11 Chapter 11 : FINITE FIELDS

11.1 THE STRUCTURE OF FINITE FIELDS

Ex. 11.1.1 *Let $\mathbb{F}_p \subset L$ be an extension such that $x^q - x$ splits completely over L, where $q = p^n$, and let F be the set of roots of this polynomial. Prove that F is a subfield of L.*

Proof. Let $q = p^n$, where p is prime. There exists an extension $\mathbb{F}_p \subset L$ such that $x^q - x$ splits completely over L. Write

$$F = \{\alpha \in L \mid \alpha^q = \alpha\}.$$

We show that F is a subfield of L, with q elements.

- $1 \in F$, since $1^q = 1$.
- As the characteristic of L is p, if $\alpha, \beta \in F$,

  $$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

  therefore $\alpha + \beta \in F$.
- If p is odd, $(-\alpha)^{p^n} = -\alpha^{p^n} = -\alpha$, so $-\alpha \in F$, and if $p = 2$, $-\alpha = \alpha \in F$.
- $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta$, so $\alpha\beta \in F$.
- If $\alpha \in F, \alpha \neq 0$, $(1/\alpha)^q = 1/\alpha^q = 1/\alpha$, therefore $1/\alpha \in F$.

Since the derivative of $f(x) = x^q - x$ is -1, then $\gcd(f, f') = 1$. Therefore $f(x)$ has q distinct roots in L, therefore $|F| = q = p^n$. □

Ex. 11.1.2 *Suppose that $f, g \in F[x]$ are polynomials, not both zero, and let h be their greatest common divisor as computed in $F[x]$. Now let L be an extension field of F. Prove that h is the greatest common divisor of f, g when considered as polynomial in $L[x]$.*

Proof. Recall the definition of the gcd in $F[x]$, where $f, g, h \in F[x]$:
$h = f \wedge g$ if and only if
(i) h is monic (or zero).
(ii) $h \mid f,\ h \mid g$
(iii) $\forall p \in F[x], (p \mid f,\ p \mid g) \Rightarrow p \mid h$.
Let L be an extension field of F. f satisfies (i)(ii) in $L[x]$, since h divides f in $F[x]$ if and only if h divides f in $L[x]$.

- If

  $$\forall p \in L[x], (p \mid f,\ p \mid g) \Rightarrow p \mid h,$$

  since $F[x] \subset L[x]$,

  $$\forall p \in F[x], (p \mid f,\ p \mid g) \Rightarrow p \mid h.$$

  So, $h = \gcd(f, g)$ in $L[x]$ implies that $h = \gcd(f, g)$ in $F[x]$.
- Conversely, suppose that $h = \gcd(f, g)$ in $F[x]$.

  By Bézout's Theorem, there exists $u, v \in F[x]$ such that $h = uf + vg$. Consequently, if $q \in L[x]$ divides f and g in $L[x]$, q divides h in $L[x]$. So h satisfies (iii), therefore h is the greatest common divisor of f, g in $L[x]$.

□

Ex. 11.1.3 *Give a proof of Corollary 11.1.8 that uses neither Theorem 11.1.7 nor the Galois correspondence.*

Corollary 11.1.8 *Let $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ be finite fields. Then $\mathbb{F}_{p^m}$ is isomorphic to a subfield of $\mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. As in the text, if $\mathbb{F}_{p^n}$ has a subfield with p^m elements, written $\mathbb{F}_{p^m}$, then

$$\mathbb{F}_p \subset \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n},$$

therefore

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \times m,$$

so $m \mid n$.

Conversely, suppose that $m \mid n$.

The elements of $\mathbb{F}_{p^n}$ are the p^n distinct roots of $x^{p^n} - x$.

Since $m \mid n$, then $n = km, k \in \mathbb{N}$, therefore $p^n - 1 = p^{km} - 1 = (p^m - 1) \sum_{i=0}^{k-1} p^{mi}$.

So $p^m - 1$ divides $p^n - 1$, thus $p^n - 1 = l(p^m - 1), l \in \mathbb{N}$. Consequently

$$x^{p^n-1} - 1 = x^{l(p^m-1)} - 1 = (x^{p^m-1} - 1) \sum_{j=0}^{l-1} x^{j(p^m-1)},$$

therefore $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$, and also $x^{p^m} - x \mid x^{p^n} - x$.

Therefore the polynomial $x^{p^m} - x$ splits completely over $\mathbb{F}_{p^n}$. By Exercise 1, the set of its roots is a subfield of $\mathbb{F}_{p^n}$ with p^m elements. By Corollary 11.1.3, it is isomorphic to $\mathbb{F}_{p^m}$. □

Ex. 11.1.4 *Prove Theorem 11.1.9*

Theorem 11.1.9 *Let $m \mid n$ and $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. Then there is a group isomorphism*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \simeq \mathbb{Z}/\frac{n}{m}\mathbb{Z}$$

that sends $(\mathrm{Frob}_p)^m \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ to $[1] \in \mathbb{Z}/\frac{n}{m}\mathbb{Z}$.

Proof. Write $F = \mathrm{Frob}_p$ the Frobenius automorphism of $\mathbb{F}_{p^n}$, which generates $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle F \rangle$ (Theorem 11.1.7).

Let $H = \langle F^m \rangle$ be the subgroup of G generated by F^m. As $m \mid n$, H is a cyclic subgroup with n/m elements, isomorphic to $\mathbb{Z}/\frac{n}{m}\mathbb{Z}$.

By the Galois correspondence, H corresponds to the fixed field L_H, and

$$\alpha \in L_H \iff F^m(\alpha) = F \iff \alpha^{p^m} = \alpha.$$

So L_H is the set of the roots of $x^{p^m} - x$. L_H is the unique subfield of $\mathbb{F}_{p^n}$ with p^m elements, written $\mathbb{F}_{p^m}$ (cf Exercise 3).

By the Fundamental Theorem of Galois Theory (section 7.3),

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \mathrm{Gal}(\mathbb{F}_{p^n}/L_H) = H = \langle F^m \rangle.$$

So

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle F^m \rangle \simeq \mathbb{Z}/\frac{n}{m}\mathbb{Z},$$

where the isomorphism sends $F^m = (\mathrm{Frob}_p)^m$ on the generator $[1] \in \mathbb{Z}/\frac{n}{m}\mathbb{Z}$. □

Ex. 11.1.5 *As noted in the text, if $f \in \mathbb{Z}[x]$ has degree n and its leading coefficient is not divisible by a prime p, then $f(x) \equiv 0 \mod p$ has at most n solutions modulo p. Here are two questions that explore what happens when $n = 2$ and the modulus is arbitrary.*

(a) How many solutions does the congruence $x^2 - 1 \equiv 0 \mod 8$ have modulo 8?

(b) Fix an integer $m > 1$, and assume that every polynomial of degree 2 in $\mathbb{Z}/m\mathbb{Z}[x]$ has at most two roots in $\mathbb{Z}/m\mathbb{Z}$. Is m prime?

Proof. (a) $\pm 1, \pm 3$ are the roots in $\mathbb{Z}/8\mathbb{Z}$ of the polynomial $x^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[x]$.

(b) Suppose that $m > 1$ is not prime. Then m is composite, so $m = uv$, where $1 < u \leq v < m$.

Let $f(x) = vx^2 \in \mathbb{Z}/m\mathbb{Z}[x]$. Then $f(0) = f(u) = f(2u) = 0$.

Moreover $u \not\equiv 0 \pmod{uv}, u \not\equiv 2u \pmod{uv}$.

If $2u \equiv 0 \pmod{uv}$, then $v \mid 2$. Since $1 < u \leq v$, then $u = v = 2$, and $m = 4$.

So if m is composite and $m > 4$, the polynomial $f(x) = vx^2 \in \mathbb{Z}/m\mathbb{Z}[x]$ has at least three distinct roots in $\mathbb{Z}/m\mathbb{Z}$.

If $m = 4$, the polynomial $g(x) = 2x^2 + 2x \in \mathbb{Z}/4\mathbb{Z}[x]$ has 4 roots, namely $0, 1, 2, 3$.

Conclusion:

If $m > 1$ is not prime, there exists some polynomial of degree 2 in $\mathbb{Z}/m\mathbb{Z}[x]$ with more than 2 roots in $\mathbb{Z}/m\mathbb{Z}[x]$.

If $m > 1$, and if every polynomial of degree 2 in $\mathbb{Z}/m\mathbb{Z}[x]$ has at most two roots in $\mathbb{Z}/m\mathbb{Z}[x]$, then m is prime.

