Nov. 17, 2006

3.5. **splitting fields and normal extensions.** We have seen that given a field K, there is a unique (up to isomorphism) algebraic closure, denoted $\overline{K}$. Then it is convenient for our further study of roots of polynomial. Even though we do not know the roots explicitly, we know that there are *in* its algebraic closure. This make the discussion of root of polynomials more concrete.

Let K be a field and $f(x) \in K[x]$. Let $\{u_1, ..., u_r\}$ be the roots of $f(x)$ in its algebraic closure $\overline{K}$. Then the field $K(u_1, ..., u_r)$ is called the **splitting field of** $f(x)$ **over** K. The splitting field is the smallest field that containing all roots.

Given a set of polynomial $S \subset K[x]$, we can similarly define the splitting field of S to be the field generated by all roots of polynomials in S.

In this section, we are going to prove the existence and uniqueness of splitting fields. And we introduce the notion of normal extension.

Proposition 3.5.1. *Let K be a field. And S be a set of polynomial in $K[x]$. Then*

1. *Any two splitting field are isomorphic.*
2. *If F_1, F_2 are two splitting fields in a fixed algebraic closure $\overline{K}$, then $F_1 = F_2$.*

Proof. Let F_1 and F_2 be two splitting fields, one has an K-embedding $\sigma : K \to \overline{F_2} = \overline{K}$. This embedding can be extended to $\tilde{\sigma} : F_1 \to \overline{F_2}$ by the extension theorem. One can prove that image of $\tilde{\sigma}$ is in F_2. Hence one has an injective homomorphism $\tilde{\sigma} : F_1 \to F_2$. Similarly there is another one $\tilde{\tau} : F_2 \to F_1$. It's easy to show that these give the isomorphism. □

Proposition 3.5.2. *Let N be an algebraic extension over K contained in $\overline{K}$. Then the following are equivalent:*

1. *Any K-embedding $\sigma : N \to \overline{K}$ induces an K-automorphism of N.*
2. *N is a splitting field of some $S \subset K[x]$ over K.*
3. *Every irreducible polynomial in $K[x]$ having a root in N splits in N.*

Proof. For $(1) \Rightarrow (2), (3)$, we prove that for every $u \in N$, with minimal polynomial $p(x)$, then $v \in N$ for every root of $p(x)$. To this end, start with an isomorphism $\sigma : K(u) \to K(v)$. By extension theorem, one can extend it to an embedding $N \to \overline{K(v)} = \overline{K}$. The embedding is an automorphism by (1). Thus, $v = \sigma(u) \in N$.

$(3) \Rightarrow (2)$ is trivial.

For $(2) \Rightarrow (1)$. Suppose that N is a splitting field of S over K. Let u be a root of $f(x) \in S$. Let $\sigma : N \to \overline{K}$ be any K-embedding. It's clear that $\sigma(u)$ is a root of $f(x)$, hence $\sigma(u) \in N$. Thus $\sigma(N) \subset N$. Since σ is injective and N/K is algebraic, σ is in fact an isomorphism. $\square$

The property of being normal is not as well-behaved as begin algebraic or finite. For example, it's not preserve after "extension"

Example 3.5.3. *If F/E and E/K are normal, then F/K is not necessarily normal. For example, take $F = \mathbb{Q}(\sqrt[4]{2}), E = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}$. It's easy to see that a degree 2 extension is always normal, however, $\mathbb{Q}(\sqrt[4]{2})$ is not normal over $\mathbb{Q}$.*

Also let's consider $K \subset E \subset F$. Then F is normal over K implies that F is normal over E. But it doesn't imply that E is normal over K. For example, take $F = \mathbb{Q}(\sqrt[4]{2}, i), E = \mathbb{Q}(\sqrt[4]{2}), K = \mathbb{Q}$

Being normal is preserved by "lifting" and "compositum"

Proposition 3.5.4. *Let E, F be extensions over K and contained in a field L. If E/K is normal then EF/F is normal. Moreover, if both $E/K, F/K$ are normal, then EF/K is normal.*

Proof. In order to show that EF is normal over F, we look at F-embedding $\sigma : EF \to \overline{F}$. Since σ is identity on F, hence on K. By the extension theorem and the proof of the previous Proposition, one can show that $\sigma_{|E}$ is an automorphism. Hence $\sigma(E) = E$. It follows that

$$\sigma(EF) = \sigma(E)F = EF.$$

Thus EF is normal over F.

