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:

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

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

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 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 Splitting Field

Example 13.10. *Since* $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ *is a root of* $x^3 - 2$*, the polynomial* $p = x^3 - 2$ *has a linear factor in* $\mathbb{Q}(\sqrt[3]{2})[x]$*. More precisely,*

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

in $\mathbb{Q}(\sqrt[3]{2})[x]$*.* **Exercise***: Is* $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ *irreducible in* $\mathbb{Q}(\sqrt[3]{2})[x]$*?*

We could repeat this process and adjoin roots of $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ to $\mathbb{Q}(\sqrt[3]{2})$ to further "split" the polynomial $x^3 - 2$ into a product of linear factors. That is the main idea behind the following theorem:

Theorem 13.11. *If* k *is a field, and* f *is a nonconstant polynomial in* $k[x]$*, then there exists a field extension* K *of* k*, such that* $f \in k[x] \subseteq K[x]$ *is a product of linear factors in* $K[x]$*.*

In other words, there exists a field extension K *of* k*, such that:*

$$f = c(x - \alpha_1) \cdots (x - \alpha_n),$$

for some $c, \alpha_i \in K$*.*

Proof. We prove by induction on $\deg f$.

If $\deg f = 1$, we are done.

Inductive Step: Suppose $\deg f > 1$. Suppose, for any field extension k' of k, and any polynomial $g \in k'[x]$ with $\deg g < \deg f$, there exists a field extension K of k' such that g splits into a product of linear factors in $K[x]$.

Suppose f is irreducible. Let $f(t)$ be the polynomial in $k[t]$ obtained from f by replacing the variable x with the variable t. Consider $k' := k[t]/(f(t))$. Then, k' is a field extension of k if we identify k with the subset $\{c + (f(t)) : c \in k\} \subseteq k'$, where c is considered as a constant polynomial in $k[t]$.

Observe that k' contains a root α of f, namely $\alpha = t + (f(t)) \in k[t]/(f(t))$. Hence, $f = (x - \alpha)q$ in $k'[x]$ for some polynomial $q \in k'[x]$ with $\deg q < \deg f$.

Now, by the induction hypothesis, there is an extension field K of k' such that q splits into a product of linear factors in $K[x]$. Consequently, f splits into a product of linear factors in $K[x]$.

If f is not irreducible, then $f = gh$ for some $g, h \in k[x]$, with $\deg g, \deg h < \deg f$. So, by the induction hypothesis, there is a field extension k' of k such that g is a product of linear factors in $k'[x]$.

Hence, $f = (x - \alpha_1) \cdots (x - \alpha_n)h$ in $k'[x]$. Since $\deg h < \deg f$, by the inductive hypothesis there exists a field extension K of k' such that h splits into linear factors in $K[x]$.

Hence, f is a product of linear factors in $K[x]$. □

13.3 WeBWorK

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

@thm If k is a field, and f is a nonconstant polynomial in $k[x]$, then there exists a field extension K of k, such that $f \in k[x] \subseteq K[x]$ is a product of linear factors in $K[x]$. @newcol In other words, there exists a field extension K of k, such that:

$$f = c(x - \alpha_1) \cdots (x - \alpha_n),$$

for some $c, \alpha_i \in K$. @endcol@end@proof@newcol We prove by induction on $\deg f$. @col If $\deg f = 1$, we are done. @col<b class="notkw">Inductive Step: Suppose $\deg f > 1$. Suppose, for any field extension k' of k, and any polynomial $g \in k'[x]$ with $\deg g < \deg f$, there exists a field extension K of

k' such that g splits into a product of linear factors in $K[x]$. @col Suppose f is irreducible. Let $f(t)$ be the polynomial in $k[t]$ obtained from f by replacing the variable x with the variable t. Consider $k' := k[t]/(f(t))$. Then, k' is a field extension of k if we identify k with the subset $\{c + (f(t)) : c \in k\} \subseteq k'$, where c is considered as a constant polynomial in $k[t]$. @col Observe that k' contains a root α of f, namely $\alpha = t + (f(t)) \in k[t]/(f(t))$. Hence, $f = (x - \alpha)q$ in $k'[x]$ for some polynomial $q \in k'[x]$ with $\deg q < \deg f$. @col Now, by the induction hypothesis, there is an extension field K of k' such that q splits into a product of linear factors in $K[x]$. Consequently, f splits into a product of linear factors in $K[x]$. @col If f is not irreducible, then $f = gh$ for some $g, h \in k[x]$, with $\deg g, \deg h < \deg f$. So, by the induction hypothesis, there is a field extension k' of k such that g is a product of linear factors in $k'[x]$. @col Hence, $f = (x - \alpha_1) \cdots (x - \alpha_n)h$ in $k'[x]$. Since $\deg h < \deg f$, by the inductive hypothesis there exists a field extension K of k' such that h splits into linear factors in $K[x]$. @col Hence, f is a product of linear factors in $K[x]$. @qed@endcol@end

13.4 Finite Fields

Recall:

Definition 13.12. *Let R be a ring with additive and multiplicative identity elements 0, 1, respectively. The* **characteristic** $\operatorname{char} R$ *of R is the smallest positive integer n such that:*

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If such an integer does not exist, we say that the ring has **characteristic zero**.

Example 13.13.
- *The ring $\mathbb{Q}$ has characteristic zero.*
- $\operatorname{char} \mathbb{Z}_6 = 6$.

