Solutions to Ireland, Rosen “A Classical Introduction to Modern Number Theory”

Richard Ganaye

October 15, 2019

Chapter 7

Ex. 7.1 *Use the method of Theorem 1 to show that a finite subgroup of the multiplicative group of a field is cyclic.*

A solution is already given in Ex. 4.15

Ex. 7.2 *Find the finite subgroups of* $\mathbb{R}^*$ *and* $\mathbb{C}^*$ *and show directly that they are cyclic.*

Proof. If G is a finite subgroup of $\mathbb{R}$ or $\mathbb{C}$, and $n = |G|$, then from Lagrange's Theorem, $x^n = 1$ for all $x \in G$.

- If G is a finite subgroup of $\mathbb{R}^*$, then the solutions of $x^n = 1$ are in $\{-1, 1\}$, so $\{1\} \subset G \subset \{-1, 1\} : G = \{1\}$ or $G = \{-1, 1\}$, both cyclic.
- If G is a finite subgroup of $\mathbb{C}^*$, then $G \subset \mathbb{U}_n = \{e^{2ik\pi/n} \mid 0 \le k \le n-1\}$. As $|G| = |\mathbb{U}_n| = n$, then $G = \mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic. $\square$

Ex. 7.3 *Let* F *a field with* q *elements and suppose that* $q \equiv 1 \pmod n$. *Show that for* $\alpha \in \mathbb{F}^*$, *the equation* $x^n = \alpha$ *has either no solutions or* n *solutions.*

Proof. This is a particular case of Prop. 7.1.2., where $d = n \wedge (q-1) = n$: the equation $x^n = \alpha$ has solutions iff $\alpha^{(q-1)/n} = 1$. In this case, there are exactly $d = n$ solutions.

We give here a direct proof.

Let g a generator of F^*. Write $x = g^y, \alpha = g^a$. Then

$$x^n = \alpha \iff g^{ny} = g^a \iff q-1 \mid ny - a.$$

Suppose that there exists $x \in F$ such that $x^n = \alpha$. Then there exists $y \in \mathbb{Z}$ such that $q - 1 \mid ny - a$. Since $n \mid q-1$, then $n \mid a$.

$$q-1 \mid ny - a \iff \frac{q-1}{n} \mid y - \frac{a}{n} \iff y = \frac{a}{n} + k\frac{q-1}{n}, k \in \mathbb{Z}.$$

As $\frac{a}{n} + (k+n)\frac{q-1}{n} = \frac{a}{n} + k\frac{q-1}{n}, k \in \mathbb{Z}$, the values $k = 0, 1 \cdots, n-1$ are sufficient :

$$x^n = \alpha \iff y = \frac{a}{n} + k\frac{q-1}{n}, k \in \{0, 1, \cdots, n-1\}.$$

Moreover, these solutions are all distinct : if $k, l \in \{0, 1, \cdots, n-1\}$,

$$\begin{aligned} g^{\frac{a}{n}+k\frac{q-1}{n}} = g^{\frac{a}{n}+l\frac{q-1}{n}} &\Rightarrow g^{(k-l)\frac{q-1}{n}} = 1 \\ &\Rightarrow q-1 \mid (k-l)\frac{q-1}{n} \\ &\Rightarrow n \mid k-l \\ &\Rightarrow k \equiv l\ [n] \Rightarrow k = l. \end{aligned}$$

Conclusion : if F is a field with q elements and $n \mid q-1$, the equation $x^n = \alpha$ has either no solutions or n solutions in F.

Remark :

$$\exists x \in F^*, x^n = \alpha \iff n \mid a \iff \alpha^{(q-1)/n} = 1.$$

Indeed, if $x^n = \alpha$ has a solution, we have proved that $n \mid a$, thus $\alpha^{(q-1)/n} = (g^{a/n})^{q-1} = 1$.

Reciprocally, if $\alpha^{(q-1)/n} = 1$, $g^{a.(q-1)/n} = 1$, thus $q-1 \mid a(q-1)/n$, so $n \mid a$: $\alpha = x^n$, with $x = g^{n/a}$. □

Ex. 7.4 *(continuation) Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.*

Proof. Here $n \mid q-1$.

Let $\varphi = F^* \to F^*$ the application defined by $\varphi(x) = x^n$. φ is a morphism of groups, and $\ker \varphi$ is the set of solutions of $x^n = 1$. As $n \mid q-1$, $x^n = 1$ has exactly n solutions (Prop 7.1.1, Corollary2, or Ex 7.3 with $\alpha = 1$). So $|\ker \varphi| = n$.

Thus $\mathrm{Im}\varphi \simeq F^*/\ker\varphi$ is a subgroup with cardinality $|F^*|/|\ker\varphi| = (q-1)/n$, and $\mathrm{Im}\varphi$ is the set of α such that $x^n = \alpha$ is solvable.

Conclusion : the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.

