A Primer on Finite Fields

Let K be a field and $f(x)$ be a nonconstant polynomial of $K[x]$. Then $f(x)$ is called *irreducible* in $K[x]$ if every factorization $f(x) = a(x)b(x)$ in $K[x]$ has $\{\deg a, \deg b\} = \{0, \deg f\}$. (This corresponds to prime numbers in $\mathbb{Z}$.) Otherwise $f(x)$ is *reducible*.

We begin with an important, general result. (It is Theorem A.2.22 of the Algebra Appendix.)

(A.2.22) Let $f(x) \in K[x]$ for K a field, with $\deg f \geq 1$. Then the ring $K[x] \pmod{f(x)}$ is a field if and only if $f(x)$ is irreducible.

PROOF. Assume that $f(x)$ is irreducible. Everything needed for $K[x] \pmod{f(x)}$ to be a field is clear except for the claim that all nonzero elements have multiplicative inverses.

Suppose that $g(x)$ is not zero in $K[x] \pmod{f(x)}$. That is, suppose that $g(x)$ is not a multiple of $f(x)$. Then $\gcd(g(x), f(x)) = \gcd(r(x), f(x))$, where $r(x)$ is the remainder upon division of $g(x)$ by $f(x)$. The polynomial $r(x)$ has degree less than $\deg f$ and is nonzero since $g(x)$ is not a multiple of $f(x)$.

Thus $\gcd(g(x), f(x)) = \gcd(r(x), f(x))$ is a divisor of $f(x)$ that has degree less than $f(x)$. As $f(x)$ is irreducible, that degree must be 0. Therefore monic $\gcd(g(x), f(x)) = \gcd(r(x), f(x)) = 1$. Now by the Extended Euclidean Algorithm, there are $s(x)$ and $t(x)$ in $K[x]$ with $s(x)g(x) + t(x)f(x) = 1$. That is, $s(x)g(x) = 1 \pmod{f(x)}$, and $s(x)$ is an inverse for $g(x)$ in the field $K[x] \pmod{f(x)}$.

Conversely suppose that $f(x)$ is reducible, and let $f(x) = a(x)b(x)$ be a factorization with $0 < \deg a < \deg f$ and $0 < \deg b < \deg f$. Then in the ring $K[x] \pmod{f(x)}$ the elements $a(x)$ and $b(x)$ are nonzero but have zero product. The ring is therefore not a field. □

From now on, F will denote a finite field.

(1) F contains a copy of $\mathbb{Z}_p = \mathbb{F}_p$, for some prime p. (This prime is called the *characteristic* of F.)

PROOF. Consider the *apparently infinite* subset

$$\{1\,,\ 1{+}1\,,\ 1{+}1{+}1\,,\ \ldots\}$$

of the *finite* field F. □

(2) There is a positive integer d with $|F| = p^d$.

PROOF. From the definitions, F is a vector space over $\mathbb{F}_p$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_d$ be a basis. Then $F = \left\{ \sum_{i=1}^{d} a_i \mathbf{e}_i \,\middle|\, a_1, \ldots, a_d \in \mathbb{F}_p \right\}$. Thus $|F|$ is the number of choices for the a_i, namely p^d. □

(3) Let $\alpha \in F \geq \mathbb{F}_p$, and let $m(x) \in \mathbb{F}_p[x]$ be a monic polynomial of minimal degree with $m(\alpha) = 0$. (It exists since F is finite.) Then $m(x)$ is irreducible and

$$\mathbb{F}_p[\alpha] = \left\{ \sum_{i=0}^{k} a_i \alpha^i \,\middle|\, k \geq 0,\ a_i \in \mathbb{F}_p \right\}$$

is a subfield of F that is a copy of $\mathbb{F}_p[x] \pmod{m(x)}$.

PROOF. It is clear that the arithmetic of $\mathbb{F}_p[\alpha]$ is the same as that of $\mathbb{F}_p[x] \pmod{m(x)}$.

