Fields and Galois Theory

Lectures by Uzi Vishne
Summary by Ari Feiglin (ari.feiglin@gmail.com)

Contents

1 Field Extensions

Suppose $F \subseteq K$ are fields, then K is certainly also an F-vector space and therefore has a dimension and we denote it $[K : F] := \dim_F K$.

1.0.1 Theorem

Suppose $F \subseteq K$ and V is a K-vector space, then V is also a vector space over F as well, and $\dim_F V = [K : F] \dim_K V$.

Proof: Let $B_1 \subseteq V$ be a basis for V over K and $B_2 \subseteq K$ be a basis for K over F, then define $B = \{\alpha v \mid \alpha \in B_2, v \in B_1\}$. This is a basis for V in F, it is linearly independent since if $\alpha_1 v_1, \dots, \alpha_n v_n \in B$ and $\beta_1, \dots, \beta_n \in F$ then $\sum_{i=1}^n \beta_i \alpha_i v_i = 0$ implies $\beta_i \alpha_i = 0$ for all i since B_1 is a basis, and this means that β_i or α_i is zero, but $\alpha_i v_i \in B$ so $\beta_i = 0$ as required. B spans V since for $v \in B$ there exist $v_1, \dots, v_n \in B_1$ and $\alpha_1, \dots, \alpha_n \in K$ such that $v = \sum_{i=1}^n \alpha_i v_i$ and α_i can be written as the linear combination of elements in B_2 by elements of F which gives a linear combination of elements in B of F. So B is indeed a basis for V over F. Finally $B \cong B_2 \times B_1$ since $(\alpha, v) \mapsto \alpha v$ is a bijection: it is obviously surjective and $\alpha_1 v_1 = \alpha_2 v_2$ implies $\alpha_1 = \alpha_2, v_1 = v_2$ since v_1, v_2 are independent. Thus we have

$$\dim_F V = |B| = |B_2 \times B_1| = [K : F] \dim_K V$$

■

In particular if $F \subseteq K \subseteq E$ are fields then $[E : F] = [E : K] \cdot [K : F]$.
The following are methods of constructing fields:

(1) If R is a commutative ring and $M \triangleleft R$ is a maximal ideal then ${}^{R}\!/_{M}$ is a field. Specifically if $R = F[x]$ and p is an irreducible polynomial, $\langle p \rangle$ is maximal and ${}^{F[x]}\!/_{\langle p \rangle}$ is a field.

(2) If F is a field, then the set of rational functions is also a field:

$$F \subseteq F(x) := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in F[x \right\},\, g(x) \neq 0]$$

In general if R is an integral domain then its field of fractions/quotients $q(R) := \left\{ \frac{a}{b} \;\middle|\; a, b \in R,\, b \neq 0 \right\}$ is a field. And $F(x)$ is the quotient field of $F[x]$.

(3) If $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ is a chain of fields then so is $\bigcup F_n$ (the theory of fields is inductive, this holds for arbitrary chains, not just inductive ones). So for example $F(\lambda_1, \lambda_2, \dots)$ is a field since we can define $F_n = F(\lambda_1, \dots, \lambda_n)$ (the quotient field of $F[\lambda_1, \dots, \lambda_n]$) and the union of this chain is $F(\lambda_1, \lambda_2, \dots)$.

Let F be a field and $F \subseteq K$ a ring with $a \in K$, we define a homomorphism $F[\lambda] \xrightarrow{\psi_a} K$ defined by $\alpha \mapsto \alpha$ for $\alpha \in F$ and $\lambda \mapsto a$, meaning

$$\psi_a\Big(\sum \alpha_i \lambda^i\Big) = \sum \alpha_i a^i \qquad (\psi_a(f) = f(a))$$

In particular ψ_a is a linear transformation from F to K, and is called the *evaluation homomorphism* at a. The kernel of the homomorphism is

$$\ker \psi_a = \{f \in F[\lambda] \mid f(a) = 0\} \triangleleft F[\lambda]$$

1.0.2 Definition

$a \in K$ is **algebraic** if $\ker \psi_a \neq 0$ and **transcendental** if the kernel is trivial.

If a is transcendental then $\ker \psi_a$ and so $\operatorname{Im} \psi_a = \{f(a) \mid f \in F[\lambda]\} = F[a] \cong F[\lambda]$. In fact we get

$$\begin{array}{ccccccc} F & \subseteq & F[a] & \subseteq & F(a) & \subseteq & K \\ & & \cong & & \cong & & \\ & & F[x] & & F(x) & & \end{array}$$

Now if a is algebraic, since $F[x]$ is a euclidean domain and therefore a PID, the kernel has a generator $\ker \psi_a = \langle h \rangle = h \cdot F[\lambda]$. So $h(a) = 0$ and $f(a) = 0 \implies h|f$, and h is called the *minimal polynomial* of a. And so

$${}^{F[\lambda]}\!\Big/_{\langle h \rangle} = {}^{F[\lambda]}\!\Big/_{\ker \psi_a} \cong \operatorname{Im} \psi_a = \{f(a) \mid f \in F[\lambda]\} = F[a] = \operatorname{span}\{1, a, \dots, a^{n-1}\} \subseteq K$$

where $n = \deg h$, since $f(x) = q(x)h(x) + r(x)$ where $\deg r < \deg h = n$ and so $f(a) = r(a)$. $\{1, \ldots, a^{n-1}\}$ is a basis due to h being minimal, a zeroing linear combination would give a zeroing polynomial of a of degree less than h. This means that the dimension of $F[a]$ as an F-vector space is n, ie. $\big[F[a] : F\big] = n$.