□

Ex. 7.5 *(continuation) Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$, show that the equation $x^n = \alpha$ has n solutions in K. [Hint: Show that $q^n - 1$ is divisible by $n(q-1)$ and use the fact that $\alpha^{q-1} = 1$.]*

Proof. As $q \equiv 1\ [n]$, $\frac{q^n-1}{q-1} = 1 + q + \cdots + q^{n-1} \equiv 0\ [n]$, then $n \mid \frac{q^n-1}{q-1}$:

$$q^n - 1 = kn(q-1), k \in \mathbb{N}.$$

Since $\alpha \in F^*$, $\alpha^{q-1} = 1$, so

$$\alpha^{(q^n-1)/n} = (\alpha^{q-1})^k = 1.$$

As $|K| = q^n$, Prop. 7.1.2 (or the final remark in Ex.7.3) show that there exists $x \in K^*$ such that $x^n = \alpha$. Then, from Ex.7.3, we know that there exist n solutions in K.

Conclusion : if $[K : F] = n$, the equation $x^n = \alpha$ has n solutions in K.

□

Ex. 7.6 *Let $K \supset F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F, it is not a square in K.*

Proof. Let $q = |F|$. Then $|K| = q^3$.

If the characteristic of F is 2, $q = 2^k$, and for all $x \in F$, $x = x^q = \left(x^{2^{k-1}}\right)^2$. So all elements in F or K are squares. We can now suppose that the characteristic of F is not 2, and consequently $1 \neq -1$ in F.

As α is not a square in F, $\alpha^{(q-1)/2} \neq 1$ (Prop. 7.1.2). From $0 = \alpha^{q-1} - 1 = (\alpha^{(q-1)/2} - 1)(\alpha^{(q-1)/2} + 1)$, we deduce $\alpha^{(q-1)/2} = -1$. Then

$$\alpha^{(q^3-1)/2} = (\alpha^{(q-1)/2})^{q^2+q+1} = (-1)^{q^2+q+1} = -1,$$

since $q^2 + q + 1$ is always odd.

$\alpha^{(q^3-1)/2} \neq 1$: this implies (Prop. 7.1.2) that α is not a square in K. $\square$

Ex. 7.7 *Generalize Exercise 6 by showing that if α is not a square in F, it is not a square in any extension of odd degree and is a square in every extension of even degree.*

Proof. Write $q = [K : F]$, and $q = \text{Card } F$.

As α is not a square in F, the characteristic of F is not 2 (see Ex.7.6), and $\alpha^{(q-1)/2} \neq 1$. Since $\alpha^{q-1} = 1$, $\alpha^{(q-1)/2} = -1$.

$$\alpha^{(q^n-1)/2} = (\alpha^{(q-1)/2})^{1+q+\cdots+q^{n-1}} = (-1)^{1+q+\cdots+q^{n-1}}.$$

- If n is odd, $1+q+\cdots+q^{n-1} \equiv 1 \pmod 2$, thus $\alpha^{(q^n-1)/2} = -1 \neq 1$, and consequently α is not a square in K.
- If n is even, as q is odd ($\text{char}(F) \neq 2$), $1 + q + \cdots + q^{n-1} \equiv 0 \pmod 2$, thus $\alpha^{(q^n-1)/2} = 1$, so α is a square in K. $\square$

Ex. 7.8 *In a field with 2^n elements, what is the subgroup of squares.*

Let F a field with $q = 2^n$ elements.

Proof 1

Proof. $d = (q-1) \wedge 2 = (2^n - 1) \wedge 2 = 1$, thus each $\alpha \in F^*$ verifies $\alpha^{(q-1)/d} = \alpha^{q-1} = 1$. Theorem 7.1.2 show that α is a square in F, of exactly one root. $\square$

Proof 2

Proof. For all $x \in F$, $x = x^q = \left(x^{2^{n-1}}\right)^2$. So all elements in F or K are squares. $\square$

Ex. 7.9 *If $K \supset F$ are finite fields, $|F| = q, \alpha \in F, q \equiv 1 \pmod n$, and $x^n = \alpha$ is not solvable in F, show that $x^n = \alpha$ is not solvable in K if $(n, [K : F]) = 1$.*

Proof. Let $k = [K : F]$. From hypothesis, $k \wedge n = 1$, so there exist integers u, v such that $uk + vn = 1$.

As $n \mid q - 1$, $n \wedge (q-1) = n$, so the hypothesis "$x^n = \alpha$ is not solvable in F" implies that $\alpha^{(q-1)/n} \neq 1$ (Prop. 7.1.2).

Write $\omega = \alpha^{(q-1)/n}$, so $\omega \neq 1$ and $\omega^n = 1$.

As $n \mid q-1$, $n \mid q^k - 1$ and

$$\alpha^{(q^k-1)/n} = (\alpha^{(q-1)/n})^{1+q+q^2+\cdots+q^{k-1}} = \omega^{1+q+q^2+\cdots+q^{k-1}}.$$

Moreover $1 + q + \cdots + q^{k-1} \equiv k \pmod n$, and $\omega^n = 1$, so $\alpha^{(q^k-1)/n} = \omega^k$.

If $\omega^k = 1$, then $\omega = \omega^{uk+vn} = (\omega^k)^u(\omega^n)^v = 1$, which is in contradiction with $\omega = \alpha^{(q-1)/n} \neq 1$.

