Historical Note

Although Carl F. Gauss had shown that the set of residues modulo a prime p satisfied the field properties, it was Evariste Galois (1811–1832) who first dealt with what he called "incommensurable solutions" to the congruence $F(x) \equiv 0 \pmod{p}$, where $F(x)$ is an nth degree irreducible polynomial modulo p. He noted in a paper written in 1830 that one should consider the roots of this congruence as "a variety of imaginary symbols" that one can use in calculations just as one uses $\sqrt{-1}$. Galois then showed that if α is any solution of $F(x) \equiv 0 \pmod{p}$, the expression $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$ takes on precisely p^n different values. Finally, he proved results equivalent to Theorems 42.3 and 42.5 of the text.

Galois' life was brief and tragic. He showed brilliance in mathematics early on, publishing several papers before he was 20 and essentially established the basic ideas of Galois theory. He was, however, active in French revolutionary politics following the July revolution of 1830. In May 1831, he was arrested for threatening the life of King Louis-Philippe. Though he was acquitted, he was rearrested for participating, heavily armed, in a republican demonstration on Bastille Day of that year. Two months after his release from prison the following March, he was killed in a duel, "the victim of an infamous coquette and her two dupes"; the previous night he had written a letter to a friend clarifying some of his work in the theory of equations and requesting that it be studied by other mathematicians. Not until 1846, however, were his major papers published; it is from that date that his work became influential.

The primitive 5th roots of unity in $\mathbb{Z}_{11}$ are of the form 2^m, where the gcd of m and 10 is 2, that is,

$$2^2 = 4, \quad 2^4 = 5, \quad 2^6 = 9, \quad 2^8 = 3.$$

The primitive square root of unity in $\mathbb{Z}_{11}$ is $2^5 = 10 = -1$. ▲

The Existence of GF(p^n)

We turn now to the question of the existence of a finite field of order p^r for every prime power p^r, $r > 0$. We need the following lemma.

42.8 Lemma 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 $\overline{F}$.

Proof Because $\overline{F}$ is algebraically closed, $x^{p^n} - x$ factors over that field into a product of linear factors $x - \alpha$, so it suffices to show that none of these factors occurs more than once in the factorization.

Exercise 15 uses derivatives to complete this proof. Although this is an elegant method, it requires some effort to develop derivatives for polynomials over an arbitrary field, so we proceed using long division. Observe that 0 is a zero of $x^{p^n} - x$ of multiplicity 1. Suppose $\alpha \neq 0$ is a zero of $x^{p^n} - x$, and hence is a zero of $f(x) = x^{p^n-1} - 1$. Then $x - \alpha$ is a factor of $f(x)$ in $\overline{F}[x]$, and by long division, we find that

$$\begin{aligned}\frac{f(x)}{(x-\alpha)} &= g(x) \\ &= x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \cdots + \alpha^{p^n-3}x + \alpha^{p^n-2}.\end{aligned}$$

Now $g(x)$ has $p^n - 1$ summands, and in $g(\alpha)$, each summand is

$$\alpha^{p^n-2} = \frac{\alpha^{p^n-1}}{\alpha} = \frac{1}{\alpha}.$$

Thus

$$g(\alpha) = [(p^n - 1) \cdot 1]\frac{1}{\alpha} = -\frac{1}{\alpha}.$$

since we are in a field of characteristic p. Therefore, $g(\alpha) \neq 0$, so α is a zero of $f(x)$ of multiplicity 1. ◆

42.9 Lemma 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 all positive integers n.

Proof Let $\alpha, \beta \in F$. Applying the binomial theorem to $(\alpha + \beta)^p$, we have

$$\begin{aligned}(\alpha + \beta)^p &= \alpha^p + (p \cdot 1)\alpha^{p-1}\beta + \left(\frac{p(p-1)}{2} \cdot 1\right)\alpha^{p-2}\beta^2 \\ &\quad + \cdots + (p \cdot 1)\alpha\beta^{p-1} + \beta^p \\ &= \alpha^p + 0\alpha^{p-1}\beta + 0\alpha^{p-2}\beta^2 + \cdots + 0\alpha\beta^{p-1} + \beta^p \\ &= \alpha^p + \beta^p.\end{aligned}$$

Proceeding by induction on n, suppose that we have $(\alpha + \beta)^{p^{n-1}} = \alpha^{p^{n-1}} + \beta^{p^{n-1}}$. Then $(\alpha + \beta)^{p^n} = [(\alpha + \beta)^{p^{n-1}}]^p = (\alpha^{p^{n-1}} + \beta^{p^{n-1}})^p = \alpha^{p^n} + \beta^{p^n}$. ◆

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

Proof Let $\overline{\mathbb{Z}}_p$ be an algebraic closure of $\mathbb{Z}_p$, and let K be the subset of $\overline{\mathbb{Z}}_p$ consisting of all zeros of $x^{p^n} - x$ in $\overline{\mathbb{Z}}_p$. Let $\alpha, \beta \in K$. Lemma 42.9 shows that $(\alpha + \beta) \in K$, and the equation $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ shows that $\alpha\beta \in K$. From $\alpha^{p^n} = \alpha$ we obtain $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)^{p^n}\alpha$. If p is an odd prime, then $(-1)^{p^n} = -1$ and if $p = 2$ then $-1 = 1$. Thus $(-\alpha)^{p^n} = -\alpha$, so $-\alpha \in K$. Now 0 and 1 are zeros of $x^{p^n} - x$. For $\alpha \neq 0, \alpha^{p^n} = \alpha$ implies that $(1/\alpha)^{p^n} = 1/\alpha$. Thus K is a subfield of $\overline{\mathbb{Z}}_p$ containing $\mathbb{Z}_p$. Therefore, K is the desired field of p^n elements, since Lemma 42.8 showed that $x^{p^n} - x$ has p^n distinct zeros in $\overline{\mathbb{Z}}_p$. ◆

