Section 33 – Finite fields

Instructor: Yifan Yang

Spring 2007
Corollary (23.6)
Let $G$ be a finite subgroup of the multiplicative group of nonzero elements in a field $F$, then $G$ is cyclic.

Theorem (27.19)
A field is either of prime characteristic $p$ containing a subfield isomorphic to $\mathbb{Z}_p$, or of characteristic 0 containing a subfield isomorphic to $\mathbb{Q}$.
In essence, if a field is of characteristic $p$, then it is an extension field of $\mathbb{Z}_p$. If a field is of characteristic 0, then it is an extension field of $\mathbb{Q}$. 
Theorem
If $E$ is an extension field of a field $F$, then $E$ is a vector space over $F$.

Definition
If the dimension of $E$ over $F$ is finite, then $E$ is a finite extension of $F$, and the dimension of $E$ over $F$ is called the degree of $E$ over $F$ and denoted by $[E : F]$.

Theorem
Every finite-dimensional vector space over a field contains a basis.
Finite fields

**Theorem (33.1)**

*Let $E$ be a finite extension of degree $n$ over a finite field $F$. If $F$ has $q$ elements, then $E$ has $q^n$ elements.*

**Proof.**

The vector space $E$ contains a basis $\{\alpha_1, \ldots, \alpha_n\}$ and each element $\beta \in E$ is uniquely expressed as $b_1\alpha_1 + \cdots + b_n\alpha_n$. Since each $b_i$ has $q$ possible different choices, $E$ has $q^n$ elements.

**Corollary (33.2)**

If $E$ is a finite field of characteristic $p$, then the number of elements in $E$ is $p^n$ for some positive integer $n$. 

Explicit construction of finite fields

Idea.

- Theorem 33.1 asserts that if $E$ is a finite extension of degree $n$ over $\mathbb{Z}_p$, then $E$ has $p^n$ elements.
- Thus, to construct a field of $p^n$ elements, we look for an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ of degree $n$.
- Let $\alpha$ be a zero of $f(x)$. Then $\mathbb{Z}[\alpha]$ is a field of $p^n$ elements. (See the slides for Section 29.)
Example

Problem. Construct a field of 16 elements.

Solution.

- We look for an irreducible polynomial of degree 4 over $\mathbb{Z}_2$.
- Such a polynomial takes the form $x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$, where $a_i \in \mathbb{Z}_2$.
- 0 cannot be a zero, so $a_4 = 1$.
- 1 cannot be a zero, so $a_1 + a_2 + a_3 + a_4 = 0$ (in $\mathbb{Z}_2$).
- Thus, there are only 4 possibilities remained $x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$, and $x^4 + x^3 + x^2 + x + 1$.
- Among them, we have $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. The others are irreducible.
- Pick any of $x^4 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x^3 + x^2 + x + 1$. Let $\alpha$ be a zero of the polynomial. Then $\mathbb{Z}_2[\alpha]$ is a field of 16 elements.
Example, continued

Problem. Assume that we pick $x^4 + x + 1 \in \mathbb{Z}_2[x]$, and let $\alpha$ be a zero of $x^4 + x + 1$. Find an element of $\mathbb{Z}_2[\alpha]$ that generates the cyclic group $\mathbb{Z}_2[\alpha]^\times$.

Solution.

- Note that the cyclic group of nonzero elements in $\mathbb{Z}_2[\alpha]$ has order 15.
- Thus, if an element $\beta$ satisfies $\beta, \beta^3, \beta^5 \neq 1$, then $\beta$ has order 15.
- Let $\alpha$ be a zero of $x^4 + x + 1 \in \mathbb{Z}_2[x]$. We have $\alpha, \alpha^3 \neq 1$.
- Also, $\alpha^5 = \alpha(\alpha^4 + \alpha + 1) + \alpha^2 + \alpha = \alpha^2 + \alpha \neq 1$.
- Thus, $\alpha$ generates the cyclic group of nonzero elements in $\mathbb{Z}_2[\alpha]$. 
In-class exercises

Find an irreducible polynomial of the given degree over the given field.

1. degree 3 over $\mathbb{Z}_3$.
2. degree 3 over $\mathbb{Z}_5$. 
Theorem (33.3)

Let $E$ be a field of $p^n$ elements contained in an algebraic closure $\overline{\mathbb{Z}_p}$ of $\mathbb{Z}_p$. Then the elements of $E$ are precisely the zeros of $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Proof.