□

Ex. 11.1.6 *Let $F \in \mathbb{Z}[x]$ have degree n, and assume that the leading coefficient of F is not divisible by p. Prove that the reduction of F modulo p is irreducible over $\mathbb{F}_p$ if and only if it is not possible to find polynomials $\varphi, \psi, \chi \in \mathbb{Z}[x]$, where $\deg(\varphi), \deg(\psi) < n$, such that*

$$\varphi(x)\psi(x) = F(x) + p\chi(x).$$

This is how Galois defines irreducibility modulo p in [Galois, p.113].

Proof. Write $\overline{F}, \overline{\varphi}, \overline{\psi} \in \mathbb{F}_p[x]$ the reductions modulo p of $F, \varphi, \psi \in \mathbb{Z}[x]$.

Let $F \in \mathbb{Z}[x]$ be a polynomial of degree $n > 0$, and assume that the leading coefficient of F is not divisible by p, so $\deg(\overline{F}) = n > 0$, $\overline{F}$ is not zero, and $\overline{F}$ is not an unit of $\mathbb{F}_p[x]$.

- Suppose that there exist polynomials $\varphi, \psi, \chi \in \mathbb{Z}[x]$, where $\deg(\varphi), \deg(\psi) < n$, such that
$$\varphi(x)\psi(x) = F(x) + p\chi(x).$$
Then $\overline{\varphi}(x)\overline{\psi}(x) = \overline{F}(x)$, and $\deg(\overline{\varphi}) \leq \deg(\varphi) < n$, and $\deg(\overline{\psi}) \leq \deg(\psi) < n$, with $\deg(\overline{F}) \geq 1$. Hence $\overline{F}$ is not irreducible in $\mathbb{F}_p[x]$.

  Conclusion: If $\overline{F}$ is irreducible over $\mathbb{F}_p$, it is not possible to find polynomials $\varphi, \psi, \chi \in \mathbb{Z}[x]$, where $\deg(\varphi), \deg(\psi) < n$, such that
$$\varphi(x)\psi(x) = F(x) + p\chi(x).$$

- Conversely, suppose that $\overline{F}$ is not irreducible in $\mathbb{F}_p[x]$. Then there exist polynomials $p, q \in \mathbb{F}_p[x]$ with $\deg(p), \deg(q) < n$ and $\overline{F}(x) = p(x)q(x)$.

  There exist some polynomials $\varphi, \psi \in \mathbb{Z}[x]$ such that $\overline{\varphi} = p, \overline{\psi} = q$ and $\deg(\varphi) = \deg(p) < n, \deg(\psi) = \deg(q) < n$ (if $p = \sum_{i=0}^{d} [a_i]x^i$, with $[a_d] \neq [0]$, take $\varphi = \sum_{i=0}^{d} a_i x^i$). Thus $\overline{F} = \overline{\varphi}\overline{\psi}$, therefore $\overline{\varphi\psi - F} = \overline{0}$, so $\varphi\psi - F \in p\mathbb{Z}[x]$: there exists $\chi \in \mathbb{Z}[x]$ such that
  $$\varphi(x)\psi(x) = F(x) + p\chi(x).$$

$\overline{F}$ is irreducible over $\mathbb{F}_p$ if and only if it is not possible to find polynomials $\varphi, \psi, \chi \in \mathbb{Z}[x]$, where $\deg(\varphi), \deg(\psi) < n$, such that

$$\varphi(x)\psi(x) = F(x) + p\chi(x).$$

□

Ex. 11.1.7 *Let $f \in \mathbb{F}_p[x]$ be irreducible of degree ν. Use (7.1) and Theorem 11.1.7 to prove Galois's observation that if i is one root of f in a splitting field, then the other roots are given by $i^p, i^{p^2}, \ldots, i^{p^{\nu-1}}$.*

Proof. Since f is irreducible, $L = \mathbb{F}_p[x]/\langle f \rangle$ is a field, and $[L : \mathbb{F}_p] = \deg(f) = \nu$, so $|L| = q = p^\nu$, and $L = \mathbb{F}_q$.

By Theorem 11.1.7, $\mathbb{F}_p \subset L = \mathbb{F}_q$ is a Galois extension, therefore L contains all roots of f, so L is the splitting field of f over $\mathbb{F}_p$.

Write $F = \mathrm{Frob}_p$ the Frobenius automorphism of $\mathbb{F}_q = \mathbb{F}_{p^\nu}$. By Theorem 11.1.7, $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle F \rangle$.

Since $\mathbb{F}_p \subset F_q$ is a Galois extension (Theorem 11.1.7(a)), the irreducible polynomial $f \in \mathbb{F}_p[x]$ is separable, so f has ν distinct roots.

If i is a root of f in $L = \mathbb{F}_q$, then $F^k(i),\ 0 \leq k < \nu$ is also a root of f. If j is any root of f, since f is irreducible, $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts transitively on the set of the roots of f, so there exists $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ such that $\sigma(i) = j$. Since $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle F \rangle$ and since the order of F is ν, there exists $k,\ 0 \leq k < \nu$, such that $F^k(i) = j$. Thus the set of the roots of f is

$$\{i, F(i) = F^2(i), \ldots, F^{\nu-1}(i)\} = \{i, i^p, i^{p^2}, \ldots, i^{p^{\nu-1}}\}.$$

Since f is separable, f has ν distinct roots, so these elements are distinct. Therefore

$$f(x) = (x - i)(x - i^p)(x - i^{p^2}) \cdots (x - i^{p^{\nu-1}}).$$

(This is an example of (7.1).) □

Ex. 11.1.8 *Let I and J be ideals in a ring R, and let $I + J = \{r + s \mid r \in I, s \in J\}$ be their sum. Also let $\overline{I} = \{r + J \mid r \in I\}$. This is a subset of the quotient ring R/J.*

(a) Prove that $I + J$ is an ideal of R and that $\overline{I}$ is an ideal of R/J.

(b) Show that the map $r + (I + J) \mapsto (r + J) + \overline{I}$ defines a well-defined ring isomorphism $R/(I + J) \simeq (R/J)/\overline{I}$.

Proof. (a) $I + J$ is a subgroup of $(R, +)$. If $t \in I + J$ and $u \in R$, then $t = r + s, r \in I, s \in J$. As I, J are ideals of R, $ur \in I, us \in J$, therefore $ut = ur + us \in I + J$, so $I + J$ is an ideal of R.

$\overline{I}$ is a subgroup of R/J, image of I by the natural projection $\pi : R \to R/J$.

Let $\overline{r} = r + J, r \in I$ be an element of $\overline{I}$, and $\overline{s} = s + J, s \in R$ be any element of R/J. Then by definition of the laws in R/J,

$$\overline{s}\,\overline{r} = (s + J)(r + J) = sr + J,$$

and $sr \in I$, since $s \in R, r \in I$. Therefore $\overline{s}\,\overline{r} \in \overline{I}$, so $\overline{I}$ is an ideal of R/J.

(b) If $r + (I + J) = s + (I + J)$, then $r - s \in I + J$, so $r - s = i + j$ for some $i \in I, j \in J$.

Then $(r + J) - (s + J) = (r - s) + J = i + j + J = i + J \in \overline{I}$, since $i \in I$. So $(r + J) + \overline{I}$ depends only of the class of r modulo $I + J$, and the map

$$\varphi : \left\{ \begin{array}{ccc} R/(I+J) & \to & (R/J)/\overline{I} \\ r + (I + J) & \mapsto & (r + J) + \overline{I} \end{array} \right.$$

is well defined.

φ is a ring homomorphism: if $\overline{r} = r + I + J, \overline{s} = s + I + J$, then

$$\begin{aligned} \varphi(\overline{r}) + \varphi(\overline{s}) &= ((r + J) + \overline{I}) + ((s + J) + \overline{I}) \\ &= ((r + J) + (s + J)) + \overline{I} \\ &= (r + s + J) + \overline{I} \\ &= \varphi(\overline{r + s}) \\ &= \varphi(\overline{r} + \overline{s}) \end{aligned}$$

and similarly $\varphi(\overline{r})\varphi(\overline{s}) = \varphi(\overline{r}\overline{s})$ (and $\varphi(1) = (1 + J) + \overline{I}$ is the unit of $(R/J)/\overline{I}$).

φ is injective: if $r + (I + J) \in \ker(\varphi)$, then $(r + J) + \overline{I} = \overline{I}$, therefore $r + J \in \overline{I}$, so $r + J = i + J$,where $i \in I$, so $j = r - i \in J$ and $r = i + j \in I + J$, $r + (I + J) = I + J$ is zero in $R/(I + J)$.

φ is surjective: any element y of $(R/J)/\overline{I}$ is of the form $y = u + \overline{I}$, where $u \in R/J$ is such as $u = r + J$, where $r \in I$, so $y = (r + J) + \overline{I} = \varphi(r + I + J)$.