So $\alpha^{(q^k-1)/n} = \omega^k \neq 1$, and consequently the equation $x^n = \alpha$ has no solution in K. □

Ex. 7.10 *If $K \supset F$ be finite fields and $[K : F] = 2$. For $\beta \in K$, show that $\beta^{1+q} \in F$ and moreover that every element in F is of the form β^{1+q} for some $\beta \in K$.*

Proof. If $\beta = 0$, $\beta^{1+q} = 0 \in F$, and if $\beta \in K^*$, $\beta^{q^2-1} = 1$, so $\left(\beta^{1+q}\right)^{q-1} = 1$, thus $\beta^{1+q} \in F$ (Prop. 7.1.1, Corollary 1).

Let g a generator of $K^* : K^* = \{1, g, g^2, \cdots, g^{q^2-2}\}$.

For every in integer $k \in \mathbb{Z}$,

$$g^k \in F^* \iff (g^k)^{q-1} = 1 \iff g^{k(q-1)} = 1 \iff q^2 - 1 \mid k(q-1) \iff q + 1 \mid k.$$

Thus $F^* = \{1, g^{q+1}, g^{2(q+1)}, \cdots, g^{(q-2)(q+1)}\}$. I $\alpha \in F^*$, there exists $i, 0 \leq i \leq q-1$ such that $\alpha = g^{i(q+1)}$. If we write $\beta = g^i$, then $\alpha = \beta^{1+q}$ (and for $\alpha = 0$, we take $\beta = 0$).

Conclusion : if K is a quadratic extension of F (F, K finite fields), every element in F is of the form β^{1+q} for some $\beta \in K$. □

Ex. 7.11 *With the situation being that of Exercise 10 suppose that $\alpha \in F$ has order $q-1$. Show that there is a $\beta \in K$ with order $q^2 - 1$ such that $\beta^{1+q} = \alpha$.*

Write $|a|$ the order of an element a in a group G. We recall the following lemma :

Lemma If $|a| = d$, then for all $i \in \mathbb{Z}$, $|a^i| = \frac{d}{d \wedge i}$.

Proof. Indeed, for all $k \in \mathbb{Z}$,

$$(a^i)^k = e \iff a^{ik} = e \iff d \mid ik \iff \frac{d}{d \wedge i} \mid \frac{i}{d \wedge i} k \iff \frac{d}{d \wedge i} \mid k.$$

□

Proof. (Ex. 7.11)

Let $\alpha \in F^*$ with $|a| = q - 1$, and g a generator of K^*, so $|g| = q^2 - 1$. We know from exercise 7.10 that there exists an integer i such that $\alpha = g^{i(q+1)}$.

Let $h = g^{q+1}$. As $h^{q-1} = 1$, then $h \in F^*$, and since $|g| = q^2 - 1$, $|h| = q - 1$, so h is a generator of F^*.

Note that for all $s \in \mathbb{Z}$, $\alpha = g^{(i+s(q-1))(q+1)}$, since $g^{q^2-1} = 1$.

We will show that we can choose s such that $j = i + s(q-1)$ is relatively prime with $q + 1$. Then j is such that $\alpha = g^{j(q+1)} = h^j$.

i is odd : if not α is an element of the subgroup of squares in F^*, so its order divides $(q-1)/2$, in contradiction with $|\alpha| = q - 1$.

$(q-1) \wedge (q+1) \mid 2$. Since $i - 1$ is even, there exist integers s, t verifying the Bézout's equation

$$i - 1 = t(q+1) - s(q-1).$$

Then $j = i + s(q-1) = 1 + t(q+1)$ is relatively prime with $q+1 : j \wedge (q+1) = 1$.

Moreover, as $\alpha = h^j$, with $|\alpha| = |h| = q-1$, the lemme implies that

$$q - 1 = |\alpha| = \frac{q-1}{(q-1) \wedge j},$$

so $(q-1) \wedge j = 1$. As $(q+1) \wedge j = 1$ and $(q-1) \wedge j = 1$, then $(q^2-1) \wedge j = 1$.

Let $\beta = g^j$: then $\alpha = \beta^{1+q}$, and using the lemma :

$$|\beta| = |g^j| = \frac{q^2-1}{(q^2-1) \wedge j} = q^2 - 1.$$

Conclusion : there exists a $\beta \in K^*$ with order $q^2 - 1$ such that $\beta^{1+q} = \alpha$. □

Ex. 7.12 *Use Proposition 7.2.1 to show that given a field k and a polynomial $f(x) \in k[x]$ there is a field $K \supset k$ such that $[K : k]$ is finite and $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ in $K[x]$.*

Proof. We show by induction on the degree n of f that for all polynomials $f \in k[x]$ with $\deg(f) = n \geq 1$, there exists a field extension K such that $[K : k]$ is finite, and $f(x)$ splits in linear factors on K.

If $n = 1$, $f(x) = ax + b = a(x - \alpha_0)$, where $\alpha_0 = -b/a : K = k$ is suitable.

