Fields and Galois Theory
File name: `ktt.tex`

Utkan Utkaner

May 2, 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 $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ be the natural map, and consider the ring map $\varphi^* : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ reducing coefficients mod p. Now

$$\varphi^*(f(x)g(x)) = \varphi^*(f(x))\varphi^*(g(x)).$$

But $\varphi^*(f(x)g(x)) = 0$ in $\mathbb{Z}_p[x]$ while $\varphi^*(f(x)) \neq 0$ and $\varphi^*(g(x)) \neq 0$, 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 irreducible over $\mathbb{Z}$, then it is also irreducible over $\mathbb{Q}$.*

Proof. The proof is by contrapositive. 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 $f(x) = (\frac{a}{b})u'(x)v'(x)$, where $\frac{a}{b} \in \mathbb{Q}$ and $u'(x)$ 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 $\mathbb{Z}$. Having proved the contrapositive, we can then infer that the original statement is true. $\square$

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. If $f(x)$ has a root $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$ and $\alpha | a_0$.*

Proof. Write $\alpha = \frac{c}{d}$, where $c, d \in \mathbb{Z}$ and $(c, d) = 1$. Then

$$a_0 + a_1(\frac{c}{d}) + \cdots + a_{n-1}(\frac{c^{n-1}}{d^{n-1}}) + \frac{c^n}{d^n} = 0.$$

Multiply the above equation by d^{n-1} to obtain

$$a_0d^{n-1} + a_1cd^{n-2} + \cdots + a_{n-1}c^{n-1} = -\frac{c^n}{d}.$$

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

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 $p^2 \nmid a_0$, $p|a_1, \ldots, p|a_{n-1}$, $p \nmid a_n$, 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 xxx, $f(x)$ 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 E and E' are extensions of a field F, an F-homomorphism of E into E' or an embedding of E in E' over F is a homomorphism $\varphi : E \to E'$ such that $\varphi(c) = c$ for all $c \in F$.

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

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

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of E/K, and let $\{\beta_1, \dots, \beta_m\}$ be a basis of K/F. It suffices to prove that $\{\beta_j\alpha_i : 1 \le i \le n, 1 \le j \le m\}$ is a basis of E/F.

This set spans E. If $\gamma \in E$; then there are b_i in K 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 $b_i = \sum c_{ij}\beta_j \in K$, so that independence of the α_i over K implies that $b_i = 0$ for all i. Hence $\sum c_{ij}\beta_j = 0$ for all i, and so the independence of the β_j over F implies that $c_{ij} = 0$ for all i, j, as desired. □

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

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

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

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 $f(x)$. If $\partial(f(x)) = 1$, then $f(x)$ is linear and we can choose $E = F$. If $\partial(f(x)) > 1$, write $f(x) = p(x)u(x)$, where $p(x)$ is irreducible. xxx provides a field B containing F and a root α of $p(x)$. Hence $p(x) = (x - \alpha)v(x)$ in $B[x]$. By induction, there is a field E containing B in which $v(x)u(x)$, hence $f(x)$ has a root. □

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

(i) $F(\alpha)$, the subfield of E generated by F and α is the set

$$F[\alpha] = \{b_0 + b_1\alpha + \cdots + b_m\alpha^m \in E : b_0 + b_1x + \cdots + b_mx^m \in F[x]\}$$

(ii) If the degree of $p(x)$ is n, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis of $F(\alpha)$ over F; that is, each element of $F(\alpha)$ can be written uniquely as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, where $a_i \in F$ and $[F(\alpha) : F] = n$.

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

$$\varphi(b_0 + b_1x + \cdots + b_mx^m) = b_0 + b_1\alpha + \cdots + b_m\alpha^m,$$

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

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

By xxx,

$$\begin{aligned} F[x]/(p(x)) &\cong \mathrm{Im}\varphi \\ &= \{b_0 + b_1\alpha + \cdots + b_m\alpha^m \in E : b_0 + b_1x + \cdots + b_mx^m \in F[x]\} \\ &= F[\alpha], \end{aligned}$$

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

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

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

2.3 Algebraic Extensions

Definition 2.4. Let E be an extension of a field F. An element $\alpha \in E$ is algebraic over F if there exists a nonconstant polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.

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

(i) $f(x)$ is irreducible over F.

(ii) If $g(x) \in F[x]$ is such that $g(\alpha) = 0$, then $f(x)|g(x)$.

(iii) There is exactly one monic polynomial $f(x) \in F[x]$ of least degree such that $f(\alpha) = 0$.

