Section VI.33. Finite Fields

Note. In this section, finite fields are completely classified. For every prime p and $n \in \mathbb{N}$, there is exactly one (up to isomorphism) field of order p^n, called the *Galois field* of order p^n, denoted $GF(p^n)$. These are the only 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.

Note. Recall Definition 19.13: If for a ring R a positive integer n exists such that $n \cdot a = a + a + \cdots + a = 0$ for all $a \in R$, then the least such positive integer n is the *characteristic* of the ring R. If no such n exists then ring R is of *characteristic* 0. Also, every field is an integral domain (Theorem 19.9) and the characteristic of an integral domain is either 0 or some prime p (Exercise 19.29).

Lemma 1. If F is a field of characteristic p then F has a subfield isomorphic to $\mathbb{Z}_p$.

Proof. since $1 \in F$, then 1 is of characteristic p and $p \cdot 1 = 1 + 1 + \cdots + 1 = 0$. So $\langle 1 \rangle$ is a subgroup of F under addition isomorphic to $\langle \mathbb{Z}_p, + \rangle$. By Corollary 19.12, $\mathbb{Z}_p$ is a field. So F has a subfield isomorphic to $\mathbb{Z}_p$. ∎

Corollary 33.2. If E is a finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.

Proof. By Lemma 1, E has a subfield isomorphic to $\mathbb{Z}_p$. So E is a finite extension field of $\mathbb{Z}_p$ and by Theorem 33.1 E is of order p^n for some $n \in \mathbb{N}$. ∎

Theorem 33.3. Let E be a field of p^n elements contained in an algebraic closure $\overline{\mathbb{Z}}_p$ of $\mathbb{Z}_p$. The elements of E are precisely the zeros in $\overline{\mathbb{Z}}_p$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Note. With $n = 1$ in Theorem 33.3, we see that every element of $\mathbb{Z}_p$ is a zero of $x^p - x$. This is because every nonzero element of $\langle \mathbb{Z}_p, + \rangle$ generates $\langle \mathbb{Z}_p, \rangle$.

Definition 33.4. An element α of a field F is an n^{th} *root of unity* if $\alpha^n = 1$. it is a *primitive* n^{th} *root of unity* if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.

Note. The primitive nth roots of unity in field $\mathbb{C}$ are each generators of $\langle U_n, \cdot \rangle$. The nonzero elements of a finite field of p^n elements are the $(p^n - 1)^{\text{th}}$ roots of unity in the field.

Theorem 33.5. Let F be a finite field and let F^* be the nonzero elements of F. The group $\langle F^*, \cdot \rangle$ is cyclic.

Proof. This is Corollary 23.6 from page 213. ∎

Corollary 33.6. If finite field E is an extension of a finite field F, then E is a simple extension of F.

Proof. By Theorem 33.5 the nonzero elements of E form a cyclic multiplicative group. Let α be a generator of this group. Then $E = F(\alpha)$. ∎

Note. The following humble-looking result is key to the classification of finite fields.

Lemma 33.8. If F is a field of prime characteristic p with algebraic closure $\overline{F}$, then $x^{p^n} - x$ has p^n distinct zeros in $\overline{F}$.

Lemma 33.9. If F is a field of prime characteristic p, then $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ for all $\alpha, \beta \in F$ and for all $n \in \mathbb{N}$.

Note. Now for the classification of finite fields.

Theorem 33.10. A finite field $GF(p^n)$ of p^n elements exists for every prime power p^n.

Note. We now take a result from Joseph Gallian's *Contemporary Abstract Algebra* 8th Edition, Brooks/Cole, 2013 (see Chapter 22). Uniqueness of $GF(p^n)$ follows from this result. Though the result is from Gallian, Fraleigh has given us the background to prove it.

Theorem. Structure of Finite Fields.

As a group under addition, the Galois field $GF(p^n)$ is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n times). That is, elements add as n-tuples of elements of $\mathbb{Z}_p$. As a group under multiplication, the set of nonzero elements of $GF(p^n)$ is isomorphic to $\mathbb{Z}_{p^n-1}$.