Since K is an integral domain and therefore so too is $F[a]$ and this means that $\langle h\rangle$ is a prime ideal (since $^{R}/_{I}$ is an integral domain if and only if I is prime), this means that h is a prime (irreducible) polynomial. And since $F[a]$ is a PID, prime and maximal ideals are one and the same, so $\langle h\rangle$ is maximal and therefore $^{F[\lambda]}/_{\langle h\rangle} \cong F[a]$ is a field. Let us summarize this:

1.0.3 Proposition

Let $F \subseteq K$ where K is an integral domain and $a \in K$ is algebraic in F, let h_a be its minimal polynomial. Then (1) h_a is irreducible, (2) $F[a]$ is a field, (3) $\big[F[a] : F\big] = \deg h_a$.

So for example let $a \in K \setminus F$ be algebraic then $F \subseteq F[a] \subseteq K$ and suppose $[K : F] = p$ is prime. Then $p = [K : F] = [K : F[a]] \cdot [F[a] : F]$, and since $a \in F[a] \setminus F$ this means $[F[a] : F] > 1$ so $[F[a] : F] = p$ and $[K : F[a]] = 1$ since p is prime so $F[a] = K$.

1.0.4 Corollary

Suppose F is a field and $F \subseteq K$ is an integral domain with finite dimension. Then every element of K is algebraic and K is a field.

Proof: Let $a \in K$ then $[K : F] = [K : F[a]] \cdot [F[a] : F]$ so $[F[a] : F]$ is finite. If a were transcendental then $F[a] \cong F[x]$ and $F[x]$ has infinite dimension over F. K is a field since every $a \in K$ must have a multiplicative inverse, since $F[a]$ is a field. ∎

Notice that $[F[a,b] : F[a]] \leq [F[b] : F]$ since if h_b is b's minimal polynomial in F then it is also a zeroing polynomial in $F[a]$. This means that

$$[F[a,b] : F] = [F[a,b] : F[a]] \cdot [F[a] : F] \leq [F[b] : F] \cdot [F[a] : F]$$

1.0.5 Corollary

Let F be a field and K a field extension, define

$$\mathrm{Alg}_F(K) := \{a \in K \mid a \text{ is algebraic over } F\}.$$

This is a field. Furthermore $F \subseteq \mathrm{Alg}_F(K)$ is an algebraic extension (all elements of $\mathrm{Alg}_F(K)$ are algebraic in F), and $\mathrm{Alg}_F(K) \subseteq K$ is a purely transcendental extension (all elements in $K \setminus \mathrm{Alg}_F(K)$ are transcendental in $\mathrm{Alg}_F(K)$).

Proof: Notice that $F[a \cdot b], F[a+b] \subseteq F[a,b]$ and so $[F[a,b] : F] \leq [F[b] : F] \cdot [F[a] : F] < \infty$, so $\mathrm{Alg}_F(K)$ is closed under addition and multiplication (and obviously additive inverses). For a algebraic, $F[a]$ is a field so $a^{-1} \in F[a]$ and so $F[a^{-1}] \subseteq F[a]$ and therefore $[F[a^{-1}] : F] < \infty$ so a^{-1} is algebraic as well (and so by symmetry $F[a] = F[a^{-1}]$). So $\mathrm{Alg}_F(K)$ is indeed a field.

To show that $\mathrm{Alg}_F(K) \subseteq K$ is a pure transcendental extension, notice that if $F_1 \subseteq F_2 \subseteq F_3$ where $F_1 \subseteq F_2$ is algebraic, if $a \in F_3$ is algebraic in F_2 it is also algebraic in F_1. Indeed if $f \in F_2[x]$ such that $f(a) = 0$, let its coefficients be b_i then a is algebraic in $F_1[b_0, \ldots, b_n]$ and so

$$[F_1[b_0, \ldots, b_n, a] : F_1[b_0, \ldots, b_n]] = [F_1[b_0, \ldots, b_n, a] : F_1[b_0, \ldots, b_n]] \cdot [F_1[b_0, \ldots, b_n] : F_1]$$

and this is finite since $b_0, \ldots, b_n$ are algebraic in F_1 as they are in F_2, so both terms are finite. So if K had any algebraic numbers not in $\mathrm{Alg}_F(K)$, they would be algebraic in F and thus in $\mathrm{Alg}_F(K)$ in contradiction. ∎