Suppose now that $E/K, F/K$ are normal. Let $\sigma : EF \to \overline{K}$ be a K-embedding. We have that $\sigma_{|E}, \sigma_{|F}$ are K-embeddings. One sees that $\sigma(E) = E$ and $\sigma(F) = F$ by the normal assumption. If follows that

$$\sigma(EF) = \sigma(E)\sigma(F) = EF.$$

$\square$

3.6. **finite dimensional Galois extension.** In this section, we are going to prove the fundamental theorem for finite dimensional Galois extension.

Let F/K be an field extension, we define the Galois group of F over K, denoted $\mathrm{Gal}_{F/K}$ or $G_{F/K}$ or $\mathrm{Aut}_K(F)$, as

$$\mathrm{Gal}_{F/K} := \{\sigma | \sigma \in \mathrm{Aut}F, \sigma_{|K} = \mathbf{1}_K\}.$$

It's clear that for $\sigma \in \mathrm{Gal}_{F/K}$ and $u \in F$ algebraic over K with minimal polynomial $p(x)$, then $\sigma(u)$ satisfies the same minimal polynomial.

On the other hand, if F/K is normal, let u, v be two elements having the same minimal polynomial $p(x)$, then we claim that there is an $\sigma \in \mathrm{Gal}_{F/K}$ such that $\sigma(u) = v$. To see this, we fix an algebraic closure $\overline{K}$ containing F. There is an K-isomorphism $\sigma_0 : K(u) \to K(v)$ which extends to an embedding $\sigma : F \to \overline{K}$. Since F is normal over K, one has $\sigma(F) \subset F$. And hence $\sigma \in \mathrm{Aut}F$.

Example 3.6.1.

Consider the field $F := \mathbb{Q}(\sqrt[3]{2}, \omega)$ which is a splitting field of $x^3 - 2$ over $\mathbb{Q}$. Thus it's normal over $\mathbb{Q}$. One can check that the Galois group $\mathrm{Gal}_{F/\mathbb{Q}}$ is generated by σ, τ that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma(\omega) = \omega$, and $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2$. It's easy to check that $\mathrm{Gal}_{F/\mathbb{Q}} \cong S_3$. $\square$

Example 3.6.2.

Consider the field $F := \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Then it's easy to check that $\mathrm{Gal}_{F/\mathbb{Q}} = \{\mathbf{1}_F\}$. $\square$

There is a natural correspondence between subgroups of Galois groups and intermediate fields. To be precise, fix an extension F/K. Let $H < G := \mathrm{Gal}_{F/K}$ be a subgroup. One can define

$$H' := \{u \in F | \sigma(u) = u, \forall \sigma \in H\}.$$

It's clear that this is a field. On the other hand, given and intermediate field L such that $K \subset L \subset F$, then one can define

$$L' := \{\sigma \in \mathrm{Gal}_{F/K} | \sigma(u) = u, \forall u \in L\} = \{\sigma \in \mathrm{Gal}_{F/K} | \sigma_{|L} = \mathbf{1}_L\}.$$

It's easy to check the following properties:

Proposition 3.6.3. *Let F/K be an extension with Galois group G. Let L be an intermediate field, i.e. $K \subset L \subset F$, and $H < G$ is a subgroup.*

(1) *$F' = \{\mathbf{1}_F\}$, $K' = G$, and $\{\mathbf{1}_F\}' = F$.*
(2) *For any L, one has $L \subset L''$, $L' = L'''$.*
(3) *For any H, one has $H < H''$, $H' = H'''$.*
(4) *For any intermediate fields $L \subset M$, one has $M' < L'$.*
(5) *For any subgroups $J < H$, one has $H' \subset J'$.*

Proof. Most of the proof follows directly from the definition. We only sketch the proof for $L' = L'''$.