Proof. Every field is an integral domain (Theorem 19.9) and the characteristic of an integral domain is either 0 or some prime p (Exercise 19.29). So $GF(p^n)$ has characteristic p. (Consider the element 1 and the subgroup it generates under addition. This subgroup has order the same as the characteristic of 1 and this subgroup has an order that divides the order of the additive group determined by $GF(p^n)$ (by Lagrange's Theorem, Theorem 10.10). So the characteristic of 1 is a prime divisor of p^n and so must be p. By Theorem 19.15, this is the characteristic of the field $GF(p^n)$ [and so p is the characteristic of any subfield of $GF(p^n)$]). Since $GF(p^n)$ forms a finite group under addition, then we can apply the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12) to it to conclude that $GF(p^n) \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_r}}$ for some primes $p_1, p_2, \ldots, p_r$ and some $n_1, n_1, \ldots, n_r \in \mathbb{N}$. This means that $GF(p^n)$ then contains elements of orders $p_i^{n_1}, p_2^{n_2}, \ldots, p_r^{n_r}$, but since every element of $GF(p^n)$ is of characteristic p, then it must be that $p_1 = p_2 = \cdots = p_r = p$ and $n_1 = n_2 = \cdots = n_r = 1$ (alternatively, we have that the order of $GF(p^n)$ would be $p^n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ which implies the same conditions on the p_i and n_i). So as an additive group, $GF(p^n) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n times). By Theorem 33.5, the $p^n - 1$ nonzero elements of $GF(p^n)$ form a cyclic group under multiplication and so is isomorphic to $\mathbb{Z}_{p^n-1}$ by Theorem 6.10. ∎

Corollary 1. $GF(p^n)$ forms a vector space of dimension n over $GF(p)$. That is, $[GF(p^n) : GF(p)] = n$.

Proof. Since we know that $GF(p^n)$ as an additive group is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n times), then we just need to find a basis for this over $GF(P) \cong \mathbb{Z}_p$. A basis of n elements is $\{(1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)\}$, and the result follows. ∎

Corollary 2. Let α be a generator of the group of nonzero elements of $GF(p^n)$ under multiplication. Then α is algebraic over $GF(p)$ of degree n. That is, $\deg(\alpha, GF(p)) = n$.

Proof. Since α generates all nonzero elements of $GF(p^n)$ (under multiplication) and $0 \in GF(p)$, then $GF(p)(\alpha) = GF(p^n)$. So by Corollary 1, $[GF(p)(\alpha) : GF(p)] = [GF(p^n) : GF(p)] = n$. Also, since α generates all nonzero elements of $GF(p^n)$, then α generates 1 and so $\alpha^m = 1$ for some $m \in \mathbb{N}$. Therefore α is algebraic over $GF(p)$ since α is a zero of $p(x) = x^m - 1 \in GF(p)[x]$. If $\deg(\alpha, GF(p)) = \ell$, then $GF(p)(\alpha) = GF(p^n)$ is an ℓ-dimensional vector space over $GF(p)$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\}$ by Theorem 30.23. But all bases of $GF(p^n)$ have the same size by Corollary 30.20, so $\deg(\alpha, GF(p)) = \ell = n$. ∎

Corollary 33.11. If F is any finite field, then for every positive integer n, there is an irreducible polynomial in $F[x]$ of degree n.

Note. Corollary 33.11 implies that no finite field is algebraically closed!

Note. Fraleigh states in Theorem 33.12 that for any prime p and $n \in \mathbb{N}$, if E and E' are fields of order p^n, then $E \cong E'$. We have covered this in the Structure of Finite Fields theorem.

Note. To clarify, by combining Exercise 19.29, Corollary 33.2, Theorem 33.10, and the Structure of Finite Feilds theorem, we see that:

> **Fundamental Theorem of Finite Fields.** A finite field of order m exists if and only if $m = p^n$ for some prime p and some $n \in \mathbb{N}$. In addition, all fields of order p^n are isomorphic.