Conclusion :

$$R/(I + J) \simeq (R/J)/\overline{I}.$$

□

Ex. 11.1.9 *Let $f \in \mathbb{Z}[x]$ be monic and irreducible, and let $\alpha \in \mathbb{C}$ be a root of f. Then let $\overline{f} \in \mathbb{F}_p[x]$ be the reduction of f modulo the prime p, and let $\langle p, f\rangle$ be as in (11.4):*

$$\langle p, f\rangle = p\mathbb{Z}[x] + f\mathbb{Z}[x] = \{pR(x) + f(x)S(x) \mid R(x), S(x) \in \mathbb{Z}[x]\}.$$

(a) Prove that the map $q(x) + f\mathbb{Z}[x] \mapsto q(\alpha)$ is a well-defined ring isomorphism

$$\mathbb{Z}[x]/f\mathbb{Z}[x] \simeq \mathbb{Z}[\alpha].$$

(b) Use Exercise 8 to prove that $\mathbb{Z}[x]/\langle p, f\rangle \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$.

(c) Similarly prove that $\mathbb{Z}[x]/\langle p, f\rangle \simeq \mathbb{F}_p[x]/\langle\overline{f}\rangle$.

Proof. (a) If $q_1, q_2 \in \mathbb{Z}[x]$ are such that $q_1(x) + f\mathbb{Z}[x] = q_2(x) + f\mathbb{Z}[x]$, then there exist $u_1, u_2 \in \mathbb{Z}[x]$ such that $q_1(x) + f(x)u_1(x) = q_2(x) + f(x)u_2(x)$. Since $f(\alpha) = 0$, then $q_1(\alpha) = q_2(\alpha)$, so the map

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}[x]/f\mathbb{Z}[x] & \to & \mathbb{Z}[\alpha] \\ q(x) + f\mathbb{Z}[x] & \mapsto & q(\alpha) \end{array} \right.$$

is well defined.

Let $\tilde{q} = q(x) + f\mathbb{Z}[x], \tilde{r} = r(x) + f\mathbb{Z}[x]$ be elements of $\mathbb{Z}[x]/f\mathbb{Z}[x]$. Then

$$\varphi(\tilde{q}) + \varphi(\tilde{r}) = q(\alpha) + r(\alpha) = (q + r)(\alpha) = \varphi(q(x) + r(x) + f\mathbb{Z}[x]) = \varphi(\tilde{q} + \tilde{r}).$$

Similarly, $\varphi(\tilde{q})\varphi(\tilde{r}) = \varphi(\tilde{q}\,\tilde{r})$, and $\varphi(\tilde{1}) = 1$, so φ is a ring homomorphism.

If $\varphi(\tilde{q}) = 0$, then $q(\alpha) = 0$. As f is the minimal polynomial of α over $\mathbb{Q}$, f divides q in $\mathbb{Q}[x]$, so $q = uf$, where $u \in \mathbb{Q}[x]$. But f is a monic polynomial in $\mathbb{Z}[x]$, so the algorithm of the Euclidean division gives a quotient $u \in \mathbb{Z}[x]$, therefore $q \in f\mathbb{Z}[x]$, and $\tilde{q} = 0$. $\ker(\varphi) = \{\tilde{0}\}$, so φ is injective.

Any element z of $\mathbb{Z}[\alpha]$ is of the form $z = q(\alpha), q \in \mathbb{Z}[x]$, so $z = q(\alpha) = \varphi(\tilde{q})$: φ is surjective.

φ is a ring isomorphism:

$$\mathbb{Z}[x]/f\mathbb{Z}[x] \simeq \mathbb{Z}[\alpha].$$

(b) Let R be the ring $\mathbb{Z}[x]$, and $I = p\mathbb{Z}[x]$, $J = f\mathbb{Z}[x]$ be the principal ideals of $\mathbb{Z}[x]$ generated by p and f. By Exercise 8,

$$\overline{I} = \{r + J \mid r \in I\} = \{pq(x) + f\mathbb{Z}[x] \mid q(x) \in \mathbb{Z}[x]\}$$

is an ideal of $\mathbb{Z}[x]/f\mathbb{Z}[x]$, and

$$\mathbb{Z}[x]/\langle p, f\rangle = \mathbb{Z}[x]/(p\mathbb{Z}[x] + f\mathbb{Z}[x]) \simeq (\mathbb{Z}[x]/f\mathbb{Z}[x])/\overline{I}.$$

The isomorphism φ of part (a) sends $\mathbb{Z}[x]/f\mathbb{Z}[x]$ on $\mathbb{Z}[\alpha]$ and the ideal $\overline{I}$ on $p\mathbb{Z}[\alpha]$, since $\varphi(pq(x) + f\mathbb{Z}[x]) = pq(\alpha)$ for all $q \in \mathbb{Z}[x]$.

Therefore $(\mathbb{Z}[x]/f\mathbb{Z}[x])/\overline{I} \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$, so

$$\mathbb{Z}[x]/\langle p, f\rangle \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha].$$

(c) If we switch I, J, then by Exercise 8, $R/(I + J) = R/(J + I) \simeq (R/I)/\overline{J}$, where

$$\overline{J} = \{s + I \mid s \in J\} = \{f(x)v(x) + p\mathbb{Z}[x] \mid v(x) \in \mathbb{Z}[x]\},$$

so

$$\mathbb{Z}[x]/\langle p, f\rangle \simeq (\mathbb{Z}[x]/p\mathbb{Z}[x])/\overline{J}.$$

Let

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}[x]/p\mathbb{Z}[x] & \to & \mathbb{F}_p[x] \\ u + p\mathbb{Z}[x] & \mapsto & \overline{u}, \end{array} \right.$$

where $\overline{u}$ is the reduction of $u \in \mathbb{Z}[x]$ modulo the prime p.

As in part (a), ψ is a well-defined ring isomorphism, and ψ sends $\overline{J}$ on $\langle\overline{f}\rangle$, since for all $v(x) \in \mathbb{Z}[x]$, $\psi(f(x)v(x) + p\mathbb{Z}[x]) = \overline{f}\,\overline{v}$, and $\overline{v}$ takes all possible values in $\mathbb{F}_p[x]$ when $v \in \mathbb{Z}[x]$. Therefore $(\mathbb{Z}[x]/p\mathbb{Z}[x])/\overline{J} \simeq \mathbb{F}_p[x]/\langle\overline{f}\rangle$, so

$$\mathbb{Z}[x]/\langle p, f\rangle \simeq \mathbb{F}_p[x]/\langle\overline{f}\rangle.$$

Finally, if α is a root of the irreducible polynomial $f \in \mathbb{Z}[x]$,

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{F}_p[x]/\langle\overline{f}\rangle,$$

and so $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ is a finite field. □

Ex. 11.1.10 *Let* $f = 2+2x+2x^2+2x^3+2x^4+2x^5+2x^6+2x^7+x^8+x^9+x^{10} \in \mathbb{F}_3[x]$.

(a) Use the method of Example 11.1.6 to determine the number of roots of f *in* $\mathbb{F}_{3^3}$ *and* $\mathbb{F}_{3^7}$.

(b) Explain why the splitting field of f *over* $\mathbb{F}_3$ *is* $\mathbb{F}_{3^{21}}$.

Proof.

(a) With the following Sage instructions:

```
sage: R.<x> = PolynomialRing(GF(3))
sage: f = -1-x-x^2-x^3-x^4-x^5-x^6-x^7+x^8+x^9+x^10
sage: gcd(f,x^(3^3) -x)
x^3 + 2*x^2 + x + 1
sage: gcd(f,x^(3^7) -x)
x^7 + 2*x^6 + 2*x^5 + x^4 + 2*x^3 + x^2 + 2
sage: gcd(f,x^3-x)
1
```

we know that f has 3 roots in $\mathbb{F}_{3^3}$, 7 roots in $\mathbb{F}_{3^7}$ (and no root in $\mathbb{F}_3$).

(The degree of $x^{3^{21}} - x$ is $10,460,353,203$. Too big for my computer!)

(b) We take all the finite field $\mathbb{F}_{p^\nu}$ as subfields of an algebraic closure Ω of $\mathbb{F}_p$, so by Corollary 11.1.8,

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n \mid m.$$

(If you don't like algebraic closure, you can replace Ω by $\mathbb{F}_{3^{21}}$ which contains all the fields considered in this exercise.)

Note that

$$\mathbb{F}_{3^3} \cap \mathbb{F}_{3^7} = \mathbb{F}_3.$$

Indeed, $\mathbb{F}_{3^3} \cap \mathbb{F}_{3^7}$ is a finite subfield of Ω, so is of the form $\mathbb{F}_{3^n}$, where $n \mid 3$ and $n \mid 7$, thus $n = 1$.

