Nov. 10, 2006 (Fri.)

3.3. irreducibility. One of the most important construction of field extension comes from the extension of the form \( K[x]/(p(x)) \) with \( p(x) \) an irreducible polynomial. It is therefore natural to give some criterion for irreducibility of polynomials.

**Theorem 3.3.1** (Gauss’ Lemma). Let \( D \) be a UFD, and \( K \) be its field of quotients. Given a polynomial \( f(x) \in D[x] \). Then \( f(x) \) is irreducible in \( D[x] \) if and only if \( f(x) \) is irreducible in \( K[x] \).

**Sketch.** 1. \( f(x) \) is irreducible in \( K[x] \) then \( f(x) \) is irreducible in \( D[x] \).
2. Given an irreducible \( f(x) \in D[x] \). We may assume that \( f(x) \) is primitive, that is, the g.c.d of coefficient is 1. If \( f(x) = g(x)h(x) \in K[x] \), by clearing the denominators, we have \( af(x) = (bg(x))(ch(x)) \) with \( a, b, c \in K \) and \( af(x), bg(x), cf(x) \in D[x] \) being primitive.
   
The main ingredient is:
3. In \( D[x] \), if \( s[x], t[x] \) are primitive, then so is \( s[x]t[x] \).
   
To see this, suppose that \( d \neq 1 \) is the g.c.d of coefficient of \( s[x]t[x] \). Let \( p \) be a prime factor of \( d \). We consider the ring homomorphism \( - : D[x] \rightarrow D/(p)[x] \). Then

\[
0 = s[x]f[x] = (s[x])(t[x]) \neq 0.
\]

4. It follows that \( af(x) \in D[x] \) is also primitive. Write \( a = \frac{z}{p} \) with \( (p, q) = 1 \). It follows that \( p(qa_0, ..., qa_n) = q, \) where \( a_i \) are coefficients of \( f(x) \). This is the required contradiction.

The following observation is easy but useful:

**Proposition 3.3.2.** Let \( f(x) \in D[x] \) be a monic polynomial, \( p < d \) be a prime ideal. We consider \( - : D[x] \rightarrow D/(p)[x] \). If \( f(x) \) is irreducible in \( D/(p)[x] \), then \( f(x) \) is irreducible in \( D[x] \).

**Example 3.3.3.**

Given \( f(x) = x^2 + 517x + 65535 \in \mathbb{Z}[x] \), we may consider \( - : \mathbb{Z}[x] \rightarrow \mathbb{Z}_2[x] \). Then \( f(x) = x^2 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \), hence irreducible in \( \mathbb{Z}[x] \). By Gauss’ Lemma, it’s also irreducible in \( \mathbb{Q}[x] \).

We also recall

**Proposition 3.3.4** (Eisenstein’s criterion). Let \( f(x) = a_nx^n + ... + a_0 \in \mathbb{Z}[x] \). If there is a prime \( p \) such that \( p \nmid a_n, p|a_{n-1}, ..., p|a_0, \) and \( p^2 \nmid a_0 \). Then \( f(x) \) is irreducible.

**Proof.** If \( f(x) = g(x)h(x) \), then we consider \( - : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x] \). Thus

\[
a_nx^n = f(x) = \overline{g(x)h(x)}.
\]

It follows that both \( \overline{g(x)}, \overline{h(x)} \) are of the form \( \alpha x^m \in \mathbb{Z}_p[x] \) with \( m \geq 1 \). Therefore, we may write \( \overline{g(x)} = b_mx^m + ... + b_0, \overline{f(x)} = c_kx^k + ... + c_0 \) with \( p|b_0, p|c_0 \). Then \( p^2|b_0c_0 = a_0 \), a contradiction. □
3.4. algebraic closed fields and algebraic closure. In this section, we are going to prove the existence and uniqueness of algebraic closure. As a consequence, we are able to show the existence and uniqueness of splitting fields.