Note. We have a clear idea of the structure of finite fields $GF(p)$ since $GF(p) \cong \mathbb{Z}_p$. However the structure of $GF(p^n)$ for $n \geq 1$ is unclear. We now give an example of a finite field of order 16.

Example. (Example 1, page 390 of Gallian.)
We construct $GF(16)$. Of course, $GF(16)$ is of characteristic 2 (by Exercise 19.29—for details see the proof of the Structure of Finite Fields theorem). So by Lemma 1, $GF(16)$ has $\mathbb{Z}_2$ as a subfield. So we will construct $GF(16)$ as an algebraic extension field of $\mathbb{Z}_2$. By Note 29.1 (or Case I an page 270 of Fraleigh), $F[x]/\langle \text{irr}(\alpha, F) \rangle$ is an extension field of field F where $\alpha \notin F$ is algebraic over F. So we want to find an

irreducible polynomial $p(x) \in \mathbb{Z}_2[x]$ of degree 4. Then the elements of $\mathbb{Z}_2[x]/\langle p(x)\rangle$ will be polynomials of degree 3 or less (details to follow) and there will be $2^4 = 16$ such polynomials.

Let $p(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Since neither 0 nor 1 is a zero of $p(x)$ then it has no linear factors. The only possible quadratic factors are $x^2 + x + 1$ and $x^2 + 1$, and neither of these is a factor. So $p(x)$ is irreducible. We take the elements of $\mathbb{Z}_2[x]/\langle p(x)\rangle$ to be cosets of $\langle p(x)\rangle$ in which addition is done as usual in $\mathbb{Z}_2[x]$ but multiplication is done "modulo $p(x)$" (since the nonzero elements form a cyclic group under multiplication by the Structure of Finite Fields theorem and every multiple of $p(x)$ is in $\langle p(x)\rangle$). Since products of polynomials will be reduced modulo $p(x)$ (that is, computed in the usual way but then replaced by the remainder when the usual product is divided by $p(x)$), then all elements of $\mathbb{Z}_2[x]/\langle p(x)\rangle$ will be represented by polynomials of degree 3 or less (and hence there will be $2^4 = 16$ of them). So, in terms of representatives, the elements of $GF(16)$ are $\{ax^3 + bx^2 + cx + d \mid a, b, c, d \in \mathbb{Z}_2\}$. We denote these as:

$$
\begin{aligned}
g_0 &= 0x^3 + 0x^2 + 0x + 0 & g_8 &= 1x^3 + 0x^2 + 0x + 0\\
g_1 &= 0x^3 + 0x^2 + 0x + 1 & g_9 &= 1x^3 + 0x^2 + 0x + 1\\
g_2 &= 0x^3 + 0x^2 + 1x + 0 & g_{10} &= 1x^3 + 0x^2 + 1x + 0\\
g_3 &= 0x^3 + 0x^2 + 1x + 1 & g_{11} &= 1x^3 + 0x^2 + 0x + 1\\
g_4 &= 0x^3 + 1x^2 + 0x + 0 & g_{12} &= 1x^3 + 1x^2 + 0x + 0\\
g_5 &= 0x^3 + 1x^2 + 0x + 1 & g_{13} &= 1x^3 + 1x^2 + 0x + 1\\
g_6 &= 0x^3 + 1x^2 + 1x + 0 & g_{14} &= 1x^3 + 1x^2 + 1x + 0\\
g_7 &= 0x^3 + 1x^2 + 1x + 1 & g_{15} &= 1x^3 + 1x^2 + 1x + 1
\end{aligned}
$$

The addition table is then:

$+$	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_0	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_1	g_1	g_0	g_3	g_2	g_5	g_4	g_7	g_6	g_9	g_8	g_{11}	g_{10}	g_{13}	g_{12}	g_{15}	g_{14}
g_2	g_2	g_3	g_0	g_1	g_6	g_7	g_4	g_5	g_{10}	g_{11}	g_8	g_9	g_{14}	g_{15}	g_{12}	g_{13}
g_3	g_3	g_2	g_1	g_0	g_7	g_6	g_5	g_4	g_{11}	g_{10}	g_9	g_8	g_{15}	g_{14}	g_{13}	g_{12}
g_4	g_4	g_5	g_6	g_7	g_0	g_1	g_2	g_3	g_{12}	g_{13}	g_{14}	g_{15}	g_8	g_9	g_{10}	g_{11}
g_5	g_5	g_4	g_7	g_6	g_1	g_0	g_3	g_2	g_{13}	g_{12}	g_{15}	g_{14}	g_9	g_8	g_{11}	g_{10}
g_6	g_6	g_7	g_4	g_5	g_2	g_3	g_0	g_1	g_{14}	g_{15}	g_{12}	g_{13}	g_{10}	g_{11}	g_8	g_9
g_7	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_0	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8
g_8	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
g_9	g_9	g_8	g_{11}	g_{10}	g_{13}	g_{12}	g_{15}	g_{14}	g_1	g_0	g_3	g_2	g_5	g_4	g_7	g_6
g_{10}	g_{10}	g_{11}	g_8	g_9	g_{14}	g_{15}	g_{12}	g_{13}	g_2	g_3	g_0	g_1	g_6	g_7	g_4	g_5
g_{11}	g_{11}	g_{10}	g_9	g_8	g_{15}	g_{14}	g_{13}	g_{12}	g_3	g_2	g_1	g_0	g_7	g_6	g_5	g_4
g_{12}	g_{12}	g_{13}	g_{14}	g_{15}	g_8	g_9	g_{10}	g_{11}	g_4	g_5	g_6	g_7	g_0	g_1	g_2	g_3
g_{13}	g_{13}	g_{12}	g_{15}	g_{14}	g_9	g_8	g_{11}	g_{10}	g_5	g_4	g_7	g_6	g_1	g_0	g_3	g_2
g_{14}	g_{14}	g_{15}	g_{12}	g_{13}	g_{10}	g_{11}	g_8	g_9	g_6	g_7	g_4	g_5	g_2	g_3	g_0	g_1
g_{15}	g_{15}	g_{14}	g_{13}	g_{12}	g_{11}	g_{10}	g_9	g_8	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_0

Multiplication can be trickier. Consider

$$g_{15}g_{11} = (x^3 + x^2 + x + 1)(x^3 + x) = x^6 + x^5 + x^2 + x \equiv x^3 + x^2 = g_{12}$$

since in $\mathbb{Z}_2$:

$$\frac{x^6 + x^5 + x^2 + x}{x^4 + x + 1} = x^2 + x + \frac{x^3 + x^2}{x^4 + x + 1}.$$

Now we know the nonzero elements of $GF(16)$ form a cyclic group of order 15

under multiplication. So if we can find a generator of this group, then creation of a multiplication table is simplified. In this example, $g_2 = x$ is a generator since

$$\begin{aligned}
g_2 &= x = g_2 \\
g_2^2 &= x^2 = g_4 \\
g_2^3 &= x^3 = g_8 \\
g_2^4 &= x^4 \equiv x + 1 = g_3 \\
g_2^5 &= x(x+1) = x^2 + x = g_6 \\
g_2^6 &= x(x^2 + x) = x^3 + x^2 = g_{12} \\
g_2^7 &= x(x^3 + x^2) = x^4 + x^3 \equiv x^3 + x + 1 = g_{11} \\
g_2^8 &= x(x^3 + x + 1) = x^4 + x^2 + x \equiv x^2 + 1 = g_5 \\
g_2^9 &= x(x^2 + 1) = x^3 + x = g_{10} \\
g_2^{10} &= x(x^3 + x) = x^4 + x^2 \equiv x^2 + x + 1 = g_7 \\
g_2^{11} &= x(x^2 + x + 1) = x^3 + x^2 + x =_{14} \\
g_2^{12} &= x(x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x \equiv x^3 + x^2 + 1 = g_{15} \\
g_2^{13} &= x(x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x \equiv x^3 + x^2 + 1 = g_{13} \\
g_2^{14} &= x(x^3 + x^2 + 1) = x^4 + x^3 + x = x^3 + 1 = g_9 \\
g_2^{15} &= x(x^3 + 1) = x^4 + 1 \equiv 1 = g_1
\end{aligned}$$