Moreover f has not root in $\mathbb{F}_3$, since $\gcd(f, x^3 - x) = 1$. So the sets of the roots of f in $\mathbb{F}_{3^3}$ and $\mathbb{F}_{3^7}$ are disjointed. Therefore f has 10 distinct roots in any field which contains $\mathbb{F}_{3^3}$ and $\mathbb{F}_{3^7}$. In particular f has 10 distinct roots in $\mathbb{F}_{3^{21}}$, and $\deg(f) = 10$, so f splits completely in $\mathbb{F}_{3^{21}}$.

Name $\alpha_1, \alpha_2, \alpha_3$ the three roots of f in $\mathbb{F}_{3^3}$, and $\alpha_4, \ldots, \alpha_{10}$ the seven roots of f in $\mathbb{F}_{3^7}$.

Since 7 is prime, there is no strictly intermediate field between $\mathbb{F}_3$ and $\mathbb{F}_{3^7}$, and since $\alpha_i \notin \mathbb{F}_3$, then $\mathbb{F}_3(\alpha_4, \ldots, \alpha_7) = \mathbb{F}_{3^7}$, and similarly $\mathbb{F}_3(\alpha_1, \alpha_2, \alpha_3) = \mathbb{F}_{3^3}$.

Let $K = \mathbb{F}_3(\alpha_1, \ldots, \alpha_{10})$. Then $K = \mathbb{F}_{3^r}$ $(r \in \mathbb{N})$, is a finite subfield of Ω, which contains $\mathbb{F}_{3^3}$ and $\mathbb{F}_{3^7}$, so $3 \mid r$ and $7 \mid r$, with $\gcd(3,7) = 1$, thus $21 \mid r$, therefore $K = \mathbb{F}_{3^r} \supset \mathbb{F}_{3^{21}}$, so $\mathbb{F}_{3^{21}} \subset \mathbb{F}_3(\alpha_1, \ldots, \alpha_{10})$. Moreover $\alpha_1, \ldots, \alpha_{10}$ are in $\mathbb{F}_{3^{21}}$, so

$$\mathbb{F}_3(\alpha_1, \ldots, \alpha_{10}) = \mathbb{F}_{3^{21}}.$$

(In other words $\mathbb{F}(\alpha_1, \ldots, \alpha_{10})$ is the compositum in Ω of $\mathbb{F}_3(\alpha_1, \alpha_2, \alpha_3) = \mathbb{F}_{3^3}$ and $\mathbb{F}_3(\alpha_4, \ldots, \alpha_7) = \mathbb{F}_{3^7}$, and the compositum of $\mathbb{F}_{3^3}$ and $\mathbb{F}_{3^7}$ in Ω is $\mathbb{F}_{3^{21}}$, so $\mathbb{F}_3(\alpha_1, \ldots, \alpha_{10}) = \mathbb{F}_{3^{21}}$.)

Therefore, $\mathbb{F}_{3^{21}}$ is the splitting field of f over $\mathbb{F}_3$. □

Ex. 11.1.11 *Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Prove that f splits completely in $\mathbb{F}_{p^n}$.*

Proof. Let $F = \mathbb{F}_p[x]/\langle f \rangle$. Since f is irreducible over $\mathbb{F}_p$, F is a field, and since $\deg(f) = n$, $|F| = p^n$, so F is a field with p^n elements.

Moreover $\overline{x} = x + \langle f \rangle$ is a root of f in F.

By Theorem 11.1.2, F is a splitting field over $\mathbb{F}_p$ of the separable polynomial $x^{p^n} - x$, therefore F is a Galois extension of $\mathbb{F}_p$. As the irreducible polynomial f has one root in F, it splits completely in F.

If $\mathbb{F}_{p^n}$ is a field with p^n elements, there exists an isomorphism $\varphi : F \to \mathbb{F}_{p^n}$, which sends the roots of f in F on roots of f in $\mathbb{F}_{p^n}$, so f splits completely in $\mathbb{F}_{p^n}$, and this don't depends of the choice of the field with p^n elements that we name $\mathbb{F}_{p^n}$. □

Note: let α be a root of f in $\mathbb{F}_{p^n}$, and $\alpha_1 = \alpha, \ldots, \alpha_n$ the roots of f in $\mathbb{F}_{p^n}$. Then $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, hence $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \subset \mathbb{F}_p(\alpha_1, \ldots, \alpha_n) \subset \mathbb{F}_{p^n}$, we conclude that

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$$

is a splitting field of f over $\mathbb{F}_p$.

Since $\mathbb{F}_{p^n}$ is a splitting field of f over $\mathbb{F}_p$, by Exercise 7,

$$f(x) = a(x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \cdots (x - \alpha^{p^{n-1}}),\ a \in \mathbb{F}_p.$$

11.2 IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS (OPTIONAL)

Ex. 11.2.1 *Let $f \in F[x]$ be irreducible, where F is a finite field. Prove that f is separable.*

Proof. Let L be the splitting field of f over F, and $n = [L : F]$. Let $q = |F|$, where $q = p^\nu$ is a power of the characteristic p. Since L is a vector space with dimension n over F, then $|L| = q^n$ for some integer n. Therefore the order of every element of the group L^* divides $q^n - 1$, so for every element $\gamma \in L^*$, $\gamma^{q^n - 1} = 1$. Consequently every element of L is a root of $h(x) = x^{q^n} - x$. Since $h'(x) = -1$, $\gcd(h, h') = 1$, so h is a separable polynomial. If α is a root of f in the splitting field L, $h(\alpha) = 0$ and f is irreducible over F, so f divides h, and h is separable, therefore f is a separable polynomial.

□

Ex. 11.2.2 *This exercise concerns Theorem 11.2.2 and the factorisation (11.7).*

(a) Compute N_3 and N_4 using only Theorem 11.2.2.

(b) Write down the factorization (11.7) explicitly when $p^n = 4$ and 8.

Proof. (a) We know (Example 11.2.3) that $N_1 = p, N_2 = \frac{1}{2}(p^2 - p)$.

By Theorem 11.2.2,

$$3N_3 + N_1 = p^3,$$
$$4N_4 + 2N_2 + N_1 = p^4.$$

Therefore

$$N_3 = \frac{1}{3}(p^3 - p),$$
$$N_4 = \frac{1}{4}(p^4 - p^2).$$

(b) For $p = 2$ and $n = 2, n = 3$, we obtain $N_2 = 1, N_3 = 2$.

The factorisation (11.7) is here

$$x^4 - x = x(x-1) \times (x^2 + x + 1),$$

so $x^2 + x + 1$ is the only irreducible polynomial over $\mathbb{F}_2$ of degree 2.

With the following Sage instructions

```
R.<x> = GF(2)[]
factor(x^8-x)
```

give

$$x \cdot (x+1) \cdot (x^3 + x + 1) \cdot (x^3 + x^2 + 1).$$

So the two irreducible polynomial over $\mathbb{F}_2$ of degree 3 are

$$x^3 + x + 1, \qquad x^3 + x^2 + 1.$$

□

Ex. 11.2.3 *Use Theorem 11.2.4 to compute N_6 and N_{36}.*

Proof. By Theorem 11.2.4,

$$N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{\frac{n}{m}}.$$

$$\begin{aligned} N_6 &= \frac{1}{6}(\mu(1)p^6 + \mu(2)p^3 + \mu(3)p^2 + \mu(6)p) \\ &= \frac{1}{6}(p^6 - p^3 - p^2 + p) \end{aligned}$$

The $9 = 3 \times 3$ factors d of $36 = 2^2 \times 3^2$, and the corresponding values of $\mu(d)$ are

d	1	2	3	4	6	9	12	18	36
$\mu(d)$	1	−1	−1	0	1	0	0	0	0

$$N_{36} = \frac{1}{36}(p^{36} - p^{18} - p^{12} + p^6)$$

□

Ex. 11.2.4 *In Theorem 11.1.4 we used slitting fields to show that a field of order p^n exists for any prime p and integer $n \geq 1$. When Galois and others considered this question in the nineteenth century, their approach was to prove the existence of an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n. In other words, they needed to prove that $N_n > 0$.*

(a) Prove that $N_n > 0$ using Theorem 11.1.4.

(b) Suppose that we have proved Theorem 11.2.4 but not Theorem 11.1.4. Use this to prove that $N_n > 0$.

Proof. (a) By Theorem 11.1.4, there exists a finite field $\mathbb{F}_{p^n}$ with p^n elements. We know that the group $\mathbb{F}_{p^n}^*$ is cyclic. If α is a generator of $\mathbb{F}_{p^n}^*$, then $\alpha^{p^n-1} = 1$, and

$$\mathbb{F}_{p^n} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\} = \mathbb{F}_p(\alpha).$$

This proves the Primitive Element Theorem in the case where the field is finite. Let f be the minimal polynomial of α. Then $\deg(f) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and f is monic irreducible over $\mathbb{F}_p$, so $N_n > 0$.