By Lagrange’s theorem, every nonzero element of $E$ is a zero of $x^{p^n-1} - 1$. Thus, every element of $E$ is a zero of $x^{p^n} - x = x(x^{p^n-1} - 1)$. On the other hand, since $\mathbb{Z}_p$ is a field, a polynomial of degree $p^n$ has at most $p^n$ zeros. Therefore, the elements of $E$ are precisely the zeros of $x^{p^n} - x$. \qed
Corollary (23.6)
The multiplicative group $F^\times$ of nonzero elements in a finite field $F$ is cyclic.

Definition
An element $\alpha$ in a field $F$ is an $n$th root of unity if $\alpha^n = 1$. It is a primitive $n$th root of unity if $\alpha^m \neq 1$ for $0 < m < n$.

Corollary (33.6)
A finite extension $E$ of a finite field $F$ is a simple extension of $F$.

Proof.
Let $\alpha$ be a generator of the multiplicative group $E^\times$. Then clearly, $E = F(\alpha)$. \qed
Existence of finite fields of $p^n$ elements

Theorem (33.10)

A finite field of $p^n$ elements exists for every prime power $p^n$.

Main idea of proof.

- In Theorem 33.3, we have shown that if $E$ is a field of $p^k$ elements contained in $\mathbb{Z}_p$, then the elements of $E$ are precisely the zeros of $x^{p^k} - x$ in $\mathbb{Z}_p$.
- Here we will show the converse is true. That is, the set $S$ of zeros of $x^{p^n} - x$ in $\mathbb{Z}_p$ forms a field of $p^n$ elements.
- Note that since $\mathbb{Z}_p$ is algebraically closed, $x^{p^n} - x$ factors completely into linear factors over $\mathbb{Z}_p$.
- We will show
  - The zeros of $x^{p^n} - x$ are all distinct so that $S$ has $p^n$ elements.
  - $S$ is a subdomain in $\mathbb{Z}_p$. Since $S$ has finitely many elements, this implies that $S$ is a field.
Derivation

Definition
Let $F$ be a field. The map $D : F[x] \to F[x]$ defined by $D(a_0 + a_1 x + \cdots + a_n x^n) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ is called the derivation, and $D(f(x))$ is called the derivative of $f(x)$.

Lemma
Let $F$ be a field. The derivation $D$ on $F[x]$ satisfies

- $D(f + g) = D(f) + D(g)$.
- $D(fg) = gD(f) + fD(g)$.

Proof.
By direct verification.
Proof of $|S| = p^n$

- Suppose that $\alpha$ is a repeated zero of $x^{p^n} - x$, say, $x^{p^n} - x = (x - \alpha)^2g(x)$ for some $g(x) \in \mathbb{Z}_p[x]$.

- We have
  $$D((x - \alpha)^2g(x)) = 2(x - \alpha)g(x) + (x - \alpha)^2D(g(x)).$$
  Thus, $\alpha$ is also a zero of
  $$D((x - \alpha)^2g(x)) = D(x^{p^n} - x) = p^n x^{p^n-1} - 1.$$

- Since the characteristic is $p$, the last polynomial is just $-1$, which has no zeros at all.

- Therefore, $x^{p^n} - x$ has no repeated root.
Proof that \( S \) is an integral domain

- We need to show that
  - \( 0, 1 \in S \).
  - If \( \alpha \in S \), then so is \(-\alpha\).
  - If \( \alpha, \beta \in S \), then so are \( \alpha + \beta \) and \( \alpha \beta \).

- 0 and 1 clearly satisfy \( x^{p^n} - x = 0 \).

- Assume that \( \alpha^{p^n} - \alpha = 0 \). If \( p = 2 \), then \(-\alpha = \alpha \in S \). If \( p \) is odd, then \((-\alpha)^{p^n} - (-\alpha) = -(\alpha^{p^n} - \alpha) = 0\), and \(-\alpha \in S \).

- If \( \alpha \) and \( \beta \) are zeros of \( x^{p^n} - x \), then \( (\alpha \beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha \beta \) and \( \alpha \beta \) is in \( S \).