Suppose that the property is true for all polynomials of degree less than n on an arbitrary field k.

Let $f(x) \in k[x], \deg(f) = n$. From propoistion 7.2.1. applied to an irreducible factor of f, there exists a field $L, [L : K] < \infty$ and $\alpha \in L$ such that $f(\alpha_1) = 0$. Then $f(x) = (x - \alpha_1)g(x), g(x) \in L[x]$.

Applying the induction hypothesis in the field L on the polynomial $g \in L[x]$ with $\deg(g) = n-1$, we obtain a field $K, [K : L] < \infty$ such that $g(x) = a(x-\alpha_2)\cdots(x-\alpha_n)$ with $\alpha_i \in K$. So $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ splits in linear factors in K. The induction is achieved. □

Ex. 7.13 *Apply Exercise 7.12 to $k = \mathbb{Z}/p\mathbb{Z}$ and $f(x) = x^{p^n} - x$ to obtain another proof of Theorem 2.*

Proof. Let $f(x) = x^{p^n} - x$. We know from Ex. 7.12 that there exists a finite extension K of $\mathbb{F}_p$ such that f splits in linear factors on K :

$$f(x) = \prod_{k=1}^{p^n} (x - \alpha_k), \qquad \alpha_1, \ldots, \alpha_{p^n} \in K.$$

The set $k = \{\alpha_1, \cdots, \alpha_{p_n}\} \subset K$ of the roots of $x^{p^n} - x$ is a subfield of K : indeed, if $\alpha, \beta \in k$,

(a) $f(1) = 0$, so $1 \in k$

(b) $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$, so $\alpha - \beta \in k$.

(c) $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, so $\alpha\beta \in k$.

(d) $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, so $\alpha^{-1} \in k$ if $\alpha \neq 0$.

As $f'(x) = -1$, $f(x) \wedge f'(x) = 1$, so f has no multiple root, so the cardinality of k is p^n.

Let $g(x) \in \mathbb{F}_p[x]$ a factor of $f(x)$, irreducible in $\mathbb{F}_p[x]$, with $d = \deg(g)$. As $g \mid f$, g splits in linear factors in $k[x]$. Let α a root of $g(x)$ in k. As g is irreducible on $\mathbb{F}_p$, $d = \deg(g) = [\mathbb{F}_p[\alpha] : \mathbb{F}_p]$. Moreover $n = [k : \mathbb{F}_p] = [k : \mathbb{F}_p[\alpha]]\,[\mathbb{F}_p[\alpha] : \mathbb{F}_p]$, so $d \mid n$.

Reciprocally, suppose that g is any irreducible polynomial in $\mathbb{F}_p[x]$, with $d = \deg(g) \mid n$. Then $K_0 = \mathbb{F}_p[x]/\langle g \rangle$ contains a root α of g, and $[K_0 : \mathbb{F}_p] = \deg(g) = d$, so $\alpha^{p^d} = \alpha$.

As $d \mid n$, then $p^d - 1 \mid p^n - 1$ and $x^{p^d} - 1 \mid x^{p^n} - 1$ (Lemma 2,3 in section 1), so

$$x^{p^d} - x \mid x^{p^n} - x.$$

$f(\alpha) = \alpha^{p^n} - \alpha = 0$ and g is the minimal polynomial of α, so $g \mid f$.

Conclusion :

$$x^{p^n} - x = \prod_{d \mid n} F_d(x),$$

where $F_d(x)$ is the product of the monic irreducible polynomial of degree d. □

Ex. 7.14 *Let F be a field with q elements and n a positive integer. Show that there exist irreducible polynomials in $F[x]$ of degree n.*

Proof. Leq $F = \mathbb{F}_q$ a field with $q = p^m$ elements, and n a positive integer.

From Theorem 2 Corollary 3, there exists an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree nm. Let g an irreducible factor of f in $\mathbb{F}_q[x]$, and α a root of g in an extension of $\mathbb{F}_q$.

We show that $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

$\mathbb{F}_q$ and $\mathbb{F}_p[\alpha]$ are two subfield of the same finite field $\mathbb{F}_q[\alpha]$. Moreover, $|\mathbb{F}_q| = p^m$, and $|\mathbb{F}_p[\alpha]| = p^{nm}$. As $m \mid n$, $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

Indeed, for all $\gamma \in \mathbb{F}_q[\alpha]$,

$$\gamma \in \mathbb{F}_q \Rightarrow \gamma^{p^m} = \gamma \Rightarrow \gamma^{p^{mn}} = \gamma \Rightarrow \gamma \in \mathbb{F}_p[\alpha].$$

So $\mathbb{F}_q \subset \mathbb{F}_p[\alpha]$.

We show that $\mathbb{F}_q[\alpha] = \mathbb{F}_p[\alpha]$.

As $\mathbb{F}_p \subset \mathbb{F}_q$, $\mathbb{F}_p[\alpha] \subset \mathbb{F}_q[\alpha]$.

