A.3. A Primer on Finite Fields

A.3.1. Recall. We first recall some general results.

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.)

thm-A.2.22 A.3.1. Theorem. *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. □

eg-e2 A.3.2. Examples.

(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 $\mathbb{F}_9$.*

(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.*

Recall Lemma A.2.20:

lem-E.7.5 A.3.3. Lemma. *Let F be a field, and let $p(x), q(x), m(x) \in F[x]$. Suppose $m(x)$ divides the product $p(x)q(x)$ but $m(x)$ and $p(x)$ are relatively prime, $\gcd(m(x), p(x)) = 1$. Then $m(x)$ divides $q(x)$.*

Also recall Proposition A.2.10:

prop-E.4 A.3.4. Proposition. *Let $p(x)$ be a nonzero polynomial in $F[x]$, F a field, of degree d. Then $p(x)$ has at most d distinct roots in F.* □

The following consequence will be of help.

lem-helpful-bis A.3.5. Lemma. *In $F[x]$ let $m_i(x)$, for $1 \leq i \leq k$, be pairwise relatively prime divisors of $f(x)$. Then $\prod_{i=1}^{k} m_i(x)$ divides $f(x)$.*

PROOF. The proof is by induction on k. Write $f(x) = m_1(x)f_1(x)$. Then by Lemma A.3.3 each $m_i(x)$, for $2 \le i \le k$, divides $f_1(x)$. By induction $\prod_{i=2}^k m_i(x)$ divides $f_1(x)$ and so $\prod_{i=1}^k m_i(x)$ divides $f(x)$. $\square$

A.3.2. Basics. From now on, F will denote a finite field.

A.3.6. LEMMA. *F contains a copy of $\mathbb{Z}_p = \mathbb{F}_p$, for some prime p. (This prime is called the* characteristic *of F.)* lem-pt1

PROOF. (See Lemma A.1.3.) Consider the *apparently infinite* subset $\{1\,,\ 1{+}1\,,\ 1{+}1{+}1\,,\ \dots\}$ of the *finite* field F. $\square$

A.3.7. LEMMA. *There is a positive integer d with $|F| = p^d$. Set $q = |F| = p^d$.* lem-pt2

PROOF. (See Problem A.1.6.) From the definitions, F is a vector space over $\mathbb{F}_p$. Let $\mathbf{e}_1, \dots, \mathbf{e}_d$ be a basis. Then $F = \left\{ \sum_{i=1}^d a_i\mathbf{e}_i \;\middle|\; a_1, \dots, a_d \in \mathbb{F}_p \right\}$. Thus $|F|$ is the number of choices for the a_i, namely p^d. $\square$

A.3.8. LEMMA. *Let $\alpha \in F \ge \mathbb{F}_p$, 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* lem-pt4

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

is a subfield of F that is a copy of $\mathbb{F}_p[x] \pmod{m(x)}$. Its size is p^e where e is the degree of $m(x)$.

PROOF. It is clear that the arithmetic of $\mathbb{F}_p[\alpha]$ is the same as that of $\mathbb{F}_p[x] \pmod{m(x)}$. Especially it has size p^e.

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. $\square$

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 $\mathbb{F}_p$. minimal polynomial

A.3.9. LEMMA. *For every β in $F \setminus \{0\}$, the smallest positive h with $\beta^h = 1$ is a divisor of $q-1$. (We write $h = |\beta|$ and call h the* order *of β.)* lem-pt3 order

PROOF. Consider the directed graph on $F \setminus \{0\}$ that has an edge directed from a to b precisely when $a\beta = b$. Each connected component of this graph is a directed circuit (cycle). Let H be the component of 1. Then $|H| = h$. Furthermore, the component containing a is aH. Thus $F \setminus \{0\}$ of size $q-1$ is the disjoint union of circuits of size h, and especially h divides $q-1$. $\square$

A.3.10. PROPOSITION. *It is possible to pick the α of Lemma A.3.8 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* prop-pt5

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

PROOF. Let $l = \mathrm{lcm}_{a \in F^\times}\big(|a|\big)$. Thus $b^l = 1$, for all $b \in F^\times$, whereas $b^{q-1} = 1$ by (3); so $l = q-1$ by Proposition A.3.4.

Let $q-1=\prod_{i=1}^{k} p_i^{e_i}$ be the factorization of $q-1$ into distinct prime powers. If a has order $mp_i^{e_i}$, then a^m has order $p_i^{e_i}$. Thus $\mathbb{F}_q^\times$ contains an element a_i of order $p_i^{e_i}$ for each i. But then $\alpha=\prod_{i=1}^{k} a_i$ is an element of order $q-1$. □

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

Another way of saying this is that the primitive polynomials of degree $d>1$ in $\mathbb{F}_p[x]$ are precisely those irreducible polynomials that divide $x^{p^d-1}-1$ but do not divide x^m-1 for any $m<p^d-1$.