(b) By Theorem 11.2.4,

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the decomposition of n in primes.The factors d of n such that $\mu\left(\frac{n}{d}\right) \neq 0$ are the integers $d = p_1^{\alpha_1-\beta_1} \cdots p_s^{\alpha_s-\beta_s}$ where $\beta_i = 0, 1$. The minimum such factor is $d_{min} = p_1^{\alpha_1-1} \cdots p_s^{\alpha_s-1}$.

If $N_n = 0$ then $\sum_{d|n} \mu(\frac{n}{d}) p^d = 0$. Dividing by $p^{d_{min}}$,

$$\sum_{d|n,\, d>d_{min}} \mu\left(\frac{n}{d}\right) p^{d-d_{min}} = -\mu\left(\frac{n}{d_{min}}\right) = \pm 1.$$

As p divides the left sum, $p \mid 1$. This is a contradiction, so $N_n > 0$.

(This gives another proof of Theorem 11.1.4.)

□

Ex. 11.2.5 *Let F be a field of characteristic p, and let $\alpha \in F$ be a root of unity. Prove that there is some $d \geq 1$ relatively prime to p such that α is a dth root of unity.*

Proof. Suppose that $\alpha \in F$ satisfies $\alpha^n = 1$ for some $n > 0$.

As the characteristic of F is p, $\mathbb{F}_p$ is a subfield of F. Since α is a root of $x^n - 1$, then α is algebraic over $\mathbb{F}_p$, and $\nu = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] < \infty$, so $|\mathbb{F}_p(\alpha)| = p^\nu$ is finite, and $\mathbb{F}_p(\alpha)$ is a finite field with $q = p^\nu$ elements. Since α is in the group $\mathbb{F}_p(\alpha)^*$, by Lagrange's Theorem,

$$\alpha^{p^\nu-1} = 1.$$

Let $d \geq 1$ the order of α in the group $\mathbb{F}_p(\alpha)^*$. Then $\alpha^d = 1$ and $d \mid p^\nu - 1$, so d is relatively prime to p. □

Ex. 11.2.6 *This exercise is concerned with Example 11.2.8.*

(a) Show that $N_4 = 3$ when $p = 2$. Then write down these three irreducible polynomials explicitly.

(b) Verify the factorization of $\Phi_{15}(x)$ given in the example.

(c) Show that the roots of $x^4 + x^3 + 1$ and $x^4 + x + 1$ are the reciprocals of each other.

Proof. (a) For $p = 2$, by Exercise 4,

$$N_4 = \frac{1}{4}(2^4 - 2^2) = 3.$$

With the Sage instructions

```
R.<x> = GF(2)[]
factor(x^16-x)
```

we obtain

$$x^{16} - x = x \cdot (x+1) \cdot (x^2+x+1) \cdot (x^4+x+1) \cdot (x^4+x^3+1) \cdot (x^4+x^3+x^2+x+1).$$

So the irreducible polynomial of degree 4 are

$$x^4 + x + 1, \qquad x^4 + x^3 + 1, \qquad x^4 + x^3 + x^2 + x + 1.$$

(b) As $x^{15} - 1 = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$,

$$\begin{aligned} \Phi_{15}(x) &= \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)} \\ &= \frac{x^{10}+x^5+1}{x^2+x+1} \\ &= x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 \end{aligned}$$

The Sage instructions

```
R.<x>= GF(2)[]
p = (x^10+x^5+1)/(x^2+x+1)
factor(p)
```

give the factorization in $\mathbb{F}_2[x]$

$$\Phi_{15}(x) = (x^4 + x + 1) \cdot (x^4 + x^3 + 1).$$

(c) If α is a root of $x^4 + x^3 + 1$, then $\alpha \neq 0$ and $\alpha^4 + \alpha^3 + 1 = 0$. Dividing by α^4,

$$1 + \frac{1}{\alpha} + \frac{1}{\alpha^4} = 0,$$

α^{-1} is a root of $x^4 + x + 1$. Similarly, if β is a root of $x^4 + x + 1$, β^{-1} is a root of $x^4 + x^3 + 1$. (All these roots are the primitive 15th roots of unity in $\mathbb{F}_{16}$.)

□

Ex. 11.2.7 *As in the discussion of Berlekamp's algorithm, let $R = \mathbb{F}_p[x]/\langle f\rangle$ and consider the pth power map $T : R \to R$. Prove that T is a linear map when R is regarded as a vector space over $\mathbb{F}_p$.*

Proof. Let $\overline{g} = g + \langle f\rangle, \overline{h} = h + \langle f\rangle \in T$, and $\lambda \in \mathbb{F}_p$. Since the characteristic is p, $(g+h)^p = g^p + h^p$, so

$$\begin{aligned} T(\overline{g} + \overline{f}) &= (g+h)^p + \langle f\rangle \\ &= g^p + h^p + \langle f\rangle \\ &= (g^p + \langle f\rangle) + (h^p + \langle f\rangle) \\ &= T(\overline{g}) + T(\overline{h}). \end{aligned}$$

Since $\lambda \in \mathbb{F}_p$, $\lambda^p = \lambda$, and $\lambda\langle f\rangle = \langle \lambda f\rangle$, $\lambda(g + \langle f\rangle) = \lambda g + \langle f\rangle$, so

$$\begin{aligned} T(\lambda\overline{g}) &= T(\lambda g + \langle f\rangle) \\ &= (\lambda g)^p + \langle f\rangle \\ &= \lambda g^p + \langle f\rangle \\ &= \lambda(g^p + \langle f\rangle) \\ &= \lambda T(\overline{g}). \end{aligned}$$

Thus $T : R \to R$ is linear. □

Ex. 11.2.8 *Prove that Gauss formula (11.10) is equivalent to the formula given in Theorem 11.2.4.*

Proof. Let $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ the decomposition of n in primes. If $m \mid n$, then $m = p_1^{\beta_1} \cdots p_s^{\beta_s^s}$, $0 \le \beta_k \le \alpha_k$.

If $\beta_k > 1$ for some $k = 1, \ldots, s$, then by definition $\mu(m) = 0$, so $\beta_k = 0$ or 1 if $\mu(m) \neq 0$.

The nonzero terms in the sum

$$N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{\frac{n}{m}}$$

are those which satisfy $m = p_{i_1} \cdots p_{i_r}$, with $1 \le i_1 < \cdots < i_r \le s$, so $\mu(m) = (-1)^r$.

Thus

$$N_n = \frac{1}{n} \sum_{m|n} \mu(m)\, p^{\frac{n}{m}} = \frac{1}{n} \sum_{1 \le i_1 < \cdots < i_r \le s} (-1)^r\, p^{\frac{n}{p_{i_1} \cdots p_{i_r}}}.$$

With a less formal writing, we obtain

$$N_n = \frac{1}{n} \sum_{m|n} \mu(m)\, p^{\frac{n}{m}} = \frac{1}{n} \left(p^n - \sum_a p^{\frac{n}{a}} + \sum_{a,b} p^{\frac{n}{ab}} - \sum_{a,b,c} p^{\frac{n}{abc}} + \cdots \right),$$

where $\sum_a$ is the sum over all distinct primes a dividing n, $\sum_{a,b}$ is the sum over all products of distinct primes a, b dividing n, and so on. □

Ex. 11.2.9 *State and prove analogs of Theorem 11.2.2 and 11.2.4 that count monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$, where q is now a power of the prime p.*

Let $q = p^\nu$ a power of the prime p.

Proposition 11.2.1 bis. *Let $f \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$, of degree m. Then:*

(a) f divides $x^{q^m} - x$.

(b) f is separable.

(c) Given an integer $n \geq 1$, f divides $x^{q^n} - x \iff f$ has a root in $\mathbb{F}_{q^n} \iff m \mid n$.

Proof. Note: we suppose that all the fields considered here are subfields of a field Ω, which can be an algebraic closure of $\mathbb{F}_q$. In this case, there is a unique subfield of Ω with a given cardinality q^d, written $\mathbb{F}_{q^d}$, where

$$\mathbb{F}_{q^d} = \{\alpha \in \Omega \mid \alpha^{q^d} = \alpha\}.$$

We begin with part (c). Let $\alpha \in \Omega$ be a root of f. Since f is irreducible over $\mathbb{F}_q$, the extension $\mathbb{F}_q \subset \mathbb{F}_q(\alpha)$ has degree $m = \deg(f)$. So $|\mathbb{F}_q(\alpha)| = q^m$, therefore $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ (see the note). If $\alpha \in \mathbb{F}_{q^n}$, then $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, therefore $m \mid n$ (Corollary 11.1.8). Conversely, if $m \mid n$, then $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$, so the root α of f is in $\mathbb{F}_{q^n}$. This proves the second equivalence of part (c).