By $L \subset L''$ and (4), one has

$$(L'')' < L'.$$

On the other hand, by (5), one has

$$L' < (L')''.$$

We are done. $\square$

Proposition 3.6.4. *There is a one-to-one correspondence between*

$$\{L | K \subset L \subset F, L'' = L\} \leftrightarrow \{H | H < G, H'' = H\}.$$

Proof. The correspondence is given by $L \mapsto L'$ (or $H \mapsto H'$).

To show the injective, one sees that if $L_1' = L_2'$, then $L_1 = L_1'' = L_2'' = L_2$.

For any H with $H'' = H$, we take $L = H'$, then $H = L'$. It suffices to check that $L'' = L$. This follows from the fact that $H''' = H'$. $\square$

In the proposition, one might expect that $G' = K$. However, this is not always the case (see e.g. Example 3.6.2). For extension with this property, we call it *Galois*. It turns out that this naive definition is a very delicate one which leads to some nice properties.

Definition 3.6.5. *An extension F/K is said to be Galois if* $(\mathrm{Gal}_{F/K})' = K$.

Example 3.6.6.

Keep the notation as in Example 3.6.1. One can check that $G' = \mathbb{Q}$, hence a Galois extension.

In fact the group G has the following subgroups: $\{\mathbf{1}\}, <\tau>, <\tau\sigma>, <\tau\sigma^2>, <\sigma>, G$ of order $1, 2, 2, 2, 3, 6$ respectively. Their fixed fields are $\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2), \mathbb{Q}(\omega), \mathbb{Q}$ respectively.

Conversely, for these intermediate subfields, their fixed groups are exactly those corresponding ones. □

In general, we have the following:

Theorem 3.6.7 (Fundamental theorem of finite dimensional Galois extension)**.** *Let F/K be a finite dimensional Galois extension with Galois group G, then*

(1) *There is an one-to-one correspondence between*

$$\{L | K \subset L \subset F\} \leftrightarrow \{H | H < G\}.$$

(2) *The corresponding degree are equal. That is, if $K \subset L \subset M \subset F$, then $[M : L] = [L' : M']$. And if $J < H < G$, then $[H : J] = [J' : H']$.*

(3) *An intermediate field E is Galois over K if and only if $E' \lhd G$. And in this case,* $\mathrm{Gal}_{E/K} \cong G/E'$.

Proof. **Step 1.** $[M : L] \geq [L' : M']$.

We prove the case that $M = L(u)$ for some $u \in M$ and by induction on $[M : L]$, we are done. Suppose now that $M = L(u)$ and let $p(x)$ be the minimal polynomial of u over L. Let S be the set of roots of $p(x)$ in F. Then one has a map

$$\Phi : L' \to S,$$

$$\sigma \mapsto \sigma(u).$$

One can check that Φ induces an injective map $L'/M' \to S$. Hence one has

$$[L' : M'] = |L'/M'| \leq |S| \leq deg(p(x)) = [M : L].$$

Step 2. $[H : J] \geq [J' : H']$.

Let $n = [H : J]$. Suppose on the contrary that there are $n+1$ elements $u_1, ..., u_{n+1} \in J'$ linearly independent over H'.

We consider the equation $\sum_{i=1}^{n+1} u_i x_i = 0$ in F Consider now a set of representative of H/J, denoted $\{e = \sigma_1, ..., \sigma_n\}$. By applying σ_i to the above equation. Then one has a system of linear equations in F.

$$(*) \begin{cases} \sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + ... + \sigma_1(u_{n+1})x_{n+1} = 0 \\ \sigma_2(u_1)x_1 + \sigma_2(u_2)x_2 + ... + \sigma_2(u_{n+1})x_{n+1} = 0 \\ \vdots \\ \sigma_n(u_1)x_1 + \sigma_n(u_2)x_2 + ... + \sigma_n(u_{n+1})x_{n+1} = 0 \end{cases}$$

Pick a solution in F with smallest number of non-zero a_i's, may assume it's $(a_1, ..., a_s, 0..., 0)$ and $a_1 = 1$.

