_1c_{m-1} + \cdots + b_mc_0$ . From this we see that  $p \nmid a_m$  (otherwise,  $p|c_m$ ), so  $m = n$ . Then  $n = m \leq s < n$ , which is impossible. Similarly, if  $p|b_0$  and  $p \nmid c_0$ , we arrive at an absurdity. Hence by Gauss's Lemma,  $f(x)$  is irreducible over  $\mathbb{Q}$ .  $\square$

*Remark 2.1.* The last three propositions hold mutatis mutandis with  $\mathbb{Z}$  replaced by a unique factorization domain  $R$  (replace  $\mathbb{Q}$  with the field of fractions of  $R$  and  $p$  with a prime element of  $R$ ).

## 2.2 Adjunction of Roots

**Definition 2.1.** If  $F$  is a subfield of a field  $E$ , one also says that  $E$  is an extension of  $F$ , and one writes  $E/F$  is an extension.

**Definition 2.2.** Let  $E/F$  be an extension. The dimension of  $E$  viewed as a vector space over  $F$  is called the degree of  $E$  over  $F$  and it is denoted by  $[E : F]$ . One says that  $E/F$  is a finite extension if  $[E : F]$  is finite.

**Definition 2.3.** When  $K$  and  $L$  are extensions of a field  $F$ , an  $F$ -homomorphism of  $K$  into  $L$  or an embedding of  $K$  in  $L$  over  $F$  is a homomorphism  $\varphi : K \rightarrow L$  such that  $\varphi(c) = c$  for all  $c \in F$ .

**Proposition 2.5** (Multiplicativity of Degrees). *If  $F \subset B \subset E$  are fields with  $[E : B]$  and  $[B : F]$  finite, then  $E/F$  is a finite extension and*

$$[E : F] = [E : B][B : F].$$

*Proof.* Let  $\{\alpha_1, \dots, \alpha_m\}$  be a basis of  $E/B$ , and let  $\{\beta_1, \dots, \beta_n\}$  be a basis of  $B/F$ . It suffices to prove that  $\{\beta_j \alpha_i : 1 \leq i \leq m, 1 \leq j \leq n\}$  is a basis of  $E/F$ .

This set spans  $E$ . If  $\gamma \in E$ , then there are  $b_i$  in  $B$  with  $\gamma = \sum b_i \alpha_i$ . But each  $b_i = \sum c_{ij} \beta_j$  for  $c_{ij}$  in  $F$ ; hence  $\gamma = \sum c_{ij} \beta_j \alpha_i$ . To see that this set is linearly independent, assume that  $\sum c_{ij} \beta_j \alpha_i = 0$  for  $c_{ij}$  in  $F$ . Now  $b_i = \sum c_{ij} \beta_j \in B$ , so that independence of the  $\alpha_i$  over  $B$  implies that  $b_i = 0$  for all  $i$ . Hence  $\sum c_{ij} \beta_j = 0$  for all  $i$ , and so the independence of the  $\beta_j$  over  $F$  implies that  $c_{ij} = 0$  for all  $i, j$ , as desired.  $\square$

**Proposition 2.6.** *If  $F$  is a field and  $p(x) \in F[x]$  is irreducible, then the quotient ring  $F[x]/(p(x))$  is a field containing (an isomorphic copy of)  $F$  and a root of  $p(x)$ .*

*Proof.* Since  $p(x)$  is irreducible, the principle ideal  $I = (p(x))$  is a nonzero prime ideal; since  $F[x]$  is a PID,  $I$  is a maximal ideal, and so  $E = F[x]/I$  is a field. Now the map  $a \mapsto a + I$  is an isomorphism from  $F$  to  $F' = a + I : a \in F \subset E$ .

Let  $\theta = x + I \in E$ ; we claim that  $\theta$  is a root of  $p(x)$ . Write  $p(x) = a_0 + a_1x + \dots + a_nx^n$ , where  $a_i \in F$ . Then, in  $E$

$$\begin{aligned} p(\theta) &= (a_0 + I) + (a_1 + I)\theta + \dots + (a_n + I)\theta^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \dots + (a_n + I)(x + I)^n \\ &= (a_0 + I) + (a_1x + I) + \dots + (a_nx^n + I) \\ &= a_0 + a_1x + \dots + a_nx^n + I \\ &= p(x) + I \\ &= I, \end{aligned}$$

because  $I = (p(x))$ . But  $I = 0 + I$  is the zero element of  $F[x]/I$ , and hence  $\theta$  is a root of  $p(x)$ .  $\square$

*Remark 2.2.* One usually identifies  $F$  with the subfield  $F'$  of  $E$  in xxx. Henceforth, whenever there is an embedding of a field  $F$  into a field  $E$ , we say that  $E$  is an extension of  $F$ .