Therefore, we get the following multiplication table for $GF(16)$:

$\cdot$	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0	g_0
g_1	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
g_2	g_0	g_2	g_4	g_6	g_8	g_{10}	g_{12}	g_{14}	g_3	g_1	g_7	g_5	g_{11}	g_9	g_{15}	g_{13}
g_3	g_0	g_3	g_6	g_5	g_{12}	g_{15}	g_{10}	g_9	g_{11}	g_8	g_{13}	g_{14}	g_7	g_4	g_1	g_2
g_4	g_0	g_4	g_8	g_{12}	g_3	g_7	g_{11}	g_{15}	g_6	g_2	g_{14}	g_{10}	g_5	g_1	g_{13}	g_9
g_5	g_0	g_5	g_{10}	g_{15}	g_7	g_2	g_{13}	g_8	g_{14}	g_{11}	g_4	g_1	g_9	g_{12}	g_3	g_6
g_6	g_0	g_6	g_{12}	g_{10}	g_{11}	g_{13}	g_7	g_1	g_5	g_3	g_9	g_{15}	g_{14}	g_8	g_2	g_4
g_7	g_0	g_7	g_{14}	g_9	g_{15}	g_8	g_1	g_6	g_{13}	g_{10}	g_3	g_4	g_2	g_5	g_{12}	g_{11}
g_8	g_0	g_8	g_3	g_{11}	g_6	g_{14}	g_5	g_{13}	g_{12}	g_4	g_{15}	g_7	g_{10}	g_2	g_9	g_1
g_9	g_0	g_9	g_1	g_8	g_2	g_{11}	g_3	g_{10}	g_4	g_{13}	g_5	g_{12}	g_6	g_{15}	g_7	g_{14}
g_{10}	g_0	g_{10}	g_7	g_{13}	g_{14}	g_4	g_9	g_3	g_{15}	g_5	g_8	g_2	g_1	g_{11}	g_6	g_{12}
g_{11}	g_0	g_{11}	g_5	g_{14}	g_{10}	g_1	g_{15}	g_4	g_7	g_{12}	g_1	g_9	g_{13}	g_6	g_8	g_3
g_{12}	g_0	g_{12}	g_{11}	g_7	g_5	g_9	g_{14}	g_2	g_{10}	g_6	g_1	g_{13}	g_{15}	g_3	g_4	g_8
g_{13}	g_0	g_{13}	g_9	g_4	g_1	g_{12}	g_8	g_5	g_2	g_{15}	g_{11}	g_6	g_3	g_{14}	g_{10}	g_7
g_{14}	g_0	g_{14}	g_{15}	g_1	g_{13}	g_3	g_2	g_{12}	g_9	g_7	g_6	g_8	g_4	g_{10}	g_{11}	g_5
g_{15}	g_0	g_{15}	g_{13}	g_2	g_9	g_6	g_4	g_{11}	g_1	g_{14}	g_{12}	g_3	g_8	g_7	g_5	g_{10}

We comment that any two irreducible polynomials of the same degree over $\mathbb{Z}_p[z]$ yield isomorphic fields through this technique (Gallian, page 392). In this example, it is a bit of a coincidence that $g_2 = x$ is a generator for the nonzero elements of $GF(16)$—in fact, the element which generates the nonzero elements is dependent on the choice of the irreducible polynomial.

Revised: 3/2/2014