If there is an $\tau \in H$ such that $\tau(a_2) \neq a_2$, then by applying τ to the system $(*)$, one get the same system of equations with a solution $(\tau(a_1), \tau(a_2), ..., \tau(a_s), 0, ..., 0$. Hence

$$(a_1, ..., a_s, 0..., 0) - (\tau(a_1), \tau(a_2), ..., \tau(a_s), 0, ..., 0) = (0, a_2 - \tau(a_2), ..., 0)$$

is a non-zero solution of smaller length. This is the required contradiction.

To find τ. We look at $u_1a_1 + ... + u_sa_s = 0$. Since $\{u_1, ..., u_s\}$ is independent over H', not all a_1 is in H'. We may assume that $a_2 \notin H'$. Hence there is a $\tau \in H$ such that $\tau(a_2) \neq a_2$. We are done.

Step 3. We show that every intermediate field L, $L'' = L$. And every subgroup $H < G$, $H'' = H$.

By Step 1, one has

$$[L'' : K] = [L'' : K''] \leq [K' : L'] \leq [L : K],$$

however, one has $L \subset L''$. Thus one has $L = L''$. Similarly, one can prove that $H'' = H$ by considering $[H'' : \{\mathbf{1}_F\}]$.

Step 4. $[M : L] = [L' : M']$ and $[H : J] = [J' : H']$.

This follows from $[M : L] = [M : K]/[L : K] = [K' : M']/[K' : L'] = [L' : M']$. And the other one is similar.

Step 5. F/K is normal and separable.

Given $u \in F$, with minimal polynomial $p(x)$ over K. As in the proof of Step 1. One has $[K(u)' : K'] \leq |S| \leq deg(p(x)) = [K(u) : K]$. By Step 4, they are equalities. In particular, every root of $p(x)$ is in F and there is no multiple roots. Thus F is normal and separable over K.

Step 6. If $N \lhd G$, then N' is stable. That is, for all $\sigma \in G$, $\sigma(N') \subset N'$ (indeed $= N'$).

Since $N \lhd G$, for all $\sigma \in G$ and for all $\tau \in N$, one has $\sigma^{-1}\tau\sigma \in N$. Thus, $\sigma^{-1}\tau\sigma(N') = N'$. It follows that $\tau\sigma(N') = \sigma(N')$, for all $\tau \in N$. Hence $\sigma(N')$ is fixed by all N and thus $\sigma(N') \subset N'$.

Step 7. If E is a stable intermediate subfield. Then the restriction map $\mathrm{Gal}_{F/K} \to \mathrm{Gal}_{E/K}$ is well-defined and surjective.

Since E is stable, then $\sigma_{|E} \in \mathrm{Gal}_{E/K}$ for any $\sigma \in \mathrm{Gal}_{F/K}$. Moreover, let $\tau \in \mathrm{Gal}_{E/K}$, by the extension theorem, there is an extension $\overline{\tau} : F \to \overline{K}$. Since F is normal over K, $\overline{\tau}$ is in fact an automorphism of F.

Step 8. If an intermediate field E is stable, then E/K is Galois.

To see this, it suffices to show that for any $u \in E - K$, there is an $\sigma \in \mathrm{Gal}_{E/K}$ such that $\sigma(u) \neq u$. Fix any $F \ni v \neq u$ with the same minimal polynomial as u. There is an K-isomorphism $\sigma_0 : K(u) \to K(v)$ such that $\sigma(u) = v$. σ can be extended to an embedding $\overline{\sigma} : F \to \overline{K}$, which gives an automorphism of F. The restriction $\sigma = \overline{\sigma}_{|E}$ gives an automorphism of E that $\sigma(u) \neq u$.