To motivate the study of algebraic closure, we start with examples:

Example 3.4.1. Consider \( \mathbb{Q}[\sqrt{2}]/\mathbb{Q} \) and \( \mathbb{Q}[\sqrt{2}\omega]/\mathbb{Q} \). There is a isomorphism \( \varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}\omega] \) with \( \varphi(\sqrt{2}) = \sqrt{2}\omega \), and \( \varphi(a) = a \) for \( a \in \mathbb{Q} \).

This follows from the natural isomorphism \( \mathbb{Q}[x]/(x^2 - 2) \to \mathbb{Q}[\sqrt{2}] \) and \( \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}[\sqrt{2}\omega] \).

In general, given an extension \( F/K \), if \( u, v \in F \) are two roots of an irreducible polynomial \( p(x) \in K[x] \), then \( K[u] \cong K[v] \). Therefore, starting with a field \( K \) and an irreducible polynomial \( p(x) \in K[x] \), it’s convenient that we have a field \( F \) containing all roots of \( p(x) \) in advance.

Or even more, we would like to have a field containing all roots of all polynomial in \( K[x] \).

Proposition 3.4.2. Let \( F \) be a field. The following are equivalent:

1. Every polynomial of \( F[x] \) of degree \( \geq 1 \) has a root in \( F \).
2. Every polynomial of \( F[x] \) of degree \( \geq 1 \) has all the roots in \( F \).
3. Every irreducible polynomial in \( F[x] \) has degree \( \leq 1 \).
4. If \( E \) is an algebraic extension over \( F \), then \( E = F \).
5. There is a subfield \( K \subset F \) such that \( F \) is algebraic over \( K \) and every polynomial in \( K[x] \) splits in \( F[x] \).

Definition 3.4.3. A field \( F \) satisfying above conditions is said to be algebraically closed.

Sketch. (1) \( \Rightarrow \) (2) by induction on degree. And hence (1) \( \iff \) (2) are equivalent. It’s easy to see that (2) \( \iff \) (3). We now look at (3) and (4). If \( E \) is an algebraic extension. Pick \( u \in E \) algebraic over \( F \) with minimal polynomial \( p(x) \). By (3), \( p(x) \) has degree 1, hence \( [E : F] = \text{deg}(p(x)) = 1 \). In particular, \( E = F \). Conversely, if there is an irreducible polynomial \( p(x) \) of degree \( > 1 \), then \( K[x]/(p(x)) \) gives an algebraic extension of degree \( \text{deg}(p(x)) \). This leads to a contradiction, hence (4) implies (3).

Lastly, it’s clear that (3) implies (5) by picking \( K = F \). We now prove that (5) \( \Rightarrow \) (4). Let \( E \) be an algebraic extension over \( F \). For any \( u \in E \), \( u \) is algebraic over \( K \) as well. Let \( p_F(x), p_K(x) \) be the minimal polynomial of \( u \) over \( F, K \) respectively. By viewing \( p_K(x) \) as a polynomial in \( F \), then one has \( p_F(x)|p_K(x) \in F[x] \). However, \( p_K(x) \) splits in \( F[x] \). It follows that \( p_F(x) \) has degree 1. And hence \( u \in F \). Thus \( E = F \).

We can also define the notion of algebraic closure.
Proposition 3.4.4. Let $F/K$ be an extension. The following are equivalent.

1. $F/K$ is algebraic, and $F$ is algebraically closed.
2. $F/K$ is algebraic, and every polynomial in $K[x]$ splits in $F[x]$.
3. $F$ is a splitting field of all polynomials of $K$.

Proof. The proof is an easy consequence of the Proposition 3.4.2, we leave it to the readers. \(\square\)

Definition 3.4.5. $F$ is said to be an algebraical closure of $K$ if $F/K$ satisfies the above conditions.

Theorem 3.4.6. Algebraic closure exists.

The following is due to M. Artin as it appeared in [Lang, Algebra].

Proof. Let $K$ be a field.

Step 1. There is an extension $E_1$ over $K$ such that every polynomial of degree $\geq 1$ has a root in $E_1$.

