Advanced Algebra I

FIELD EXTENSIONS AND ALGEBRAIC CLOSURE

Let K be a subfield of F, then we say that F is an extension over K and denote it by F/K. Recall that F can be viewed as a vector space over K. We say that the extension F/K is finite of infinite according the dimension of F as a vector space over K.

Let F/K be an extension, an element $u \in F$ is said to be *algebraic* over K if there is a non-zero polynomial $f(x) \in K[x]$ such that $f(u) = 0$. In other words, the ring homomorphism

$$\varphi : K[x] \to F,$$

$$f(x) \mapsto f(u)$$

has a non-zero kernel. Let I be the kernel. Since $K[x]$ is a PID, $I = (p(x))$ for some $p(x)$. Let $K[u]$ be the image of φ, then

$$K[x]/(p(x)) \cong K[u] \subset F.$$

It's easy that $(p(x))$ is a prime ideal , that is, $p(x)$ is irreducible. We may assume that $p(x)$ has leading coefficient 1. Such $p(x)$ is called the minimal polynomial of u over K.

We say that F/K is algebraic if every element of F is algebraic over K.

Let's recall some more properties. If F/K, then we denote $[F : K]$ to be the dimension $\dim_K F$.

Proposition 0.1. *If E/F and F/K, then $[E : F][F : K] = [E : K]$.*

Sketch of the proof. Let $\{u_i\}_{i\in I}$ be a basis of E/F and $\{v_j\}_{j\in J}$ be a basis of F/K. Then one can prove that $\{u_i v_j\}_{(i,j)\in I\times J}$ is a basis of E/K. Hence

$$[E : K] = |I \times J| = |I| \cdot |J| = [E : F] \cdot [F : K].$$

□

Proposition 0.2. *Suppose that we have a tower of fields $K \subset F \subset E$. Then E is finite over K if and only if E is finite over F and F is finite over K.*

Proof. Easy corollary of the previous proposition. □

Proposition 0.3. *If F/K is finite, then F/K is algebraic.*

Proof. suppose that $[F : K] = n$. For any $u \neq 0 \in F$, then $\{1, u, ..., u^n\}$ is linearly dependent over K. Thus there are $a_0, ..., a_n \in K$ non all zero such that $\sum_{i=0}^{n} a_i u^i = 0$. It follows that u satisfies the polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$. □

Let F/K be an extension, and $u \in F$. We denote by $K(u)$ the smallest subfield of F containing K and u. It's easy to see that

$$K(u) = \{\frac{f(u)}{g(u)} | f(x), g(x) \in K[x], g(u) \neq 0\}.$$

Similarly, for $S \subset F$, we denote by $K(S)$ the smallest subfield containing both K and S. If $F = K(S)$ for a finite set S, then F is said to be *finitely generated* over K.

Proposition 0.4. *Let F/K be an extension. Then $u \in F$ is algebraic over K if and only if $K(u) = K[u]$. And in the algebraic case, $[K[u] : K] = deg(p(x))$, where $p(x)$ is the minimal polynomial.*

Sketch of the proof. If $u \in F$ is algebraic over K, let $p(x)$ be the minimal polynomial. One sees that $g(u) \neq 0$ if and only $(g(x), p(x)) = 1$. There are $s(x), t(x)$ such that

$$1 = s(x)g(x) + t(x)p(x),$$

hence $1 = s(u)g(u)$. One has $\frac{f(u)}{g(u)} = f(u)s(u)$ and hence $K(u) \subset K[u]$.

Conversely, $\frac{1}{u} \in K(u) = K[u]$. Thus $\frac{1}{u} = f(u)$ for some $f(x) \in K[x]$. One sees that u satisfies $xf(x) - 1$. □

Proposition 0.5. *F/K is finite if and only if F/K is finitely generated and algebraic.*

Sketch of the proof. If F/K is finite, let $\{u_1, ..., u_n\}$ be a basis of F/K, then $F = K(u_1, ..., u_n)$ hence is finitely generated.

Conversely, suppose that $F = K(u_1, ..., u_n)$ is algebraic over K. In particular, each u_i is algebraic over K. In particular, u_1 is algebraic over K, u_2 is algebraic over $K(u_1)$, and so on. Then one has that

$$[K(u_1, ..., u_n) : K] = [K(u_1, ..., u_n) : K(u_1, ..., u_{n-1})] \cdot [K(u_1, ..., u_{n-1}) : K]$$

is finite by induction. □

Proposition 0.6. *Suppose that we have a tower of fields $K \subset F \subset E$. Then E is algebraic over K if and only if E is algebraic over F and F is algebraic over K.*

Sketch of the proof. We will only prove that E is algebraic over F and F is algebraic over K implies that E is algebraic over K. The remaining statement are easy.

Pick any $u \in E$. Since u is algebraic over F, let $f(x) = \sum a_i x^i$ be the minimal polynomial of u over F.

We then consider the field $F' := K(a_0, ..., a_n)$. It's clear that u satisfies a polynomial $f(x) \in F'$. It follows that $u \in F'(u)$ which is finite over K. Therefore, u is algebraic over K. □

Let L/K and M/K are extensions over K and both L, M are contained in a field F. We denote by LM the smallest subfield containing both L and M. LM is called the compositum of L and M.

A useful remark is that if $L = K(S)$ for some $S \subset L$, then $LM = M(S)$.

For a certain property of field extension, denoted $\mathcal{C}$, we are interested whether $\mathcal{C}$ is preserved after extension, lifting or compositum. More precisely, we would like to know a property $\mathcal{C}$ satisfying the following conditions:

(1) (extension) Both E/F and F/K are $\mathcal{C}$ if and only if E/K is $\mathcal{C}$.
(2) (lifting/ base change) If E/K is $\mathcal{C}$, then EF/F is $\mathcal{C}$.
(3) (compositum) If both $E/K, F/K$ are $\mathcal{C}$, then EF/K is $\mathcal{C}$.

Proposition 0.7. *The property of being finite or algebraic satisfying the above three.*

Sketch of the proof. It's easy to that being finite and finitely generated satisfies the above three statement. Hence so does being algebraic. $\square$