If f has a root $\alpha \in \mathbb{F}_{q^n}$, then $\alpha^{q^n} = \alpha$, so α is a root of $x^{q^n} - x$. As f is the minimal polynomial of α over $\mathbb{F}_q$, $f(x) \mid x^{q^n} - x$.

Conversely, suppose that $f(x) \mid x^{q^n} - x$. Take any root α of f in Ω. As $f(x) \mid x^{q^n} - x$, then $\alpha^{q^n} = \alpha$, and this implies $\alpha \in \mathbb{F}_{q^n}$, so (c) is proved.

We get part (a) by taking $n = m$ in part (c), and part (b) follows immediately, since $x^{q^n} - x = x^{p^{n\nu}} - x$ is separable by the proof of Theorem 11.1.4.

□

Theorem 11.2.2 bis. *Let*

$$\mathcal{N}'_m = \{f \in \mathbb{F}_q[x] \mid f \text{ is monic irreducible over } \mathbb{F}_q \text{ of degree } m\},$$

and $N'_m = |\mathcal{N}'_m|$.

Then, for any $n \geq 1$, we have

$$\sum_{m|n} m N'_m = q^n,$$

where the sum is over all positive divisors of n.

Proof. Since $x^{q^n} - x$ is separable, we know that it factors as a product of distinct irreducible polynomials in $\mathbb{F}_p[x]$. Furthermore, since it is monic, we can assume that the polynomials in the factorization are also monic. Finally, part (c) of Proposition 11.2.1 bis shows that the polynomials in the factorization are *all* monic irreducible polynomials of $\mathbb{F}_p[x]$ whose degree m divides n. Thus

$$x^{q^n} - x = \prod_{m|n} \prod_{f \in \mathcal{N}'_m} f.$$

Since every $f \in \mathcal{N}_m$ has degree m, taking the degree of each side give the desired formula. □

Theorem 11.2.4 bis. The number of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ is given by

$$N'_n = \frac{1}{n}\sum_{m|n}\mu(m)q^{\frac{n}{m}}.$$

Proof. Write $F(n) = nN'_n$,and $G(n) = \sum_{m|n} F(m) = q^n$.

The Möbius inversion formula gives $F(n) = \sum_{m|n}\mu(m)G\left(\frac{n}{m}\right)$. So

$$nN'_n = \sum_{m|n}\mu(m)q^{\frac{n}{m}}.$$

□

Ex. 11.2.10 *Suppose that a monic polynomial $f \in \mathbb{F}_p[x]$ has a factorization $f = f_1 \cdots f_k$, where $f_1, \ldots, f_k$ are distinct monic irreducible polynomials. Let $R = \mathbb{F}_p[x]/\langle f\rangle$, and let $R_i = \mathbb{F}_p[x]/\langle f_i\rangle$ for $i = 1, \ldots, k$. Then consider the map*

$$\varphi : R \to R_1 \times \cdots \times R_k$$

defined by

$$\varphi(g + \langle f\rangle) = (g + \langle f_1\rangle, \ldots, g + \langle f_k\rangle).$$

The goal of this exercise is to prove that φ is a ring isomorphism when we make $R_1 \times \cdots R_k$ into a ring using coordinatewise addition and multiplication.

(a) Prove that φ is a well-defined ring homomorphism.

(b) Prove that φ is one-to-one.

(c) Show that R and $R_1 \times \cdots \times R_k$ have the same dimension when considered as vector spaces over $\mathbb{F}_p$.

(d) Use the dimension theorem from linear algebra to conclude that φ is a ring isomorphism.

Proof. (a) Let $g, h \in \mathbb{F}_p[x]$. If $g+\langle f\rangle = h+\langle f\rangle$, then $f \mid g-h$. Since $f_i \mid f$, $i = 1, \ldots, k$, then $f_i \mid g - h$, so $g + \langle f_i\rangle = h + \langle f_i\rangle$. Therefore φ is well-defined.

Write $\overline{g} = g + \langle f\rangle, g \in \mathbb{F}_p[x]$. For all $g, h \in \mathbb{F}_p[x]$,

$$\begin{aligned}\varphi(\overline{g} + \overline{h}) &= (g + h + \langle f_1\rangle, \ldots, g + h + \langle f_k\rangle)\\ &= (g + \langle f_1\rangle + h + \langle f_1\rangle, \ldots, g + \langle f_k\rangle + h + \langle f_k\rangle)\\ &= (g + \langle f_1\rangle, \ldots, g + \langle f_k\rangle) + (h + \langle f_1\rangle, \ldots, h + \langle f_k\rangle)\\ &= \varphi(\overline{g}) + \varphi(\overline{h}),\end{aligned}$$

and similarly

$$\varphi(\overline{g}\,\overline{h}) = \varphi(\overline{g})\varphi(\overline{h}).$$

Finally $\varphi(1 + \langle f\rangle) = (1 + \langle f_1\rangle, \ldots, 1 + \langle f_k\rangle)$ is the unit of $R_1 \times \cdots \times R_k$ for the product. So φ is a ring homomorphism.

(b) If $\overline{g} = g+\langle f\rangle \in \ker(\varphi)$, then $(g+\langle f_1\rangle, \ldots, g+\langle f_k\rangle) = (0, \ldots, 0)$, so $f_1 \mid g, \ldots, f_k \mid g$. Since $f_1, \ldots, f_k$ are distinct monic irreducible polynomials, $f_1, \ldots, f_k$ are relatively prime, therefore $f = f_1 \cdots f_k \mid g$. This implies that $\overline{g} = g + \langle f\rangle = \langle f\rangle = \overline{0}$.

$\ker(\varphi) = \{\overline{0}\}$, so φ is injective.

(c) We know that

$$\dim R = \dim(\mathbb{F}_p[x]/\langle f\rangle) = \deg(f),$$

where $\dim R = \dim_{\mathbb{F}_p} R$ is the dimension of R over $\mathbb{F}_p$.

Similarly, since $f = f_1 \cdots f_k$,

$$\begin{aligned}\dim(R_1 \times \cdots \times R_k) &= \dim R_1 + \cdots + \dim R_k \\ &= \deg(f_1) + \cdots + \deg(f_k) \\ &= \deg(f).\end{aligned}$$

So

$$\dim R = \dim(R_1 \times \cdots \times R_k).$$

(d) Since φ is a ring homomorphism and $\varphi(\lambda\overline{g}) = \lambda\varphi(\overline{g}), \lambda \in \mathbb{F}_p, \overline{g} \in R$, φ is linear (φ is an algebra homomorphism).

$\varphi : R \to R_1 \times \cdots \times R_k$ is linear, injective, and $\dim R = \dim(R_1 \times \cdots \times R_k)$, therefore φ is bijective. So φ is a ring isomorphism.

□

Ex. 11.2.11 *In the situation of Theorem 11.2.9, let $T : R \to R$ be the pth-power map, where $R = \mathbb{F}_p[x]/\langle f\rangle$ and f is separable of degree n. The goal of this exercise is to prove that the rank of $T - 1_R$ is $n - k$, where k is the number of irreducible factors of f in $\mathbb{F}_p[x]$. We will use the isomorphism $\varphi : R \simeq R' = R_1 \times \cdots \times R_k$ constructed in Exercise 10.*

(a) Let $T' : R' \to R'$ be the map that is the pth power on each coordinate. Prove that φ induces an isomorphism between the kernel of $T - 1_R$ and the kernel of $T' - 1_{R'}$.

(b) Prove that the kernel of $T' - 1_{R'}$ has dimension k as a vector space over $\mathbb{F}_p$.

(c) Prove that $T - 1_R$ has rank $n - k$, and use this to give another proof of Theorem 11.2.9.

