Nov. 3, 2006 (Fri.)

3. FIELD THEORY

3.1. **definitions and basic properties.** A field F is a set together two binary operation $+, *$ such that $(F, +)$ is an abelian group with identity 0, $(F^* := F - \{0\}, *)$ is an abelian group with identity 1, and satisfying $a * (b + c) = a * b + a * c$.

Let E, F be fields, a homomorphism of fields is nothing but a ring homomorphism $\varphi : E \to F$. Note that $\varphi(1_E) = 1_F$

Example 3.1.1.

Let p be a prime. Then $\mathbb{Z}_p$ is a field. Let F be a field of p elements, then clearly there is an isomorphism $F \cong \mathbb{Z}_p$ (by sending $1_{\mathbb{Z}_p}$ to 1_F). Thus we usually say *the* field of p-elements and denoted $\mathbb{F}_p$. □

Give a field F, let P be its minimal (non-zero) subfield. Then we have:

Proposition 3.1.2. *P is isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$.*

Proof. Consider the additive subgroup H generated by 1_F, then H is either $\mathbb{Z}$ or $\mathbb{Z}_p$. If it's $\mathbb{Z}_p$ then this is exactly P. And if $H = \mathbb{Z}$, then one can show that $P \cong \mathbb{Q}$. □

Definition 3.1.3. *The minimal subfield if called the* **prime field** *of F. If the prime field is $\mathbb{F}_p$, then we say that F has characteristic p, denoted $\mathrm{char}(F) = p$. Otherwise, we say that F has characteristic 0, denoted $\mathrm{char}(F) = 0$.*

The most important feature for field of characteristic p is that it has a non-trivial *Frobenius map* $\varphi : F \to F, \varphi(x) \mapsto x^p$. To verify that this is an homomorphism, we need to check that $\varphi(x) + \varphi(y) = \varphi(x + y)$. Note that $px = 0$ for all $x \in F$ and thus $nx = 0$ for all n divisible by p. It follows that $C_i^p x = 0$ for all $0 < i < p$ and all $x \in F$. Hence $(x + y)^p = x^p + y^p$.

In fact, the FRobenius map is always injective for if $x^p = y^p$, then $x^p - y^p = (x - y)^p = 0$. Thus $x - y = 0$.

Example 3.1.4.

We have the following important construction of fields. Let F be a field, $F[x]$ be the polynomial ring. Let $p(x) \in F[x]$ be an irreducible polynomial. We claim that $F[x]/(p(x))$ is a field.

Recall that there is a division algorithm on $F[x]$. That is, given $f(x), g(x) \neq 0 \in F[x]$, there exist $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ with either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$. (This shows that $F[x]$ is an Euclidean domain (E.D.).)

With this properties, one can show that every ideal is of the form $(f(x))$, i.e. $F[x]$ is a principal ideal domain (PID). For a given ideal

$I \lhd F[x]$, this can be achieved by pick $f(x) \in I$ of minimal degree. For any $g(x) \in I$, performing the division algorithm, one sees that $r(x) = 0$ for otherwise one gets a polynomial of even smaller degree, which is absurd.

One method is to show that $(p(x))lhdF[x]$ is a maximal ideal. Suppose we have $(p(x)) < \mathfrak{m} \lneq F[x]$. Since $\mathfrak{m} = (f(x))$, it follows that $p(x) \in (f(x))$ and thus $p(x) = f(x)g(x)$. $p(x)$ is irreducible implies that $f(x) = cp(x)$ for some $c \in F$. Anyway, $(p(x)) = (f(x))$.

Or explicitly, a non-zero element in $F[x]/(p(x))$ is of the form $\overline{f(x)}$ for some $f(x) \in F[x]$ and $f(x) \notin (p(x))$. Thus $(f(x), p(x)) = 1$. By the division algorithm, there exists $s(x), t(x)$ such that $1 = s(x)f(x) + t(x)p(x)$. Hence $\overline{f(x)s(x)} = 1$.

If $n = deg(p(x))$, then the element in the field $F[x]/(p(x))$ can be written as $\{a_0 + a_1\bar{x} + ...a_{n-1}\bar{x}^{n-1}\}$. □

Before we move on, we need the following facts.

Proposition 3.1.5. *Let $f(x) \in F[x]$ be a polynomial of degree n, then there are at most n roots in F.*

Proof. a is said to be a root of $f(x)$ if $f(a) = 0$. Note that, by division algorithm, $f(x) = q(x)(x-a)+r(x)$ with $r(x) = 0$ or $deg(r(x)) = 0$. a is a root if and only if $r(x) = 0$ if and only if $(x-a)|f(x)$. Inductively and by the unique factorization of $F[x]$. One sees that there are at most n roots. □

Proposition 3.1.6. *Let $G < F^*$ be a finite group. Then G is cyclic.*

Proof. By Corollary 2.7.8, $G \cong \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_d}$. Note that, on the right hand side, $m_d x = 0$ for all x. Thus $a^{m_d} = 1$ for all $a \in G$. (On G, we use multiplicative notations, while right hand side is additive). Thus every element in G is a root of $x^{m_d} - 1$. So we have

$$|G| = m_1...m_d \leq m_d.$$

This is possible only when $d = 1$. □

3.2. **field extensions.** 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 3.2.1. *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 3.2.2. *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 3.2.3. *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 3.2.4. *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 3.2.5. *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 3.2.6. *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 $f(x) \in F'[x]$. 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 3.2.7. *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. □

Theorem 3.2.8. *Let F be an extension over K, and E the set of all elements in F which is algebraic over K. Then E is a field.*

Proof. If $u, v \in E$, we need to show that $u + v, uv \in E$. Note that $u + v, uv \in K(u, v)$ and $K(u, v)/K$ is finitely generated and algebraic, hence finite. It follows that both $u + v, uv$ are algebraic over K. $\square$

Example 3.2.9.

Consider $\mathbb{C}/\mathbb{Q}$. A number $u \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$ is called an algebraic number. The set of all algebraic numbers, denoted $\mathcal{A}$, is a field, algebraic but not finite over $\mathbb{Q}$.