**Proposition 2.7** (Kronecker Theorem). *Let  $f(x) \in F[x]$ , where  $F$  is a field. There exists an extension  $E$  of  $F$  in which  $f(x)$  has a root.*

*Proof.* The proof is by induction on the degree of  $\partial(f(x))$ . If  $\partial(f(x)) = 1$ , then  $f(x)$  is linear and we can choose  $E = F$ . If  $\partial(f(x)) > 1$ , write  $f(x) = p(x)g(x)$ , where  $p(x)$  is irreducible. xxx provides a field  $B$  containing  $F$  and a root  $\theta$  of  $p(x)$ . Hence  $p(x) = (x - \theta)h(x)$  in  $B[x]$ . By induction, there is a field  $E$  containing  $B$  in which  $h(x)g(x)$ , hence  $f(x)$  has a root.  $\square$

**Proposition 2.8.** *Let  $F$  be a field. Let  $p(x)$  be an irreducible polynomial in  $F[x]$  and  $u$  be a root of  $p(x)$  in an extension  $E$  of  $F$ . Then*

(i)  $F(u)$ , the subfield of  $E$  generated by  $F$  and  $u$  is the set

$$F[u] = \{b_0 + b_1u + \cdots + b_mu^m \in E : b_0 + b_1x + \cdots + b_mx^m \in F[x]\}$$

(ii) *If the degree of  $p(x)$  is  $n$ , the set  $\{1, u, \dots, u^{n-1}\}$  forms a basis of  $F(u)$  over  $F$ ; that is, each element of  $F(u)$  can be written uniquely as  $c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$ , where  $c_i \in F$  and  $[F(u) : F] = n$ .*

*Proof.* Let  $p(x)$  be an irreducible polynomial in  $F[x]$  having a root, say  $u$ , in an extension  $E$  of  $F$ . We denote by  $F(u)$  the subfield of  $E$  generated by  $F$  and  $u$  that is, the smallest subfield of  $E$  containing  $F$  and  $u$ . Consider the mapping  $\phi : F[x] \rightarrow E$  defined by

$$\phi(b_0 + b_1x + \cdots + b_mx^m) = b_0 + b_1u + \cdots + b_mu^m,$$

where  $b_0 + b_1x + \cdots + b_mx^m \in F[x]$ . Obviously,  $\phi$  is a homomorphism whose kernel contains  $p(x)$ , because  $p(u) = 0$ . We show that  $\text{Ker}\phi = (p(x))$ .

Because  $F[x]$  is a PID,  $\text{Ker}\phi = (g(x))$  for some  $g(x) \in F[x]$ . Then  $p(x) \in \text{Ker}\phi$  implies  $p(x) = g(x)h(x)$  for some  $h(x) \in F[x]$ . Because  $p(x)$  is irreducible over  $F$ ,  $h(x) \in F$ . Thus  $\text{Ker}\phi = (g(x)) = (p(x))$ .

By xxx,

$$\begin{aligned} F[x]/(p(x)) &\cong \text{Im}\phi \\ &= \{b_0 + b_1u + \cdots + b_mu^m \in E : b_0 + b_1x + \cdots + b_mx^m \in F[x]\} \\ &= F[u], \end{aligned}$$

say. Because  $F[x]/(p(x))$  is a field, the set  $F[u]$  is a field. Obviously  $F[u]$  is the smallest subfield of  $E$  containing  $F$  and  $u$ , so  $F(u) = F[u]$ . If the degree of  $p(x)$  is  $n$ , then  $u$  cannot satisfy any polynomial in  $F[x]$  of degree less than  $n$ . This shows that the set

$$\{1, u, \dots, u^{n-1}\}$$

forms a basis of  $F(u)$  over  $F$ , and  $[F(u) : F] = n$ .  $\square$

## 2.3 Algebraic Extensions

**Definition 2.4.** Let  $E$  be an extension of a field  $F$ . An element  $\alpha \in E$  is said to be algebraic over  $F$  if there exist elements  $a_0, \dots, a_n$  ( $n \geq 1$ ) of  $F$ , not all equal to 0, such that

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0.$$

In other words, an element  $\alpha \in E$  is algebraic over  $F$  if there exists a nonconstant polynomial  $p(x) \in F[x]$  such that  $p(\alpha) = 0$ .