Proof. (i) Let $f(x) = u(x)v(x)$, and $\partial(u(x))$, $\partial(v(x))$ be less than $\partial(f(x))$. Then $0 = f(\alpha) = u(\alpha)v(\alpha)$. This gives $u(\alpha) = 0$ or $v(\alpha) = 0$; that is, α satisfies a polynomial of degree less than that of $f(x)$, a contradiction. So $f(x)$ is irreducible of F.

(ii) By the division algorithm $g(x) = f(x)q(x) + r(x)$, where $r(x) = 0$ or $\partial(r(x)) < \partial(f(x))$. Then $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$; that is, $r(\alpha) = 0$. Because $f(x)$ is of the least degree among the polynomials satisfied by α, $r(x)$ must be 0. Thus, $f(x)|g(x)$.

(iii) Let $g(x)$ be a monic polynomial of least degree such that $g(\alpha) = 0$. Then by *(ii)* $f(x)|g(x)$ and $g(x)|f(x)$, which gives $f(x) = g(x)$ since both are monic polynomials.

□

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

Proposition 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 $a_i \in F$ for $i = 0, 1, \ldots, n$, not all 0, with

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

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

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* $\mathbb{Q}$. *Than* $\mathbb{A}/\mathbb{Q}$ *is an algebraic extension that is not finite.*

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

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*

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

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.*

Proposition 2.11. *Let* $E = F(\alpha_1, \ldots, \alpha_n)$ *be a finitely generated extension of* F *such that each* α_i, $i = 1, \ldots, n$, *is algebraic over* F. *Then* E *is finite over* F *and, hence, an algebraic extension of* F.

Proof. Set $E_i = F(\alpha_1, \ldots, \alpha_i)$, $1 \leq i \leq n$. Observe that if an element in E is algebraic over a field F, then, trivially, it is algebraic over any field B such that $F \subset B \subset E$. Therefore, each α_i is algebraic over E_{i-1}, $i = 1, \ldots, n$, with $E_0 = F$. Also, $E_i = E_{i-1}(\alpha_i)$. Therefore, by xxx, $[E_i : E_{i-1}]$ is finite, say d_i. By xxx,

$$[E : F] = [E : E_{n-1}][E_{n-1} : E_{n-2}] \ldots [E_1 : F];$$

hence,

$$[E : F] = d_n d_{n-1} \ldots d_1.$$

Thus, E is a finite extension of F and therefore algebraic over F. □

Proposition 2.12. *Let* E *be an extension of* F. *If* K *is the subset of* E *consisting of all the elements that are algebraic over* F, *then* K *is a subfield of* E *and an algebraic extension of* F.

Proof. We need only show that if $\alpha, \beta \in E$ and are algebraic over F, then $\alpha \pm \beta, \alpha\beta$ and $\alpha\beta^{-1}$(if $\beta \neq 0$) are also algebraic over F. This follows from the fact that all these elements lie in $F(\alpha, \beta)$, which by xxx, is an algebraic extension of F.

Thus, K is an algebraic extension of F in E. □

2.4 Algebraically Closed Fields

Definition 2.8. A field F is algebraically closed if it possesses no proper algebraic extensions.

Definition 2.9. A field E is an algebraic closure of a subfield F if it is algebraically closed and algebraic over F.

Proposition 2.13. *Let F be a field. Then there is an extension E of F that is algebraically closed.*

Proof. The following proof is due to Emil Artin. The first step is to construct an extension field F_1 of F, with the property that all nonconstant polynomials in $F[x]$ have a root in F_1. To this end, for each nonconstant polynomial $p(x) \in F[x]$, let x_p be an independent variable and consider the ring R of all polynomials in the variables x_p over the field F. Let I be the ideal generated by the polynomials $p(x_p)$. We contend that I is not the entire ring R. For if it were, then there would exist polynomials $q_1, \dots, q_n \in R$ and $p_1, \dots, p_n \in I$ such that

$$q_1 p_1(x_{p_1}) + \cdots + q_n p_n(x_{p_n}) = 1.$$

This is an algebraic expression over F in a finite number of independent variables. But there is an extension field E of F in which each of the polynomials $p_1(x), \dots, p_n(x)$ has a root, say $\alpha_1, \dots, \alpha_n$. Setting $x_{p_i} = \alpha_i$ and setting any other variables appearing in the equation above equal to 0 gives $0 = 1$. This contradiction implies that $I \neq R$.

Since $I \neq E$, there exists a maximal ideal J such that $I \subseteq J \subset R$. Then $F_1 = R/J$ is a field in which each polynomial $p(x) \in F[x]$ has a root, namely $x_p + J$. (We may think of F_1 as an extension of F by identifying $\alpha \in F$ with $\alpha + J$.)