Step 9. If E/K is Galois, then E is stable.

One first notices that E/K is normal. For every $\sigma \in \mathrm{Gal}_{F/K}$, σ gives an embedding $\sigma_{|E} : E \to \overline{K}$. Since E/K is normal, $\sigma_{|E}$ is an automorphism of E. And hence E is stable under the Galois group $\mathrm{Gal}_{F/K}$ action.

Step 10. If E is stable, then E' is normal.

This can be checked directly. For all $\sigma \in G$ and $\tau \in E'$ and for all $u \in E$,

$$\sigma^{-1}\tau\sigma(u) = \sigma^{-1}\tau(\sigma(u)) = \sigma^{-1}\sigma(u) = u,$$

since $\sigma(u) \in E$. Therefore, $\sigma^{-1}\tau\sigma \in E'$. $\square$

Remark 3.6.8. *Some of the result we proved still true in a more general setting. We list some here:*

1. *If F/K is an extension, and an intermediate field E is stable, then $E' \lhd \mathrm{Gal}_{F/K}$.*
2. *Let F/K be an extension. If $N \lhd \mathrm{Gal}_{F/K}$, then H' is stable.*
3. *If F/K is Galois, and E is a stable intermediate field, then E is Galois over K. (finite-dimensional assumption is unnecessary here)*
4. *An intermediate field E is algebraic and Galois over K, then E is stable.*

We conclude this section with the following theorem concerning the relation between Galois extension, normal extension and splitting fields.

Definition 3.6.9. *An irreducible polynomial $f(x) \in K[x]$ is said to be* **separable** *if its roots are all distinct in $\overline{K}$.*

Let F be an extension over K and $u \in F$ is algebraic over K. Then u is separable over K if its minimal polynomial is separable.

An extesnion F over K is separable if every element of F is separable over K.

Theorem 3.6.10. *Let F/K be an extension, then the following are equivalent*

1. *F is algebraic and Galois over K.*
2. *F is separable over K and F is a splitting field over K of a set S of polynomials.*
3. *F is a splitting field of separable polynomials in $K[X]$.*
4. *F/K is normal and separable.*

Proof. Fix $u \in F$ with minimal polynomail $p(x)$ over K. Let $\{u = u_1, ..., u_r\}$ be distinct roots of $p(x)$ in F. For any σ, then σ permutes $\{u = u_1, ..., u_r\}$. Thus $f(x) := \prod_{i=1}^{r}(x - u_i)$ is invariant under σ. Hence $f(x) \in K[x]$. It follows that $f(x) = p(x)$. This proved that $(1) \Rightarrow (2), (3), (4)$.

One notices that $(2) \Leftrightarrow (4)$. Thus it remains to show that $(2) \Rightarrow (3)$, and $(3) \Rightarrow (1)$.

For $(2) \Rightarrow (3)$, let $f(x) \in S$ and let $g(x)$ be an monic irreducible component of $f(x)$. Since $f(x)$ splits in F, it's clear that $g(x)$ is an minimal polynomial of some element in F. Moreover, since F/K is separable, $g(x)$ is separable. One sees that F is in fact a splitting field of such $g(x)$'s.

For $(3) \Rightarrow (1)$, we first note that F/K is algebraic since F is a splitting field. We shall prove that $(4) \Rightarrow (1)$. The implication $(3) \rightarrow (4)$ follows from a general fact about separable extension that an algebraic extension F/K is separable if F is generated by separable elements.

To this end, pick any $u \in F - K$, with minimal polynomial $p(x)$ of degree ≥ 2 and separable. Hence there is a different root, say v, of $p(x)$ in F. It's natural to consider the K-isomorphism $\sigma : K(u) \rightarrow K(v)$. Which can be extended to $\bar{\sigma} : F \rightarrow \overline{K}$. Since F is normal, $\bar{\sigma}$ is an automorphism of F, hence in $\mathrm{Gal}_{F/K}$ sending u to $v \neq u$. So F/K is Galois.

□