Proof. (a) Let

$$T' : \left\{ \begin{array}{ccc} R' & \to & R' \\ y = (g_1 + \langle f_1\rangle, \ldots, g_k + \langle f_k\rangle) & \mapsto & y^p = (g_1^p + \langle f_1\rangle, \ldots, g_k^p + \langle f_k\rangle) \end{array} \right.$$

We show first that

$$T' = \varphi \circ T \circ \varphi^{-1},$$

which means that the following diagram is commutative:

$$\begin{array}{ccc} R & \xrightarrow{T} & R \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\simeq} & & {\scriptstyle\varphi}\downarrow{\scriptstyle\simeq} \\ R' & \xrightarrow{T'} & R' \end{array}$$

Let $y = (g_1 + \langle f_1\rangle, \ldots, g_k + \langle f_k\rangle)$ be any element of R'. By Exercise 10, φ is bijective, so there exists a unique $x = g + \langle f\rangle \in R$ such that $\varphi(x) = y$. So there exists $g \in \mathbb{F}_p[x]$ such that $(g + \langle f_1\rangle, \ldots, g + \langle f_k\rangle) = (g_1 + \langle f_1\rangle, \ldots, g_k + \langle f_k\rangle)$. We have so proved the Chinese Remainder Theorem: there exists $g \in \mathbb{F}_p[x]$ such that

$$g \equiv g_1 \pmod{f_1}, \ldots, g \equiv g_k \pmod{f_k}.$$

This implies

$$g^p \equiv g_1^p \pmod{f_1}, \ldots, g^p \equiv g_k^p \pmod{f_k},$$

thus

$$\begin{aligned}(\varphi \circ T \circ \varphi^{-1})(y) &= (\varphi \circ T)(g + \langle f\rangle)\\ &= \varphi(g^p + \langle f\rangle)\\ &= (g^p + \langle f_1\rangle, \ldots, g^p + \langle f_k\rangle)\\ &= (g_1^p + \langle f_1\rangle, \ldots, g_k^p + \langle f_k\rangle)\\ &= T'(y).\end{aligned}$$

Therefore $T' = \varphi \circ T \circ \varphi^{-1}$.

Now we prove that, for all $\overline{g} = g + \langle f\rangle \in R$,

$$T(\overline{g}) = \overline{g} \iff T'(\varphi(\overline{g})) = \varphi(\overline{g}).$$

- If $T(\overline{g}) = \overline{g}$, then

$$T'(\varphi(\overline{g})) = (\varphi \circ T \circ \varphi^{-1})(\varphi(\overline{g})) = \varphi(T(\overline{g})) = \varphi(\overline{g}).$$

- If $T'(\varphi(\overline{g})) = \varphi(\overline{g})$, then $(\varphi \circ T \circ \varphi^{-1})(\varphi(\overline{g})) = \varphi(\overline{g})$, so $(\varphi \circ T)(\overline{g}) = \varphi(T(\overline{g})) = \varphi(\overline{g})$. Since φ is bijective, $T(\overline{g}) = \overline{g}$, and the equivalence is proved.

Thus, if $\overline{g} \in \ker(T - 1_R)$, then $T(\overline{g}) = \overline{g}$, $T'(\varphi(\overline{g})) = \varphi(\overline{g})$, $\varphi(\overline{g}) \in \ker(T' - 1_{R'})$. Conversely, if $y \in \ker(T' - 1_{R'})$, then $y = \varphi(g), g \in R$, so $T'(\varphi(\overline{g})) = \varphi(\overline{g})$, therefore $T(\overline{g}) = \overline{g}$, so $g \in \ker(T - 1_R)$. We have proved

$$\varphi(\ker(T - 1_R)) = \ker(T' - 1_{R'}),$$

so φ induces an isomorphism between the kernel of $T - 1_R$ and the kernel of $T' - 1_{R'}$.

(b) Let $y = (g_1 + \langle f_1\rangle, \ldots, g_k + \langle f_k\rangle)$. Then

$$y \in \ker(T' - 1_{R'}) \iff f_1 \mid g_1^p - g, \ldots, f_k \mid g_k^p - g_k.$$

Let $T_i : R_i \to R_i$ defined by $T_i(g_i + \langle f_i\rangle) = g_i^p + \langle f_i\rangle$, where $1 \le i \le k$. Then

$$\ker(T' - 1_{R'}) = \ker(T_1 - 1_{R_1}) \times \cdots \times \ker(T_k - 1_{R_k}).$$

Moreover

$$g_1 \in \ker(T_1 - 1_{R_1}) \iff f_1 \mid g_1^p - g_1.$$

The set of $\alpha \in R_1 = \mathbb{F}_p[x]/\langle f_1\rangle$ such that $\alpha^p - \alpha = 0$ is a subfield isomorphic to $\mathbb{F}_p$, the prime field $\{[0] + \langle f_1\rangle, \cdots, [p-1] + \langle f_1\rangle\}$, whose dimension is 1 as subspace of R_1:

$$\dim_{\mathbb{F}_p} \ker(T_1 - 1_{R_1}) = 1.$$

Similarly $\dim_{\mathbb{F}_p} \ker(T_i - 1_{R_i}) = 1$ for $i = 1, \ldots, k$. Therefore

$$\dim_{\mathbb{F}_p} \ker(T' - 1_{R'}) = k.$$

(c) By part (a), $\varphi(\ker(T-1_R)) = \ker(T'-1_{R'})$, where φ is a vector space isomorphism, thus

$$\dim(\ker(T-1_R)) = \dim\ker(T'-1_{R'}) = k.$$

Therefore, by the Rank Theorem, $T-1_R$ has rank $n-k$. In particular,

f is irreducible over $\mathbb{F}_p \iff k=1 \iff T-1_R$ has rank $n-1$.

This is another proof of Theorem 11.2.9.

□

Ex. 11.2.12 *Let $f \in \mathbb{F}_p[x]$ be monic and separable of degree $n>1$, and assume that $T-1_R$ has rank $\neq n-1$. By theorem 11.2.9, f is reducible. In this exercise, you will use the kernel of $T-1_R$ to produce a nontrivial factorization of f.*

(a) Show that the constant polynomials in $\mathbb{F}_p[x]$ give a one-dimensional subset of the kernel of $T-1_R$.

(b) Prove that there is a nonconstant polynomial h of degree $<n$ such that $f \mid h^p-h$. Parts (c),(d) and (e) will use h to produce a nontrivial factorization of f.

(c) Explain why $h^p-h = \prod_{a\in\mathbb{F}_p}(h-a)$.

(d) Use parts (b) and (c) to show that $f = \prod_{a\in\mathbb{F}_p}\gcd(f,h-a)$.

(e) Use $\deg(h)<n$ to show that $f \nmid \gcd(f,h-a)$. Conclude that the factorization of part (d) is nontrivial, i.e., $\gcd(f,h-a)$ is a nonconstant factor of f of degree $<n$ for at least two $a\in\mathbb{F}_p$.

The basic idea of Berlekamp's algorithm is that one can factor f into irreducibles by taking the gcd's of the nontrivial factors $\gcd(f,h-a)$ produced by part (e) as we vary h and a.

Proof. (a) Let $\alpha = [i]+\langle f\rangle$ be the coset of the constant polynomial $[i]\in\mathbb{F}_p$. Then $(T-1_R)(\alpha) = \alpha^p-\alpha = ([i]^p-[i])+\langle f\rangle = [0]+\langle f\rangle = \overline{0}$, so $\alpha\in\ker(T-1_R)$.

$$\mathrm{vect}_{\mathbb{F}_p}([1]+\langle f\rangle) = \{\alpha\in R \mid \exists [i]\in\mathbb{F}_p,\ \alpha = [i]+\langle f\rangle\}$$

is a one-dimensional subspace of the kernel of $T-1_R$, corresponding to the constant polynomials in $\mathbb{F}_p[x]$.

(b) By part (a), the rank of $T-1_R$ is not n, and by hypothesis this rank is not $n-1$, so the rank of $T-1_R$ is less than $n-1$, so the kernel of $T-1_R$ has dimension at least 2.

Therefore there exists a polynomial h, with $\deg(h)<n$, such that $\overline{h} = h+\langle f\rangle \in \ker(T-1_R)$ which is not in the one-dimensional subspace of part (a), thus h is not a constant polynomial. Since $h\in\ker(T-1_R)$, $h^p+\langle f\rangle = h+\langle f\rangle$, thus $f\mid h^p-h$.

Conclusion: there is a nonconstant polynomial h of degree $<n$ such that $f\mid h^p-h$.

(c) In $k[x]$, we know that

$$x^p-x = \prod_{a\in\mathbb{F}_p}(x-a).$$

The formal composition with $h(x)$ gives

$$h^p-h = \prod_{a\in\mathbb{F}_p}(h-a).$$

(d) We know that if $f_1, \ldots, f_s$ are polynomials in $\mathbb{F}_p[x]$ such that $\gcd(f_i, f_j) = 1$ if $i \neq j$, then

$$\gcd(f, f_1 \cdots f_s) = \gcd(f, f_1) \cdots \gcd(f, f_s).$$

Take $f_a = h - a \in \mathbb{F}_p[x]$. Then $a \neq b \Rightarrow \gcd(f_a, f_b) = 1$, since

$$\frac{1}{b-a}(h-a) - \frac{1}{b-a}(h-b) = 1.$$

Therefore, since $f \mid h^p - h$,

$$\begin{aligned} f &= \gcd(f, h^p - h) \\ &= \gcd(f, \prod_{a \in \mathbb{F}_p} (h - a)) \\ &= \prod_{a \in \mathbb{F}_p} \gcd(f, h - a) \end{aligned}$$

(e) Since $\deg(h) < n$, $\deg(h - a) < n$, therefore $\deg(\gcd(f, h - a)) < n$. Moreover, since $f \neq 0$, $\deg(\gcd(f, h - a)) \geq 0$, so f cannot divide $\gcd(f, h - a)$ when $a \in \mathbb{F}_p$.