To this end, let $S$ be the set of all polynomials of degree $\geq 1$. We consider $K[S]$ to be the polynomial ring with indeterminates $x_f$, for $f \in S$. Consider now an ideal $I = \langle f(x_f) >_{f \in S}$. We claim that $I \neq K[S]$, hence $I \subset m$ for some maximal ideal $m$. The field $K[S]/m$ gives an extension $E_1$ over $K$. Now, for every $f(x) \in K[x]$, one sees that $f(x_f) = 0 \in E_1$. Hence $f(x)$ has a root in $E_1$.

It remains to show that $I \neq K[S]$. Suppose on the contrary that $I = K[S]$, in particular, $1 \in I$. We may write

$$1 = \sum_{i=1}^{r} g(X)f_i(x_{f_i}).$$

One can construct an algebraic extension $F/K$ such that each $f_i$ has a root $u_i$ in $F$. Substitute $x_{f_i}$ by $u_i$ in $F$, one has

$$1 = \sum_{i=1}^{r} g(X)f_i(u_i) = 0 \in F,$$

which is the required contradiction.

Step 2. Inductively, one has $K = E_0 \subset E_1 \subset E_2...$. Let $E = \cup E_i$, then $E$ is a field extension over $K$. And $E$ is algebraically closed.

To see this, for any polynomial $f(x) = \sum a_i x^i \in E[x]$, $a_i \in E_{j_i}$ for some $j_i$. One can pick $J$ maximal among $j_i$ so that $a_i \in E_J$ for all $i$. Hence $f(x) \in E_J$. By construction, $f(x)$ has a root in $E_{J+1}$, and inductively, $f(x)$ has all its root in $E_{J+d}$, where $d = \deg(f(x))$. Therefore, $f(x)$ has all its root in $E$.

Step 3. Let $E_a := \{u \in E | u \text{ is algebraic over } K\}$. Then $E_a$ is an algebraic closure of $K$.

It’s an easy exercise to check that $E_a$ is a field extension over $K$. We leave it to the readers. It’s also clear that $E_a$ is algebraic over $K$. Hence, it suffices to check that $E_a$ is algebraically closed.
To see this, one notices that every polynomial of $K[x]$ splits in $E$ and it follows that every root of $K[x]$ is in $E$. Therefore, one has that every polynomial of $K[x]$ splits in $E$ and we are done. □

**Remark 3.4.7.** An algebraically closed field must be infinite.
Suppose that $F$ is algebraically closed and $F = \{a_1, \ldots, a_n \neq 0\}$. We consider $f(x) := \prod(x - a_i) + a_n$. Then $f(x)$ has no root in $F$, a contradiction.

We next work on the uniqueness of algebraic closure. The main ingredient is the following extension theorem.

**Theorem 3.4.8 (Extension theorem).** Let $\sigma : K \to L$ be an embedding to an algebraically closed field $L$. Let $E/K$ be an algebraic extension.
Then one can extend the embedding $\sigma$ to an embedding $\bar{\sigma} : E \to L$. That is, there is an embedding $\bar{\sigma} : E \to L$ such that $\bar{\sigma}|_K = \sigma$.

We remark that $L$ is not necessarily an algebraic closure of $K$. For example, $L$ could be something like $\overline{K(x)}$, an algebraic closure of $K(x)$.

In order to prove the uniqueness, we need the following useful Lemma.

**Lemma 3.4.9.** Let $E/K$ be an algebraic extension and $\sigma : E \to E$ be an embedding such that $\sigma|_K = 1_K$. Then $\sigma$ is an isomorphism.

**Proof.** If $E/K$ is finite, then injective implies isomorphic in the case of finite dimensional vector space.

In general, let’s pick any $u \in E$. It suffices to show that $u$ is in the image of $\sigma$. To see this, let $p(x)$ be the minimal polynomial of $u$ over $K$ and $u = u_1, u_2, \ldots, u_r$ be the roots of $p(x)$ in $E$. Let $E' := K(u_1, \ldots, u_r)$. It’s clear that for each $i$, $\sigma(u_i) = u_j$ for some $j$. Hence $\sigma|_{E'}$ gives an homomorphism from $E'$ to $E'$.