The previous two results immediately give:

cor-pt6 A.3.11. COROLLARY. *Every finite field F is a copy of $\mathbb{F}_p[x] \pmod{f(x)}$ for some monic irreducible polynomial $f(x)\in\mathbb{F}_p[x]$. If $f(x)$ has degree d, then $|F|=p^d$.* □

thm-pt7 A.3.12. THEOREM. (The converse of Lemma A.3.7.) *For every prime p and positive integer d, there is a finite field F with $|F|=p^d$.*

As we have seen, this is equivalent to proving that there is an irreducible polynomial of degree d in $\mathbb{F}_p[x]$ for every d. This is harder to prove. The result follows from Theorem A.3.16 of the next subsection. Here is the idea:

> One can view our proof of Proposition A.3.10 as a counting argument—all the elements of $F\setminus\{0\}$ have order at most $q-1$ but $F\setminus\{0\}$ is so big that it is not possible for all of its elements to have order less than $q-1$. A similar (but more complicated) counting argument concerning irreducible polynomials of degree at most d gives this result.

eg-gf4 A.3.13. EXAMPLE. *The polynomial $x^2+x+1\in\mathbb{F}_2[x]$ is irreducible (as otherwise it would have a root 0 or 1). 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.*

eg-gf8 A.3.14. EXAMPLE. *The polynomial $x^3+x+1\in\mathbb{F}_2[x]$ is irreducible (as otherwise it would have a root 0 or 1). 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.*

eg-gf9 A.3.15. EXAMPLE. *As we have noted, 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; 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 $\mathbb{F}_9$. Here i is not a primitive element but $1+i$ is.*

A.3.3. Existence in all cases. We only need the case $q=p$ of the next Theorem, but no extra work is required to prove the following stronger result.

thm-irred-exist A.3.16. THEOREM. *For every finite field $\mathbb{F}_q$ and positive integer d, there is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree d.*

We make use of a sequence of lemmas.

lem-split-poly-bis A.3.17. LEMMA. *Let K be a field containing the subfield $\mathbb{F}_q$. Then the elements of $\mathbb{F}_q$ are precisely the roots in K of the polynomial $x^q-x\in\mathbb{F}_q[x]\le K[x]$. That is, $x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$.*

PROOF. By Lemma A.3.9 every nonzero element of $\mathbb{F}_q$ is a root of $x^{q-1} - 1$, hence each of the q elements of $\mathbb{F}_q$ is a root of $x^q - x$. The result follows from Proposition A.3.4. $\square$

Compare the next lemma with the definition of a primitive polynomial.

A.3.18. LEMMA. *If $f(x) \in \mathbb{F}_q[x]$ is irreducible of degree d, then it divides $x^{q^d} - x$ but does not divide $x^{q^a} - x$ for any $a < d$.* lem-irred-split-bis

PROOF. Let α be the image of x in $K = \mathbb{F}_{q^d} = \mathbb{F}_q[x] \pmod{f(x)}$, a field by Theorem A.3.1. As $f(\alpha) = 0$ in $\mathbb{F}_{q^d}$, the irreducible $f(x)$ must be the minimal polynomial of α over $\mathbb{F}_q$ (up to a scalar). In particular $f(x)$ divides $x^{q^d} - x$.

Suppose $f(x)$ divides $x^{q^e} - x$, say $f(x)g(x) = x^{q^e} - x$. Then in $\mathbb{F}_{q^d}$, we have $\alpha^{q^e} - \alpha = f(\alpha)g(\alpha) = 0$, so $\alpha^{q^e} = \alpha$. Every element b of $\mathbb{F}_{q^d}$ can be written uniquely as $b = \sum_{i=0}^{d-1} b_i\alpha^i$, for certain $b_i \in \mathbb{F}_q$. By the previous lemma $b_i^q = b_i$, for all i. Then by the Freshman's Dream

$$
\begin{aligned}
b^{q^e} &= \left(\sum_{i=0}^{d-1} b_i\alpha^i\right)^{q^e} = \sum_{i=0}^{d-1} (b_i)^{q^e}(\alpha^i)^{q^e} \\
&= \sum_{i=0}^{d-1} b_i\alpha^i = b\,.
\end{aligned}
$$

That is, every $b \in \mathbb{F}_{q^d}$ satisfies $b^{q^e} - b = 0$; and $x^{q^e} - x$ has at least q^d distinct roots. By Proposition A.3.4 again, $e \geq d$ as claimed. $\square$

A.3.19. LEMMA. *$x^{q^k} - x$ is square free.* lem-square-free-bis

PROOF. We prove this using the formal derivative. Indeed

$$
\gcd(x^{q^k} - x, (x^{q^k} - x)') = \gcd(x^{q^k} - x, -1) = 1\,,
$$

so $x^{q^k} - x$ is square-free. $\square$

PROOF OF THEOREM A.3.16:
Let $F_d(x)$ be the product of all distinct monic irreducible polynomials of degree d. Furthermore let $f_d(x)$ be the product of all degree d monic irreducible factors of $x^{q^k} - x$.

By results A.3.5, A.3.18, and A.3.19, the polynomial $f_d(x)$ divides $F_d(x)$ and $F_d(x)$ divides $x^{q^d} - x$. Also by Lemma A.3.18 we have $x^{q^k} - x = \prod_{d=1}^{k} f_d(x)$. Therefore

$$
(x^{q^k} - x)/f_k(x) = \prod_{d=1}^{k-1} f_d(x) \quad \text{divides} \quad \prod_{d=1}^{k-1} F_d(x)
$$

of degree at most $\sum_{d=1}^{k-1} q^d < q^k$. We conclude that $f_k(x)$ has positive degree, and so $x^{q^k} - x$ possesses irreducible factors of degree k, as desired. $\square$