Let $\beta \in \mathbb{F}_q[\alpha]$: $\beta = \sum_{i=1}^{k} a_i \alpha^i$, where $a_i \in \mathbb{F}[q] \subset \mathbb{F}_p[\alpha]$, so $a_i = p_i(\alpha), p_i \in \mathbb{F}_p[\alpha]$. Consequently

$$\beta = \sum_{i=1}^{k} p_i(\alpha)\alpha^i \in \mathbb{F}_p[\alpha],$$

so $\mathbb{F}_q[\alpha] = \mathbb{F}_p[\alpha]$.

$$nm = [\mathbb{F}_p[\alpha] : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] \times [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] \times m.$$

Thus $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = n$, and g is the minimal polynomial of α on $\mathbb{F}_q$, so $\deg(g) = n$.

Conclusion : if F is a field with $q = p^m$ elements, there exist irreducible polynomials in $F[x]$ of degree n for all positive integers n. □

Ex. 7.15 *Let $x^n - 1 \in F[x]$, where F is a finite field with q elements. Suppose that $(q, n) = 1$. Show that $x^n - 1$ splits into linear factors in some extension field and that the least degree of such a field is the smallest integer f such that $q^f \equiv 1 \pmod n$.*

Proof. From exercise 7.12, we know that $x^n - 1$ splits into linear factors in some extension field K, with $[K : F] < \infty$:

$$u(x) = x^n - 1 = (x - \zeta_0)(x - \zeta_1) \cdots (x - \zeta_{n-1}), \qquad \zeta_i \in K.$$

$u'(x) \wedge u(x) = nx^{n-1} \wedge (x^n - 1) = 1$, since $x(nx^{n-1}) - n(x^n - 1) = n$, and $n \neq 0$ in the field F, since we know from the hypothesis $q \wedge n = 1$ that the characteristic p doesn't divide n. So the n roots of $x^n - 1$ are distinct.

The set $G = \{x \in K \mid x^n = 1\}$ is a subgroup of K^*, thus G is cyclic of order n. Let ζ a generator of G. Then

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}).$$

Let $p(x)$ the minimal polynomial of ζ on F, and f the degree of p :

$$f = \deg(p) = [F[\zeta] : F].$$

So $\operatorname{Card} F[\zeta] = q^f$, and since $\zeta \in F[\zeta]^*$, $\zeta^{q^f - 1} - 1 = 0$. As the order of ζ in the group G is n, $n \mid q^f - 1$, namely $q^f \equiv 1 \pmod n$.

Let k any positive integer such that $q^k \equiv 1 \pmod n$.

Then $n \mid q^k - 1$, so $\zeta^{q^k - 1} - 1 = 0$, $\zeta^{q^k} - \zeta = 0$. Let L an extension of K such that $x^{q^k} - x$ splits in linear factors in L. As $\zeta^{q^k} - \zeta = 0$, ζ belongs to the subfield M of L with cardinality q^k, such that $[M : F] = k$. Thus $\mathbb{F}[\zeta] \subset M$, so $f = [F[\zeta] : F] \leq k = [M : F]$.

$f = [F[\zeta] : F]$ is the smallest $k \in \mathbb{N}^*$ such that $q^k \equiv 1 \pmod n$.

If K is any extension of F containing the roots of $x^n - 1$, then $K \supset F[\zeta]$, where ζ is a primitive root of unity, so $[K : F] \geq [F[\zeta] : F] = f$.

Conclusion : the minimal degree of a extension $K \supset F$ containing the roots of $x^n - 1$, with $n \wedge q = 1$, is the smallest positive integer f such that $q^f \equiv 1 \pmod n$, the order of q modulo n. $\square$

Ex. 7.16 *Calculate the monic irreducible polynomials of degree 4 in $\mathbb{Z}/2\mathbb{Z}[x]$.*

Proof. Write F_d the product of irreducible monic polynomials in $\mathbb{F}_2[x]$.

Theorem 2 gives

$$x^{16} - x = x^{2^4} - x = \prod_{d|4} F_d(x) = F_1(x)F_2(x)F_4(x)$$

and

$$x^4 - x = x^{2^2} - x = \prod_{d|2} F_d(x) = F_1(x)F_2(x)$$

so $F_4(x) = \frac{x^{16} - x}{x^4 - x} = \frac{x^{15} - 1}{x^3 - 1} = x^{12} + x^9 + x^6 + x^3 + 1$

$F_4(x) = (x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)$

Among the 16 monic polynomials of degree 4 in $\mathbb{F}_2[x]$, 3 are irreducible :

$$\begin{aligned} P_1(x) &= x^4 + x^3 + x^2 + x + 1, \\ P_2(x) &= x^4 + x + 1 \\ P_3(x) &= x^4 + x^3 + 1 \end{aligned}$$

With sage :

```
sage: A = PolynomialRing(GF(2),'x')
sage: x = A.gen()
sage: f = (x^16-x)/(x^4-x)
sage: factor(f)
(x^4 + x + 1) * (x^4 + x^3 + 1) * (x^4 + x^3 + x^2 + x + 1)
```

□

Ex. 7.17 *Let q and p be distinct odd primes. Show that the number of monic irreducibles of degree q in $\mathbb{Z}/p\mathbb{Z}$ is $q^{-1}(p^q - p)$.*