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

Proof Let F have $q = p^r$ elements, where p is the characteristic of F. By Theorem 42.10, there is a field $K \leq \bar{F}$ containing $\mathbb{Z}_p$ (up to isomorphism) and consisting precisely of the zeros of $x^{p^{rn}} - x$. We want to show $F \leq K$. Every element of F is a zero of $x^{p^r} - x$, by Theorem 42.3. Now $p^{rs} = p^r p^{r(s-1)}$. Applying this equation repeatedly to the exponents and using the fact that for $\alpha \in F$ we have $\alpha^{p^r} = \alpha$, we see that for $\alpha \in F$,

$$\alpha^{p^{rn}} = \alpha^{p^{r(n-1)}} = \alpha^{p^{r(n-2)}} = \cdots = \alpha^{p^r} = \alpha.$$

Thus $F \leq K$. Then Theorem 42.1 shows that we must have $[K : F] = n$. We have seen that K is simple over F in Corollary 42.6, so $K = F(\beta)$ for some $\beta \in K$. Therefore, irr(β, F) must be of degree n. ◆

42.12 Theorem Let p be a prime and let $n \in \mathbb{Z}^+$. If E and E' are fields of order p^n, then $E \simeq E'$.

Proof Both E and E' have $\mathbb{Z}_p$ as prime field, up to isomorphism. By Corollary 42.6, E is a simple extension of $\mathbb{Z}_p$ of degree n, so there exists an irreducible polynomial $f(x)$ of degree n in $\mathbb{Z}_p[x]$ such that $E \simeq \mathbb{Z}_p[x]/\langle f(x)\rangle$. Because the elements of E are zeros of $x^{p^n} - x$, we see that $f(x)$ is a factor of $x^{p^n} - x$ in $\mathbb{Z}_p[x]$. Because E' also consists of zeros of $x^{p^n} - x$, we see that E' also contains zeros of irreducible $f(x)$ in $\mathbb{Z}_p[x]$. Thus, because E' also contains exactly p^n elements, E' is also isomorphic to $\mathbb{Z}_p[x]/\langle f(x)\rangle$. ◆

In section 29 we saw that the field $\mathbb{Z}_2$ can be used to construct polynomial codes. Other finite fields have been used to construct algebraic codes with interesting properties. For example, in the *American Mathematical Monthly* 77 (1970): 249–258, Normal Levinson constructed an algebraic code that corrects three transmission errors. In this construction, the field of order 16 was used. Finite fields are also used in many other areas of mathematics including combinatorial designs, finite geometries, and algebraic topology.

EXERCISES 42

Computations

In Exercises 1 through 3, determine whether there exists a finite field having the given number of elements. (A calculator may be useful.)

1. 4096 **2.** 3127 **3.** 68,921

4. Find the number of primitive 8th roots of unity in GF(9).

5. Find the number of primitive 18th roots of unity in GF(19).

6. Find the number of primitive 15th roots of unity in GF(31).

7. Find the number of primitive 10th roots of unity in GF(23).

Concepts

8. Determine whether each of the following is true or false.

a. The nonzero elements of every finite field form a cyclic group under multiplication.
b. The elements of every finite field form a cyclic group under addition.
c. The zeros in $\mathbb{C}$ of $(x^{28} - 1) \in \mathbb{Q}[x]$ form a cyclic group under multiplication.
d. There exists a finite field of 60 elements.
e. There exists a finite field of 125 elements.
f. There exists a finite field of 36 elements.
g. The complex number i is a primitive 4th root of unity.
h. There exists an irreducible polynomial of degree 58 in $\mathbb{Z}_2[x]$.
i. The nonzero elements of $\mathbb{Q}$ form a cyclic group $\mathbb{Q}^*$ under field multiplication.
j. If F is a finite field, then every isomorphism mapping F onto a subfield of an algebraic closure $\overline{F}$ of F is an automorphism of F.

Theory

9. Let $\overline{\mathbb{Z}_2}$ be an algebraic closure of $\mathbb{Z}_2$, and let $\alpha, \beta \in \overline{\mathbb{Z}_2}$ be zeros of $x^3 + x^2 + 1$ and of $x^3 + x + 1$, respectively. Using the results of this section, show that $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2(\beta)$.

10. Show that every irreducible polynomial in $\mathbb{Z}_p[x]$ is a divisor of $x^{p^n} - x$ for some n.

11. Let F be a finite field of p^n elements containing the prime subfield $\mathbb{Z}_p$. Show that if $\alpha \in F$ is a generator of the cyclic group $\langle F^*, \cdot\rangle$ of nonzero elements of F, then $\deg(\alpha, \mathbb{Z}_p) = n$.

12. Show that a finite field of p^n elements has exactly one subfield of p^m elements for each divisor m of n.

13. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ of a degree d dividing n.

14. Let p be an odd prime.