**Theorem 2.9.** Let  $E$  be an extension of a field  $F$ , and let  $u \in E$  be algebraic over  $F$ . Let  $p(x) \in F[x]$  be a polynomial of the least degree such that  $p(u) = 0$ . Then

- (i)  $p(x)$  is irreducible over  $F$ .
  - (ii) If  $g(x) \in F[x]$  is such that  $g(u) = 0$ , then  $p(x)|g(x)$ .
  - (iii) There is exactly one monic polynomial  $p(x) \in F[x]$  of least degree such that  $p(u) = 0$ .
- Proof.* (i) Let  $p(x) = p_1(x)p_2(x)$ , and  $\partial(p_1(x)), \partial(p_2(x))$  be less than  $\partial(p(x))$ . Then  $0 = p(u) = p_1(u)p_2(u)$ . This gives  $p_1(u) = 0$  or  $p_2(u) = 0$ ; that is,  $u$  satisfies a polynomial of degree less than that of  $p(x)$ , a contradiction. So  $p(x)$  is irreducible over  $F$ .
- (ii) By the division algorithm  $g(x) = p(x)q(x) + r(x)$ , where  $r(x) = 0$  or  $\partial(r(x)) < \partial(p(x))$ . Then  $g(u) = p(u)q(u) + r(u)$ ; that is,  $r(u) = 0$ . Because  $p(x)$  is of the least degree among the polynomials satisfied by  $u$ ,  $r(x)$  must be 0. Thus,  $p(x)|g(x)$ .
- (iii) Let  $g(x)$  be a monic polynomial of least degree such that  $g(u) = 0$ . Then by (ii)  $p(x)|g(x)$  and  $g(x)|p(x)$ , which gives  $p(x) = g(x)$  since both are monic polynomials. □

**Definition 2.5.** The monic irreducible polynomial in  $F[x]$  of which  $u$  is a root will be called the minimal polynomial of  $u$  over  $F$ .

**Definition 2.6.** An extension  $E$  of a field  $F$  is called algebraic if each element of  $E$  is algebraic over  $F$ .

Extensions that are not algebraic are called transcendental extensions.

**Theorem 2.10.** If  $E/F$  is a finite extension, then it is an algebraic extension.

*Proof.* Assume that  $[E : F] = n$  and  $\alpha \in E$ . In any  $n$ -dimensional vector space, any sequence of  $n + 1$  vectors is linearly dependent. There are thus scalars  $c_i \in F$  for  $i = 0, 1, \dots, n$ , not all 0, with

$$\sum_{i=0}^n c_i \alpha^i = 0;$$

there is thus a nonzero polynomial in  $F[x]$  having  $\alpha$  as a root, and so  $\alpha$  is algebraic over  $F$ .  $\square$

*Remark 2.3.* Not every algebraic extension is finite.

**Example 1.** Define the algebraic numbers  $\mathbb{A}$  to be the set of all those complex numbers that are algebraic over  $\mathbb{Q}$ . Then  $\mathbb{A}/\mathbb{Q}$  is an algebraic extension that is not finite.

**Definition 2.7.** An extension  $E/F$  is finitely generated if there are elements  $\alpha_1, \alpha_2, \dots, \alpha_k$  in  $E$  such that  $E = F(\alpha_1, \alpha_2, \dots, \alpha_k)$ .

*Remark 2.4.* A finitely generated extension need not be algebraic.

**Example 2.** Let  $f(x)$  be a polynomial ring over a field  $F$  in a variable  $x$ . Consider the field of quotients  $E$  of  $F[x]$ . The elements of  $E$  are of the form

$$(a_0 + a_1x + \cdots + a_mx^m)(b_0 + b_1x + \cdots + b_nx^n)^{-1},$$

where  $a_i, b_i \in F$  and not all  $b_i$  are zero. Thus,  $E$  is generated by  $x$  over  $F$ ; that is,  $E = F(x)$ . Clearly, by the definition of a polynomial ring,  $x$  cannot be algebraic over  $F$ . Hence,  $E$  is not an algebraic extension.

**Theorem 2.11.**

### 3 Normal and Separable Extensions

### 4 Galois Theory

## **References**

[1]