- Recall that \( p | \binom{p}{k} \) for \( 1 \leq k \leq p - 1 \). Thus
  \[(u + v)^p = u^p + v^p \text{ for all } u, v \in \mathbb{Z}_p.\]
  Then, \( (\alpha + \beta)^{p^n} = ((\alpha + \beta)^p)^{p^{n-1}} = ((\alpha^p + \beta^p)^{p^{n-1}} = \cdots = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta.\)
  Therefore, \( \alpha + \beta \in S.\)
Galois fields $GF(p^n)$

Corollary (33.11)
Let $F$ be a field. Then for every positive integer $n$, there exists an irreducible polynomial of degree $n$ over $F$.

Theorem (33.12)
Let $F$ and $F'$ be two fields of order $p^n$. Then $F$ and $F'$ are isomorphic.

Definition
The unique field of $p^n$ (up to isomorphism) is called the Galois field of order $p^n$. 
Proof of Theorem 33.12

- Assume that $F$ and $F'$ are fields of $p^n$ elements.
- Since $F$ and $F'$ are both algebraic extensions of $\mathbb{Z}_p$, $F$ and $F'$ are isomorphic to some subfields of order $p^n$ in $\overline{\mathbb{Z}}_p$.
- However, in $\overline{\mathbb{Z}}_p$, there is only one subfield of order $p^n$, namely, the set of all zeros of $x^{p^n} - x$ in $\overline{\mathbb{Z}}_p$.
- In other words, $F$ and $F'$ are both isomorphic to this subfield of $p^n$ elements in $\overline{\mathbb{Z}}_p$. □
Example

- Let $\alpha$ be a zero of $x^3 + x + 1$ in $\mathbb{Z}_2[x]$.
- Since $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$, $\mathbb{Z}_2[\alpha]$ is a field of 8 elements.
- Theorem 33.3 says that $\alpha$ is a zero of $x^8 - x$. This implies that $x^3 + x + 1$ is a factor of $x^8 - x$.
- Indeed, we have $x^8 - x = x(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$.
- Note that $x^3 + x^2 + 1$ is also irreducible over $\mathbb{Z}_2$, giving rise to the field $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$ of 8 elements.
Example

**Question.** Observe that over $\mathbb{Z}_2$ we have $x^{16} - x = x(x - 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$, where the factors are all irreducible. Why isn’t there any polynomial of degree 3 in the factorization?

**Answer.**

- Suppose that an irreducible factor $f(x)$ of $x^{16} - x$ has degree 3.
- Let $\alpha$ be a zero of $f(x)$. Then $[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2] = \deg f = 3$.
- However, by Theorem 31.4, we must have $4 = [GF(16) : \mathbb{Z}_2] = [GF(16) : \mathbb{Z}_2[\alpha]][\mathbb{Z}_2[\alpha] : \mathbb{Z}_2] = 3[GF(16) : \mathbb{Z}_2[\alpha]]$, which is absurd.
Galois fields

Theorem
In $\mathbb{Z}_p$, $GF(p^m)$ is contained in $GF(p^n)$ if and only if $m|n$.

Proof.
The argument in the above example shows that $GF(p^m) \leq GF(p^n)$ implies $m|n$. Conversely, assume that $m|n$. It suffices to prove that if $\alpha \in \mathbb{Z}_p$ is a zero of $x^{p^m} - x$, then it is also a zero of $x^{p^n} - x$. Now $\alpha^{p^n} = (\alpha^{p^m})^{p^{n-m}} = \alpha^{p^{n-m}} = \alpha^{p^{n-2m}} = \cdots$. Since $m|n$, eventually we arrive at $\alpha^{p^n} = \alpha$.

Corollary
The polynomial $x^{p^n} - x$ is equal to the product of all monic irreducible polynomial over $\mathbb{Z}_p$ with degree $d$ dividing $n$. 

Over \( \mathbb{Z}_2 \), we have

\[
x^{64} - x = x(x + 1)(x^2 + x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \\
\quad \times (x^6 + x + 1)(x^6 + x^3 + 1)(x^6 + x^5 + 1) \\
\quad \times (x^6 + x^4 + x^2 + x + 1)(x^6 + x^4 + x^3 + x + 1) \\
\quad \times (x^6 + x^5 + x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1) \\
\quad \times (x^6 + x^5 + x^4 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).
\]
Homework

Problems 4, 6, 9, 10, 13, 14 of Section 33.