Now $\sigma|_{E'} : E' \to E'$ is an injective homomorphism of finite dimensional vector space $E'/K$. Therefore, $\sigma|_{E'}$ is an isomorphism. In particular, $u$ is in the image of $\sigma|_{E'}$ and therefore in the image of $\sigma$. □

**Sketch of the theorem.** The staring point is an extension to a simple extension. More precisely, let $u \in E$ be algebraic over $K$ with minimal polynomial $p(x)$. Then $p^\sigma(x)$ is an irreducible polynomial in $\sigma(K)[x]$. In $L$, Pick any root $v$ of $p^\sigma(x)$ in $\sigma(K)[x]$. This is possible since $L$ is algebraically closed. One claims that there is an isomorphism ( hence an embedding to $L$)

$$\bar{\sigma} : K(u) \to \sigma(K)(v) \subset L$$

extending $\sigma$. We leave the detail to the readers.

In order to work on the general case, we apply Zorn’s Lemma to the non-empty P.O. set of fields

$$S := \{(F, \tau)|K \subset F \subset E, \tau : F \to L, \tau|_K = \sigma\}$$

The ordering is given naturally as: $(F_1, \tau_1) \leq (F_2, \tau_2)$ if $F_1 \subset F_2$ and $\tau_1 = \tau_2|_{F_1}$.
By Zorn’s Lemma, there is a maximal element, say $E_m$. It’s easy to see that $E_m = E$. Otherwise, pick any $u \in E$, which is algebraic over $K$ and hence over $E_m$. There is an extension to $E_m(u)$ as we have seen in the first paragraph. This is a contradiction to the maximality of $E_m$. Hence $E_m = E$. □

Lemma 3.4.10. Let $E/K$ be an algebraic extension and $\sigma : E \to E$ be an embedding such that $\sigma|_K = 1_K$. Then $\sigma$ is an isomorphism.

Proof. If $E/K$ is finite, then injective implies isomorphic in the case of finite dimensional vector space.

In general, let’s pick any $u \in E$. It suffices to show that $u$ is in the image of $\sigma$. To see this, let $p(x)$ be the minimal polynomial of $u$ over $K$ and $u = u_1, u_2, \ldots, u_r$ be the roots of $p(x)$ in $E$. Let $E' := K(u_1, \ldots, u_r)$. It’s clear that for each $i$, $\sigma(u_i) = u_j$ for some $j$. Hence $\sigma|_{E'}$ gives an homomorphism from $E'$ to $E'$.

Now $\sigma|_{E'} : E' \to E'$ is an injective homomorphism of finite dimensional vector space $E'/K$. Therefore, $\sigma|_{E'}$ is an isomorphism. In particular, $u$ is in the image of $\sigma|_{E'}$ and therefore in the image of $\sigma$. □

Corollary 3.4.11. Algebraic closure of a field is unique up to isomorphism.

Proof. Suppose that $E, F$ are algebraic closure of $K$. By the extension theorem, there are embedding $\sigma : E \to F$ and $\tau : F \to E$ such that $\sigma|_K = \tau|_K = 1_K$.

Hence one has an embedding $\sigma \circ \tau : F \to F$, which is an isomorphism by the Lemma. Similarly, $\tau \circ \sigma$ is an isomorphism. Hence $E$ and $F$ are isomorphic. □

Therefore, 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 splitting field more concrete.

3.5. splitting fields. Let $K$ be a field and $f(x) \in K[x]$. Let $\{u_1, \ldots, u_r\}$ be the roots of $f(x)$ in its algebraic closure $\overline{K}$. Then the field $K(u_1, \ldots, u_r)$ is called the splitting field of $f(x)$ over $K$. 