Exercise 13.14. *If a ring R as finitely many elements, then it has positive (i.e. nonzero) characteristic.*

Claim 13.15. *If a field F has positive characteristic* $\operatorname{char} F$*, then* $\operatorname{char} F$ *is a prime number.*

Example 13.16. $\operatorname{char} \mathbb{F}_5 = 5$, *which is prime.*

Remark. *Note that all finite rings have positive characteristics, but there are rings with positive characteristics which have infinitely many elements, e.g. the polynomial ring $\mathbb{F}_5[x]$.*

Claim 13.17. *Let F be a finite field. Then, the number of elements of F is equal to p^n for some prime p and $n \in \mathbb{N}$.*

Proof. Since F is finite, it has finite characteristic. Since it is a field, $\operatorname{char} F$ is a prime p.

Exercise: $\mathbb{F}_p$ is isomorphic to a subfield of F.

Viewing $\mathbb{F}_p$ as a subfield of F, we see that F is a vector space over $\mathbb{F}_p$. Since the cardinality of F is finite, the dimension n of F over $\mathbb{F}_p$ must necessarily be finite.

Hence, there exist n basis elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ in F, such that each element of F may be expressed uniquely as:

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n,$$

where $c_i \in \mathbb{F}_p$.

Since $\mathbb{F}_p$ has p elements, it follows that F has p^n elements. □

Claim 13.18. *Let k be a field, f a nonzero irreducible polynomial in $k[x]$, then $k[x]/(f)$ is a vector space of dimension $\deg f$ over k.*

Proof. Let $K = k[t]/(f(t))$, then K is a field extension of k which contains a root α of f, namely, $\alpha = t + (f(t))$.

It is clear that $K = k(\alpha)$, since any element in $K = k[t]/(f(t))$ has the form $\sum b_i\alpha^i$, where $b_i \in k$.

On the other hand, by Theorem 13.4, every element in $k(\alpha)$ may be expressed uniquely in the form:

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in k,\ n = \deg f,$$

which shows that $K = k(\alpha)$ is a vector space of dimension $\deg f$ over k.

Since K is simply $k[x]/(f)$ with the variable x replaced with t, we conclude that $k[x]/(f)$ is a vector space of dimension $\deg f$ over k. □

Corollary 13.19. *If k is a finite field with $|k|$ elements, and f is an irreducible polynomial of degree n in $k[x]$, then the field $k[x]/(f)$ has $|k|^n$ elements.*

Example 13.20. *Let $p = 2$, $n = 2$. To construct a finite field with $p^n = 4$ elements. We first start with the finite field $\mathbb{F}_2$, then try to find an irreducible polynomial $f \in \mathbb{F}_2[x]$ such that $\mathbb{F}_2[x]/(f)$ has 4 elements.*

Based on our discussion so far, the degree of f should be equal to $n = 2$, since n is precisely the dimension of the desired finite field over $\mathbb{F}_2$.

Consider $f = x^2 + x + 1$. Since p is of degree 2 and has no root in $\mathbb{F}_2$, it is irreducible in $\mathbb{F}_2[x]$. Hence, $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field with 4 elements.

Theorem 13.21. *(**Galois**) Given any prime p and $n \in \mathbb{N}$, there exists a finite field F with p^n elements.*

Proof. (Not within the scope of the course.)

Consider the polynomial:

$$f = x^{p^n} - x \in \mathbb{F}_p[x]$$

By Kronecker's theorem, there exists a field extension K of $\mathbb{F}_p$ such that f splits into a product of linear factors in $K[x]$. Let:

$$F = \{\alpha \in K : f(\alpha) = 0\}.$$

Exercise 13.22. *Let $g = (x - a_1)(x - a_2)\cdots(x - a_n)$ be a polynomial in $k[x]$, where k is a field. Show that the roots $a_1, a_2, \ldots, a_n$ are distinct if and only if $gcd(g, g') = 1$, where g' is the derivative of g.*

In this case, we have $f' = p^n x^{p^n-1} - 1 = -1$ in $\mathbb{F}_p[x]$. Hence, $gcd(f, f') = 1$, which implies by the exercise that the roots of f are all distinct. So, f has p^n distinct roots in K, hence F has exactly p^n elements.

It remains to show that F is a field. Let $q = p^n$. By definition, an element $a \in K$ belongs to F if and only if $f(a) = a^q - a = 0$, which holds if and only if $a^q = a$. For $a, b \in F$, we have:

$$(ab)^q = a^q b^a = ab,$$

which implies that F is closed under multiplication. Since K, being a extension of $\mathbb{F}_p$, has characteristic p. we have $(a + b)^p = a^p + b^p$. Hence,

$$\begin{aligned}(a+b)^q = (a+b)^{p^n} &= ((a+b)^p)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} \\ &= (a^p + b^p)^p)^{p^{n-2}} = (a^{p^2} + b^{p^2})^{p^{n-2}} \\ &= \cdots = a^{p^n} + b^{p^n} = a + b,\end{aligned}$$

which implies that F is closed under addition.

Let $0, 1$ be the additive and multiplicative identity elements, respectively, of K. Since $0^q = 0$ and $1^q = 1$, they are also the additive and multiplicative identity elements of F.

For nonzero $a \in F$, we need to prove the existence of the additive and multiplicative inverses of a in F.

Let $-a$ be the additive inverse of a in K. Since $(-1)^q = -1$ (even if $p = 2$, since $1 = -1$ in $\mathbb{F}_2$), we have:

$$(-a)^q = (-1)^q a^q = -a,$$

so $-a \in F$. Hence, $a \in F$ has an additive inverse in F. Since $a^q = a$ in K, we have:

$$a^{q-2}a = a^{q-1} = 1$$

in K. Since $a \in F$ and F is closed under multiplication, $a^{q-2} = \underbrace{a \cdots a}_{q-2 \text{ times}}$ lies in F. So, a^{q-2} is a multiplicative inverse of a in F. $\square$