Proof. From Theorem 2 Corllary 2, we know that the number of irreducible polynomials on $\mathbb{F}_p$ of degree q is given by

$$N_q = \frac{1}{q} \sum_{d \mid q} \mu\left(\frac{q}{d}\right) p^d.$$

As q is prime, d takes the values $1, q$, with $\mu(1) = 1, \mu(q) = -1$, so

$$N_q = \frac{p^q - p}{q}.$$

□

Ex. 7.18 *Let p be a prime with $p \equiv 3 \pmod 4$. Show that the residue classes modulo p in $\mathbb{Z}[i]$ form a field with p^2 elements.*

Proof. If p is a prime rational integer, with $p \equiv 3 \pmod 4$, then p is a prime in $\mathbb{Z}[i]$.

Indeed, p is irreducibel : if $p = uv,\ u, v \in \mathbb{Z}[i]$, where $u = c + di, v$ are not units, then $p^2 = N(u)N(v),\ N(u) > 1, N(v) > 1$, so $p = N(u) = u\overline{u} = c^2 + d^2$.

As $c^2 \equiv 0, 1 \pmod 4, d^2 \equiv 0, 1 \pmod 4$, so $p \equiv 1 \pmod 4$, which is in contradiction with the hypothesis.

So p is irreducible in $\mathbb{Z}[i]$, and since $\mathbb{Z}[i]$ is a principal ideal domain, p is prime in $\mathbb{Z}[i]$, thus $\mathbb{Z}[i]/(p)$ is a field.

Let $z = a + bi \in \mathbb{Z}[i]$. The Euclidean division of a, b by q gives

$$a = qp + r,\ 0 \le r < p, \qquad b = q'p + s,\ 0 \le s < p,$$

so

$$z \equiv r + is \pmod p,\ 0 \le r < p, 0 \le s < p.$$

Let's verify that these p^2 elements are in differnet classes of congruences modulo p.

If $r + is \equiv r' + is' \pmod p$, then $(r - r')/p + i(s - s')/p \in \mathbb{Z}[i]$, so $r \equiv r', s \equiv s' \pmod p$.

As r, r', s, s' are between 0 and $p - 1$, $r = r', s = s'$.

So the cardinality of the field $\mathbb{Z}[i]/(p)$ is p^2. □

Ex. 7.19 *Let F be a finite field with q elements . If $f(x) \in F[x]$ has degree t, put $|f| = q^t$. Verify the formal identity $\sum_f |f|^{-s} = (1-q^{1-s})^{-1}$. The sum is over all monic polynomials.*

Proof. Let U the set of monic polynomials in $\mathbb{F}_q[x]$, and U_t the set of monic polynomials of degree t, and $s \in \mathbb{C}$. Then $U = \coprod_{t\in\mathbb{N}} U_t$, so

$$\begin{aligned}\sum_{f\in U} |f|^{-s} &= \sum_{t=0}^{\infty} \sum_{f\in U_t} |f|^{-s}\\ &= \sum_{t=0}^{\infty} \frac{1}{q^{ts}} \sum_{f\in U_t} 1\end{aligned}$$

As $\sum_{f\in U_t} 1 = \mathrm{Card}\,(U_t) = q^t$, then, for $\mathrm{Re}(s) > 1$

$$\begin{aligned}\sum_{f\in U} |f|^{-s} &= \sum_{t=0}^{\infty} \frac{1}{q^{t(s-1)}}\\ &= \frac{1}{1-\frac{1}{q^{s-1}}}\\ &= (1-q^{1-s})^{-1}\end{aligned}$$

As $\left|\frac{1}{q^{t(s-1)}}\right| = \frac{1}{q^{t(\mathrm{Re}(s)-1)}}$, the serie is absolutely convergent for $\mathrm{Re}(s) > 1$. This justifies the grouping of terms in this sum.

Conclusion : if $\mathrm{Re}(s) > 1$,

$$\sum_{f\in U} |f|^{-s} = (1-q^{1-s})^{-1},$$

where U is the set of monic polynomials in $\mathbb{F}_q[x]$. □

Ex. 7.20 *With the notation of Exercise 19 let $d(f)$ be the number of monic divisors of f and $\sigma(f) = \sum_{g|f} |g|$, where the sum is over the monic divisors of f. Verify the following identities :*

(a) $\sum_f d(f)|f|^{-s} = (1-q^{1-s})^{-2}$

(b) $\sum \sigma(f)|f|^{-s} = (1-q^{1-s})^{-1}(1-q^{2-s})^{-1}$

Proof. (a) With the notation of 7.19, for $s \in \mathbb{C}, \mathrm{Re}(s) > 1$, $\sum_{f\in U} |f|^{-s}$ is absolutely convergent and

$$(1-q^{1-s})^{-1} = \sum_{f\in U} |f|^{-s}$$

Then

$$\begin{aligned}(1-q^{1-s})^{-2} &= \sum_{f\in U} |f|^{-s} \sum_{g\in U} |g|^{-s}\\ &= \sum_{(f,g)\in U^2} |fg|^{-s}\\ &= \sum_{h\in U} \sum_{g\in U,\, g|h} |h|^{-s},\end{aligned}$$

indeed, the application

$$\varphi : \begin{cases} U \times U & \to & \{(h,g) \in U \times U, g \mid h\} \\ (f,g) & \mapsto & (fg,g) \end{cases}$$

is a bijection.

