Math 2070 Week 13

Field Extensions, Finite Fields

13.1 Field Extensions

Definition 13.1. Let R be a ring. A subset S of R is said to be a **subring** of R if it is a ring under the addition $+_R$ and multiplication $\times_R$ associated with R, and its additive and multiplicative identity elements 0, 1 are those of R.

Remark. To show that a subset S of a ring R is a subring, it suffices to show that:

- S contains the additive and multiplicative identity elements of R.
- S is "closed under addition": $a +_R b \in S$ for all $a, b \in S$.
- S is "closed under multiplication": $a \times_R b \in S$ for all $a, b \in S$.
- S is closed under additive inverse: For all $a \in S$, the additive inverse $-a$ of a in R belongs to S.

Definition 13.2. A **subfield** k of a field K is a subring of K which is a field.

In particular, for each nonzero element $r \in k \subseteq K$. The multiplicative inverse of r in K lies k.

Definition 13.3. Let K be a field and k a subfield. Let α be an element of K. We define $k(\alpha)$ to be the smallest subfield of K containing k and α. In other words, if F is a subfield of K which contains k and α, then $F \supseteq k(\alpha)$. We say that $k(\alpha)$ is obtained from k by **adjoining** α.

Theorem 13.4. *Let k be a subfield of a field K. Let α be an element of K.*

1. *If α is a root of a nonzero polynomial $f \in k[x]$ (viewed as a polynomial in $K[x]$ with coefficients in k), then α is a root of an irreducible polynomial $p \in k[x]$, such that $p|f$ in $k[x]$.*

2. *Let p be an irreducible polynomial in $k[x]$ of which α is a root. Then, the map $\phi : k[x]/(p) \longrightarrow K$, defined by:*

$$\phi\left(\sum_{j=0}^{n} c_j x^j + (p)\right) = \sum_{j=0}^{n} c_j \alpha^j,$$

   is a well-defined one-to-one ring homomorphism with $\operatorname{im}\phi = k(\alpha)$. (Here, $\sum_{j=0}^{n} c_j x^j + (p)$ is the congruence class of $\sum_{j=0}^{n} c_j x^j \in k[x]$ modulo (p).)

   Hence,
$$k[x]/(p) \cong k(\alpha).$$

3. *If $\alpha, \beta \in K$ are both roots of an irreducible polynomial p in $k[x]$, then there exists a ring isomorphism $\sigma : k(\alpha) \longrightarrow k(\beta)$, with $\sigma(\alpha) = \beta$ and $\sigma(s) = s$, for all $s \in k$.*

4. *Let p be an irreducible polynomial in $k[x]$ of which α is a root. Then, each element in $k(\alpha)$ has a unique expression of the form:*

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

   where $c_i \in k$, and $n = \deg p$.

Remark. Suppose p is an irreducible polynomial in $k[x]$ of which $\alpha \in K$ is a root. Part 4 of the theorem essentially says that $k(\alpha)$ is a vectors space of dimension $\deg p$ over k, with basis:
$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}.$$

Example 13.5. Consider $k = \mathbb{Q}$ as a subfield of $K = \mathbb{R}$. The element $\alpha \in \sqrt[3]{2} \in \mathbb{R}$ is a root of the the polynomial $p = x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible in $\mathbb{Q}[x]$ by the Eisenstein's Criterion for the prime 2.

The theorem applied to this case says that $\mathbb{Q}(\alpha)$, i.e. the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and α, is equal to the set:

$$\{c_0 + c_1\alpha + c_2\alpha^2 : c_i \in \mathbb{Q}\}$$

The addition and multiplication operations in $\mathbb{Q}(\alpha)$ are those associated with $\mathbb{R}$, in other words:

$$(c_0 + c_1\alpha + c_2\alpha^2) + (b_0 + b_1\alpha + b_2\alpha^2)$$
$$= (c_0 + b_0) + (c_1 + b_1)\alpha + (c_2 + b_2)\alpha^2,$$

$$
\begin{aligned}
(c_0 + c_1\alpha + c_2\alpha^2) \cdot (b_0 + b_1\alpha + b_2\alpha^2) \\
= c_0b_0 + c_0b_1\alpha + c_0b_2\alpha^2 + c_1b_0\alpha + c_1b_1\alpha^2 \\
+ c_1b_2\alpha^3 + c_2b_0\alpha^2 + c_2b_1\alpha^3 + c_2b_2\alpha^4 \\
= (c_0b_0 + 2c_1b_2 + 2c_2b_1) + (c_0b_1 + c_1b_0 + 2c_2b_2)\alpha \\
+ (c_0b_2 + c_1b_1 + c_2b_0)\alpha^2
\end{aligned}
$$

Exercise 13.6. Given a nonzero $\gamma = c_0 + c_1\alpha + c_2\alpha^2 \in \mathbb{Q}(\alpha)$, $c_i \in \mathbb{Q}$, find $b_0, b_1, b_2 \in \mathbb{Q}$ such that $b_0 + b_1\alpha + b_2\alpha^2$ is the multiplicative inverse of γ in $\mathbb{Q}(\alpha)$.

Proof of Exercise 13.6. (of Theorem 13.4)

1. Define a map $\psi : k[x] \longrightarrow K$ as follows:

   $$\psi\left(\sum c_j x^j\right) = \sum c_j \alpha^j.$$

   Exercise: ψ is a ring homomorphism.