Suppose that $m(x)$ is reducible, and let $m(x) = a(x)b(x)$ be a factorization with $0 < \deg a < \deg m$ and $0 < \deg b < \deg m$. Then $a(\alpha)b(\alpha) = m(\alpha) = 0$. Therefore either $a(\alpha) = 0$ or $b(\alpha) = 0$. But both contradict our choice of $m(x)$ as a nonzero polynomial of minimal degree having α as a root. So $m(x)$ is not reducible and is irreducible. In particular, by Theorem A.2.22, $\mathbb{F}_p[\alpha]$ is a field. □

The polynomial $m(x)$ is called the *minimal polynomial* of α over $\mathbb{F}_p$ and is uniquely determined. We sometimes write $m_\alpha(x)$ or even $m_{\alpha,\mathbb{F}_p}(x)$ for the minimal polynomial of α over $\mathbb{F}_p$.

(4) It is possible to pick the α of **(3)** so that $F = \mathbb{F}_p[\alpha]$. Indeed, it is possible to pick an α with $\alpha^{q-1} = 1$, (where $q = |F| = p^d$) and

$$F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\}.$$

PROOF. (sketch)

(*i*). For every β in $F \setminus \{0\}$, the smallest positive h with $\beta^h = 1$ is a divisor of $q-1$. (Consider the equivalence relation on $F \setminus \{0\}$ given by $\alpha \sim \omega$ if and only if $\alpha\omega^{-1}$ is a power of β.)

(*ii*). For every h that divides $q-1$ there are at most h elements β of $F \setminus \{0\}$ with $\beta^h = 1$ by Proposition A.2.10.

(*iii*). By counting, we see that the total number of elements of $F \setminus \{0\}$ that satify $\beta^h = 1$ for any h smaller than $q-1$ is itself less than $q-1$. Therefore there is at least one α with $1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$ all distinct and $\alpha^{q-1} = 1$. □

An element α with $F = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^i, \ldots, \alpha^{q-2}\}$ is called a *primitive element* in F, and its minimal polynomial $m_\alpha(x)$ is a *primitive* polynomial.

(5) (*The converse of* **(2)**.) For every prime p and positive integer d, there is a finite field F with $|F| = p^d$.

This is harder to prove. One uses counting techniques similar to those of **(4)** to show that, for every positive integer d, not all polynomials in $\mathbb{F}_p[x]$ of degree d are reducible, therefore there is at least one irreducible polynomial of degree d. The result then follows from Theorem A.2.22.

Examples

(E1) For every prime p the integers with arithmetic done mod p is a field $\mathbb{F}_p$. The real numbers $\mathbb{R}$ and rational numbers $\mathbb{Q}$ are also fields.

(E2) (*i*). The polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ (as otherwise it would have a root in $\mathbb{R}$). Therefore $\mathbb{R}[x] \pmod{x^2+1}$ is a field. Indeed, it is a copy of the complex numbers $\mathbb{C} = \mathbb{R} + \mathbb{R}i$, where i is a root of $x^2 + 1$ in $\mathbb{C}$.

(*ii*). The polynomial $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$ (as otherwise it would have a root in $\mathbb{F}_3 = \{0, 1, 2\}$). Therefore $\mathbb{F}_3[x] \pmod{x^2+1}$ is a field. Indeed, it is a field with nine elements $\mathbb{F}_9 = \mathbb{F}_3 + \mathbb{F}_3 i$, where i is a root of $x^2 + 1$ in $\mathbb{F}_9$. (Convince yourself that i is not a primitive element but $1 + i$ is.)

(*iii*). The polynomial $x^2 + 1$ is reducible in $\mathbb{F}_5[x]$ since 2 is a root ($(x-2)(x+2) = x^2 - 4 = x^2 + 1$). Therefore $\mathbb{F}_5[x] \pmod{x^2+1}$ is not a field.

(E3) The polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. Thus $\mathbb{F}_2[x] \pmod{x^2+x+1}$ is a field $\mathbb{F}_4$ with $4 = 2^2$ elements. Let ω be a root of $x^2 + x + 1$. Then $\mathbb{F}_4$ is $\mathbb{F}_2[\omega] = \{0, 1, \omega, \omega^2 = 1 + \omega\}$. The element ω is primitive, and the polynomial $x^2 + x + 1$ is a primitive polynomial.

(E4) The polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible. Thus $\mathbb{F}_2[x] \pmod{x^3+x+1}$ is a field $\mathbb{F}_8$ with $8 = 2^3$ elements. Let α be a root of $x^3 + x + 1$. Then $\mathbb{F}_8$ is $\mathbb{F}_2[\alpha]$. The element α is primitive, and the polynomial $x^3 + x + 1$ is a primitive polynomial.