So

$$\begin{aligned}(1-q^{1-s})^{-2} &= \sum_{h \in U} |h|^{-s} \mathrm{Card}\{g \in U, g \mid h\} \\ &= \sum_{h \in U} |h|^{-s} d(h) \\ &= \sum_{f \in U} d(f)|f|^{-s}\end{aligned}$$

(b) Similarly,

$$\begin{aligned}(1-q^{1-s})^{-1}(1-q^{2-s})^{-1} &= \sum_{f \in U} |f|^{-s} \sum_{g \in U} |g|^{-s+1} \\ &= \sum_{(f,g) \in U^2} |g|\,|fg|^{-s} \\ &= \sum_{h \in U} \sum_{g \in U,\, g \mid h} |g|\,|h|^{-s} \\ &= \sum_{h \in U} |h|^{-s} \sum_{g \in U,\, g \mid h} |g| \\ &= \sum_{h \in U} \sigma(h)|h|^{-s} \\ &= \sum_{f \in U} \sigma(f)|f|^{-s}\end{aligned}$$

□

Ex. 7.21 *Let F be a field with $q = p^n$ elements. For $\alpha \in F$ set $f(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2}) \cdots (x-\alpha^{p^{n-1}})$. Show that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. In particular, $\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ and $\alpha\alpha^p\alpha^{p^2} \cdots \alpha^{p^{n-1}}$ are in $Z/p\mathbb{Z}$.*

Proof. Let $F : \begin{cases} \mathbb{F}_q & \to & \mathbb{F}_q \\ x & \mapsto & x^p \end{cases}$.

As the characteristic of $\mathbb{F}_q$ is p, $(x+y)^p = x^p + y^p$ et $(xy)^p = x^p y^p$, and each homomorphism of field is injective, F is a field automorphism (Frobenius automorphism).

For every automorphism H in $\mathbb{F}_q$, and every polynomial $p(x) = \sum a_i x^i \in \mathbb{F}_q[x]$, write $(H.p)(x) = \sum_i H(a_i)x^i$. Then for all $(p,q) \in \mathbb{F}_q[x]^2$, $H.(pq) = (H.p)(H.q)$.

With this notation,

$$f(x) = (x-\alpha)(x-F\alpha)(x-F^2\alpha)\cdots(x-F^{n-1}\alpha),$$

$$(H.f)(x) = (x-F\alpha)(x-F^2\alpha)(x-F^3\alpha)\cdots(x-F^n\alpha).$$

Since $\alpha \in \mathbb{F}_{p^n}$, $F^n\alpha = \alpha^{p^n} = \alpha$, thus

$$H.f = f.$$

In other words, if $f(x) = \sum_i a_i x^i$, then for all i, $H(a_i) = a_i$, so $a_i^p = a_i$, thus $a_i \in \mathbb{F}_p$, and $f \in \mathbb{F}_p[x]$. In particular, the coefficients $a_{n-1} = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}, a_0 = \alpha\alpha^p\alpha^{p^2}\cdots\alpha^{p^{n-1}}$ are in $\mathbb{F}_p$. $\square$

Ex. 7.22 *(continuation) Set* $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$*. Prove that*

(a) $\mathrm{tr}(\alpha) + \mathrm{tr}(\beta) = \mathrm{tr}(\alpha + \beta)$.

(b) $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$ *for* $a \in \mathbb{Z}/p\mathbb{Z}$.

(c) There is an $\alpha \in F$ *such that* $\mathrm{tr}(\alpha) \neq 0$.

Proof. Let F the Frobenius automorphism of $\mathbb{F}_q$ introduced in Ex.7.21.

(a),(b) : If $x, y \in \mathbb{F}_q$, and $a \in \mathbb{F}_p$, then $a^p = a$, so $F(x + y) = (x + y)^p = x^p + y^p = F(x) + F(y)$, and $F(ax) = a^p x^p = ax^p = aF(x)$, so F is $\mathbb{F}_p$-linear, and also $tr = I + F + F^2 + \cdots + F^{n-1}$.

(c) The polynomial $p(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ has degree p^{n-1}, so $p(x)$ has at most p^{n-1} roots in $\mathbb{F}_q$, and $|\mathbb{F}_q| = p^n > deg(p) = p^{n-1}$. Therefore there exist in $\mathbb{F}_q$ some element α which is not a root of $p(x)$, and so $\mathrm{tr}(\alpha) = p(\alpha) \neq 0$. $\square$

Ex. 7.23 *(continuation) For* $\alpha \in F$ *consider the polynomial* $x^p - x - \alpha \in F[x]$*. Show that this polynomial is either irreducible or the product of linear factors. Prove that the latter alternative holds iff* $\mathrm{tr}(\alpha) = 0$.