   By assumption, f lies in $\ker\psi$. Since k is a field, the ring $k[x]$ is a PID. So, there exists $p \in k[x]$ such that $\ker\psi = (p)$. Hence, $p|f$ in $k[x]$.

   By the First Isomorphism Theorem, $\operatorname{im}\psi$ is a subring of K which is isomorphic to $k[x]/(p)$. In particular, $\operatorname{im}\psi$ is an integral domain because K has no zero divisors. Hence, by Theorem 11.20 , the polynomial p is an irreducible in $k[x]$.

   Since $p \in (p) = \ker\psi$, we have $0 = \psi(p) = p(\alpha)$. Hence, α is a root of p.

2. If $f+(p) = g+(p)$ in $k[x]/(p)$, then $g-f \in (p)$, or equivalently: $g = f+pq$ for some $q \in k[x]$.

   Hence, $\phi(g + (p)) = f(\alpha) + p(\alpha)q(\alpha) = f(\alpha) = \phi(f + (p))$.

   This shows that ϕ is a well-defined map. We leave it as an exercise to show that ϕ is a one-to-one ring homomorphism.

   We now show that $\operatorname{im}\phi = k(\alpha)$. By the First Isomorphism Theorem, $\operatorname{im}\phi$ is isomorphic to $k[x]/(p)$, which is a field since p is irreducible. Moreover, $\alpha = \phi(x + (p))$ lies in $\operatorname{im}\phi$. Hence, $\operatorname{im}\phi$ is a subfield of K containing α.

   Since each element in $\operatorname{im}\phi$ has the form $\sum_{j=0}^{n} c_j\alpha^j$, where $c_j \in k$, and fields are closed under addition and multiplication, any subfield of K which contains k and α must contain $\operatorname{im}\phi$. This shows that $\operatorname{im}\phi$ is the smallest subfield of K containing k and α. Hence, $k[x]/(p) \cong \operatorname{im}\phi = k(\alpha)$.

3. Define $\phi' : k[x]/(p) \longrightarrow k(\beta)$ as follows:
$$\phi'\left(\sum c_j x^j + (p)\right) = \sum c_j \beta^j.$$
By the same reasoning applied to ϕ before, the map ϕ' is a well-defined ring isomorphism, with:
$$\phi'(x + (p)) = \beta, \quad \phi'(s + (p)) = s \text{ for all } s \in k.$$
It is then easy to see that the map $\sigma := \phi' \circ \phi^{-1} : k(\alpha) \longrightarrow k(\beta)$ is the desired isomorphism between $k(\alpha)$ and $k(\beta)$.

4. Since ϕ in Part 2 is an isomorphism onto $\operatorname{im}\phi = k(\alpha)$, we know that each element $\gamma \in k(\alpha)$ is equal to $\phi(f + (p)) = f(\alpha) := \sum c_j \alpha^j$ for some $f = \sum c_j x^j \in k[x]$.

   By the division theorem for $k[x]$. There exist $m, r \in k[x]$ such that $f = mp + r$, with $\deg r < \deg p = n$. In particular, $f + (p) = r + (p)$ in $k[x]/(p)$.

   Write $r = \sum_{j=0}^{n-1} b_j x^j$, with $b_j = 0$ if $j > \deg r$.

   We have:
$$\gamma = \phi(f + (p)) = \phi(r + (p)) = \sum_{j=0}^{n-1} b_j \alpha^j.$$
   It remains to show that this expression for γ is unique. Suppose $\gamma = g(\alpha) = \sum_{j=0}^{n-1} b'_j \alpha^j$ for some $g = \sum_{j=0}^{n-1} b'_j x^j \in k[x]$.

   Then, $g(\alpha) = r(\alpha) = \gamma$ implies that $\phi(g + (p)) = \phi(r + (p))$, hence:
$$(g - r) + (p) \in \ker\phi.$$
   Since ϕ is one-to-one, we have $(g - r) \equiv 0$ modulo (p), which implies that $p|(g - r)$ in $k[x]$.

   Since $\deg g, \deg r < \deg p$, this implies that $g - r = 0$. So, the expression $\gamma = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ is unique.

□

Terminology:

- If k is a subfield of K, we say that K is a **field extension** of k.
- Let α be an element in a field extension K of a field k. If there exists a polynomial $p \in k[x]$ of which α is a root, then α is said to be **algebraic over** k.

- If $\alpha \in K$ is algebraic over k, then there exists a unique *monic irreducible* polynomial $p \in k[x]$ of which α is a root (**Exercise**). This polynomial p is called the **minimal polynomial** of α over k.

For example, $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$. Its minimal polynomial over $\mathbb{Q}$ is $x^3 - 2$.

Exercise 13.7. Find the minimal polynomial of $2 - \sqrt[3]{6} \in \mathbb{R}$ over $\mathbb{Q}$, if it exists.

Exercise 13.8. Find the minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$.

Exercise 13.9. Express the multiplicative inverse of $\gamma = 2 + \sqrt[3]{5}$ in $\mathbb{Q}(\sqrt[3]{5})$ in the form:

$$\gamma^{-1} = c_0 + c_1\sqrt[3]{5} + c_2\left(\sqrt[3]{5}\right)^2,$$

where $c_i \in \mathbb{Q}$, if possible.

13.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**