Using the same technique, we may define a tower of extensions

$$F/F_1/F_2/\dots$$

such that each nonconstant polynomial $p(x) \in F_i[x]$ has a root in F_{i+1}. The union $E = \bigcup F_i$ is an extension field of F. Moreover, any polynomial $p(x) \in E[x]$ has all of its coefficients in F_i for some i and so has a root in F_{i+1}, hence in E. It follows that every polynomial $p(x) \in E[x]$ factors into linear factors over E. Hence E is algebraically closed.

$\square$

Proposition 2.14. *Let E/F be an extension where E is algebraically closed. Then the collection of elements K of E that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to homomorphism.*

Proof. By xxx, K is an algebraic extension of F. Let $f(x) \in K[x]$. Then $f(x)$ has a root $\alpha \in E$ because E is algebraically closed. But then $\alpha \in E$ is algebraic over K, and because K is algebraic over F, we obtain, that α is algebraic over F. Hence, $\alpha \in K$. Thus, K is algebraically closed, which proves that K is an algebraic closure of F. $\square$

Lemma 2.15. *Let f be a field and let $\varphi : F \to E$ be an embedding of F into an algebraically closed field E. Let $K = F(\alpha)$ be an algebraic extension of F. Then φ can be extended to an embedding $\phi : K \to E$, and the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α.*

Proof. Let $p(x) = a_0 + a_1 + \cdots + a_{n-1} + a_n$ be the minimal polynomial of α over F. Let

$$p^{\varphi}(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_{n-1})x^{n-1} + x^n \in E[x].$$

Let β be a root of $p^{\varphi}(x)$ in E. Recall that if α is algebraic over a field F, then a typical element of the field $F(\alpha)$ can be written uniquely as $b_0+b_1\alpha+\cdots+b_m\alpha^m$, where m ¡ degree of the minimal polynomial of α over F, and $b_i \in F$, $i = 1, \ldots, m$.

Define $\phi : F(\alpha) \to E$ by the rule

$$\phi(b_0 + b_1\alpha + \cdots + b_m\alpha^m) = \varphi(b_0) + \varphi(b_1)\beta + \cdots + \varphi(b_m)\beta^m.$$

Then ϕ is a well defined mapping. Routine computation shows that ϕ is a homomorphism. Thus ϕ is an embedding of $F(\alpha)$ into E, and it extends φ. Clearly, there is a 1-1 correspondence between the set of distinct roots of $p^{\varphi}(x)$ in E and the set of embeddings ϕ of $F(\alpha)$ into E that extends φ. This proves the last assertion. □

Proposition 2.16. *Let K be an algebraic extension of a field F, and let $\varphi : F \to E$ be an embedding of F into an algebraically closed field E. Then φ can be extended to an embedding $\phi : K \to E$.*

Proof. Let S be the set of all pairs (L, Φ), where L is a subfield of K containing F, and Φ is an extension of φ to an embedding of L into E. If (L, Φ) and (L', Φ') are in S, we write $(L, \Phi) \leq (L', \Phi')$ if $L \subset L'$ and Φ' restricted to L is Φ. Because $(F, \varphi) \in S$, $S \neq \varnothing$. Also, if $\{(L_i, \Phi_i)\}$ is a chain in S, we set $L = \bigcup L_i$ and define Φ on L as follows. Let $a \in L$. Then $a \in L_i$ for some i, and we define $\Phi(a) = \Phi_i(a)$. Φ is well defined. Let $a \in L_i$ and $a \in L_j$. Because either $L_i \subset L_j$ or $L_j \subset L_i$ by definition of a chain in S, we get $\Phi_i(a) = \Phi_j(a)$. Hence, Φ is well defined. Then (L, Φ) is an upper bound for the chain $\{(L_i, \Phi_i)\}$. Using Zorn's Lemma, let (L, ϕ) be a maximal element in S. Then ϕ is an extension of φ, and we contend that $L = K$. Otherwise, there exists $\alpha \in K$, $\alpha \notin L$. Then by xxx the embedding $\phi : L \to E$ has an extension $\phi^* : L(\alpha) \to E$, thereby contradicting the maximality of (L, ϕ). Hence, $L = K$, which proves the theorem. □

Proposition 2.17. *Let E and E' be algebraic closures of a field F. Then $E \cong E'$ under an isomorphism that is an identity on F.*

Proof. Let $\varphi : F \to E$ be the injection; that is, $\varphi(a) = a$ for all $a \in F$. By xxx, φ can be extended to an embedding $\varphi^* : E' \to E$. Now $E' \cong \varphi^*(E')$. Hence, $\varphi^*(E')$ is also an algebraically closed field containing F. Because E is an algebraic extension of F, E is also an algebraic extension of $\varphi^*(E')$, which lies between F and E. But then $\varphi^*(E') = E$, so φ^* is an isomorphism of E' onto E, as desired. □

3 Normal and Separable Extensions

4 Galois Theory

References

[1]