Proof. Let $f(x) = x^p - x - \alpha \in F[x]$. There exists an extension $K \supset F$ with finite degree on F which contains a root γ of f.

As $\gamma^p - \gamma - \alpha = 0$, then for all $i \in \mathbb{F}_p$,

$$(\gamma + i)^p - (\gamma + i) - \alpha = (\gamma^p - \gamma - \alpha) + i^p - i = 0.$$

So f has n distinct roots in K : $\gamma, \gamma + 1, \ldots, \gamma + p - 1$, and so

$$f(x) = (x - \gamma)(x - \gamma - 1)\cdots(x - \gamma - (p - 1)).$$

$F[\gamma]$ contains all roots of f.

• If $\gamma \in F$, $f(x)$ splits in linear factors in F. $f(x)$ is not irreducible, since $\deg(f) = p > 1$.

• If $\gamma \notin F$, we will show that f is irreducible in $F[x]$.

If not, then $f(x) = g(x)h(x)$ is the product of two polynomials $g, h \in F[x]$ such that $1 \leq \deg(g) \leq p - 1$.

The unicity of the decomposition in irreducible factors in $F[\gamma][x]$ shows that

$$g(x) = \prod_{i\in A}(x - \gamma - i),$$

where A is a subset of $\mathbb{F}_p$, with $A \neq \emptyset, A \neq \mathbb{F}_p$. As $g(x) \in F[x]$, $\sum\limits_{i\in A}(\gamma + i) = k\gamma + l \in \mathbb{F}_p$, where $1 \leq k = |A| \leq p - 1$ and $l = \sum\limits_{i\in A} i \in \mathbb{F}_p$.

So $k\gamma \in \mathbb{F}_p$. Since $\gamma \notin \mathbb{F}_p$, k is not invertible in $\mathbb{F}_p$, in contradiction with $1 \le k \le p-1$. Consequently, $f(x)$ is irreducible.

We conclude that $x^p - x - \alpha \in F[x]$ is irreducible iff $\gamma \notin F$.

Let F the Frobenius automorphism of K (cf. Ex. 7.21).

$$\alpha = F(\gamma) - \gamma, F(\alpha) = F^2(\gamma) - F(\gamma), \dots, F^{n-1}(\alpha) = F^n(\gamma) - F^{n-1}(\gamma).$$

The sum of these equalities gives

$$\mathrm{tr}(\alpha) = \alpha + F(\alpha) + \cdots + F^{n-1}(\alpha) = F^n(\gamma) - \gamma = \gamma^{p^n} - \gamma.$$

As the cardinality of F is $q = p^n$,

$$\gamma \in F \iff \gamma^{p^n} - \gamma = 0 \iff \mathrm{tr}(\alpha) = 0.$$

Conclusion : $x^p - x - \alpha$ is irreducible iff $\mathrm{tr}(\alpha) \ne 0$. If $\mathrm{tr}(\alpha) = 0$, $x^p - x - \alpha$ splits in linear factors in $F[x]$. □

Ex. 7.24 *Suppose that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has the property that $f(x+y) = f(x) + f(y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$. Show that $f(x)$ must be of the form $a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_mx^{p^m}$.*

Lemma *If the prime number p divides all binomial coefficients $\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}$, then n is a power of p.*

Proof. Let $u(x) = (x+1)^n - x^n - 1 \in \mathbb{F}_p[x]$. Then $f(x) = \sum\limits_{k=1}^{n-1} \binom{n}{i} x^i = 0$.

Write $n = p^a q$, with $p \wedge q = 1$. With a reductio as absurdum, suppose that $q > 1$. Then

$$f(x) = 0 = (x+1)^{p^\alpha q} - x^{p^\alpha q} - 1 = (x^{p^\alpha} + 1)^q - x^{p^\alpha q} - 1 = \sum_{k=1}^{q-1} \binom{q}{k} x^{kp^a}.$$

Consequently, the coefficient of x^{p^a} is null, so $p \mid q$: this is absurd. Therefore $q = 1$ and $n = p^a$. □

Proof. (Ex. 7.24)

Suppose that $f \in \mathbb{F}_p[x]$ verify in $\mathbb{F}_p[x,y]$ the equality $f(x+y) = f(x) + f(y)$.

Write $f(x) = \sum\limits_{k=1}^{d} c_i x^i$.

$$\begin{aligned} 0 = f(x+y) - f(x) - f(y) &= \sum_{n=0}^{d} c_n[(x+y)^n - x^n - y^n] \\ &= \sum_{n=0}^{d} \sum_{k=1}^{n-1} c_n \binom{n}{k} x^k y^{n-k} \end{aligned}$$

So for all n, for all k, $1 \le k \le n-1$, $c_n \binom{n}{k} = 0$ in $\mathbb{F}_p$.

From the lemma, if n is not a power of p, there exists a k, $1 \le k \le n-1$ such that $\binom{n}{k} \not\equiv 0 \pmod p$, so $c_n = 0$. If we write $a_k = c_{p^k}$, then $f(x)$ is of the form

$$f(x) = a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_mx^{p^m}.$$

□