Therefore the product $\prod_{a \in \mathbb{F}_p} \gcd(f, h - a)$ has more than one nonconstant factor (if all factors except one are constant, then $f \mid \gcd(f, h - a)$ for some $a \in \mathbb{F}_p$, which is impossible).

So $\gcd(f, h - a)$ is a nonconstant factor of f (and non associate to f) for at least two $a \in \mathbb{F}_p$.

□

Ex. 11.2.13 *Consider the polynomial $f = x^6 + x^4 + x + 1 \in \mathbb{F}_2[x]$.*

(a) Use Exercise 11 and the method of Example 11.2.10 to show that f is the product of three irreducible polynomials in $\mathbb{F}_2[x]$. Also find a basis of the kernel of $T - 1_R$.

(b) One element of the kernel is $(0, 0, 1, 1, 0, 1)$. This corresponds to $h = x^2 + x^3 + x^5$, since we are using the basis of R given by the cosets of $1, x, \ldots, x^5$. Show that $\gcd(f, h)$ and $gcd(h + 1)$ give a non trivial factorization $f = g_1 g_2$ as in Exercise 12.

(c) Pick an element h' of the kernel not in the span of 1 and h. Compute $\gcd(g_i, h')$ and $gcd(g_i, h' + 1)$ for $i = 1, 2$.

(d) Part (c) should show that f is a product of three nonconstant polynomials. Why is this the irreducible factorization of f?

Proof. (a) Since $f' = 1$, $\gcd(f, f') = 1$, so f is separable and we can use Berlekamp's algorithm directly. If we apply T to each element of the basis, then

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto x^2 \\ x^2 &\mapsto x^4 \\ x^3 &\mapsto 1 + x + x^4 \\ x^4 &\mapsto 1 + x + x^2 + x^3 + x^4 \\ x^5 &\mapsto 1 + x + x^2 + x^3 + x^5. \end{aligned}$$

It follows that the matrix A of T relative to the basis $1, x, x^2, x^4, x^4, x^5$ is

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$A - I = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

With Sage :

```
(A-1).rank()
```

we know that the rank of $A - I$ is $3 = 6 - 3$, so f is the product of 3 irreducible factors.

With Sage :

```
(A-1).right_kernel()
```

we obtain that the kernel of $A - I$ is the span of v_1, v_2, v_3, where

$$\begin{aligned} v_1 &= (1, 0, 0, 0, 0, 0) \\ v_2 &= (0, 0, 1, 1, 0, 1) \\ v_3 &= (0, 0, 0, 0, 1, 1), \end{aligned}$$

corresponding to the 3 polynomials

$$\begin{aligned} h_0 &= 1 \\ h &= x^2 + x^3 + x^5 \\ h' &= x^4 + x^5 \end{aligned}$$

By exercise 12 (e), $\gcd(f, h - a)$ is a non trivial factor for at least two a in $\mathbb{F}_2$. Since $\mathbb{F}_2$ has only two elements, $\gcd(f, h)$ and $\gcd(f, h - 1)$ are two non trivial factors of f, and

$$\begin{aligned} \gcd(f, h) &= \gcd(x^6 + x^4 + x + 1, x^2 + x^3 + x^5) = x^3 + x + 1 \\ \gcd(f, h + 1) &= \gcd(x^6 + x^4 + x + 1, 1 + x^2 + x^3 + x^5) = x^3 + 1 \end{aligned}$$

So we obtain two factors of degree 3, therefore

$$f(x) = x^6 + x^4 + x + 1 = (x^3 + x + 1)(x^3 + 1),$$

but the factors are not necessarily irreducible.

(c) The two polynomials

$$\gcd(f, h') = \gcd(x^6 + x^4 + x + 1, x^4 + x^5) = x + 1$$
$$\gcd(f, h' + 1) = \gcd(x^6 + x^4 + x + 1, 1 + x^4 + x^5) = x^5 + x^4 + 1$$

are also nontrivial factors of f.

(d) As $x + 1$ divides $x^3 + 1$, and $x^3 + 1 = (x + 1)(x^2 + x + 1)$, we obtain

$$f = x^6 + x^4 + x + 1 = (x^3 + x + 1)(x + 1)(x^2 + x + 1).$$

Since part (a) shows that f has 3 irreducible factors, the factors $x^3 + x + 1, x + 1, x^2 + x + 1$ are necessarily irreducible, and this is the irreducible factorisation of f.

□

Ex. 11.2.14 *In this exercise we will count the number of primitive elements of the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$. This is the number*

$$P_n = \big|\{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)\}\big|.$$

(a) Use Corollary 11.1.8 to prove that $p^n = \sum_{m|n} P_m$.

(b) Use the Möbius inversion formula to conclude that $P_n = \sum_{m|n} \mu(m) p^{\frac{n}{m}}$. This formula was first proved by Dedekind in 1857.

(c) Explain how the formula of part (b) relates to Theorem 11.2.4.

Proof. (a) Let $n \geq 1$ an integer. For every k such that $k \mid n$, there exists a unique subfield of $\mathbb{F}_{p^n}$ with cardinality p^k, written $\mathbb{F}_{p^k}$, and no such subfield if $k \nmid n$ (Corollary 11.1.8).

If $\alpha \in \mathbb{F}_{p^n}$, $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^n}$, so $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$ for some m, with $m \mid n$. Therefore

$$\mathbb{F}_{p^n} = \coprod_{m|n} \{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}\}.$$

As $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$ implies that $\alpha \in \mathbb{F}_{p^m}$,

$$\{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}\} = \{\alpha \in \mathbb{F}_{p^m} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}\},$$

therefore

$$\big|\{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}\}\big| = P_m.$$

Consequently,

$$p^n = \big|\mathbb{F}_{p^n}\big| = \sum_{m|n} \big|\{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}\}\big| = \sum_{m|n} P_m.$$

(b) If we write $G(n) = p^n$ and $F(n) = P_n$ as in the proof of Theorem 11.2.4, then

$$G(n) = \sum_{m|n} F(n).$$

By the Möbius inversion formula,

$$F(n) = \sum_{m|n} \mu(m) G\left(\frac{n}{m}\right),$$

so, for all positive integer n,

$$P_n = \sum_{m|n} \mu(m) p^{\frac{n}{m}}.$$

(c) Let α be a primitive element of $\mathbb{F}_{p^n}$, and f the minimal polynomial of α over $\mathbb{F}_p$. Then $\deg(f) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Since the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is normal, f splits completely in $\mathbb{F}_{p^n}$, so there exist exactly n primitive elements in $\mathbb{F}_{p^n}$ with the same minimal polynomial. Moreover two distinct monic irreducible polynomials have no common root.

If we write $A_n = \{\alpha \in \mathbb{F}_{p^n} \mid \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)\}$ the set of primitive elements of the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, and $\mathcal{N}_n$ the set of monic irreducible polynomials $f \in \mathbb{F}_p[x]$ of degree n, then by definition $|A_n| = P_n$ and $|\mathcal{N}_n| = N_n$. The map $\varphi : A_n \to \mathcal{N}_n$ defined by $\alpha \mapsto \mathrm{Irr}(\alpha, \mathbb{F}_p)$, where $\mathrm{Irr}(\alpha, \mathbb{F}_p)$ is the minimal polynomial of α over $\mathbb{F}_p$ is onto, and is such that every element of $\mathcal{N}_n$ has n preimages, with $\varphi^{-1}(f) \cap \varphi^{-1}(g) = \emptyset$ if $f, g \in \mathcal{N}_n, f \neq g$, thus $|A_n| = n|\mathcal{N}_n|$:

$$P_n = nN_n.$$

We find a new proof of the Theorem 11.2.4:

$$N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{\frac{n}{m}}.$$

Conversely, if we know Theorem 11.2.4, we find the formula of part (b): these two formulas are equivalent. □

Ex. 11.2.15 *This exercise will illustrate how the word "primitive" is sometimes overused in mathematics. In the previous problem, we computed the number of primitive elements of $\mathbb{F}_p \subset \mathbb{F}_{p^n}$. In this problem, we consider the primitive roots of $\mathbb{F}_{p^n}$, which are generators of the cyclic group $\mathbb{F}_{p^n}^*$. The minimal polynomial over $\mathbb{F}_p$ of a primitive root of $\mathbb{F}_{p^n}$ is called a primitive polynomial for $\mathbb{F}_{p^n}$. These are the minimal polynomials of the primitive $(p^n - 1)$st roots of unity in characteristic p.*

(a) Prove that $\mathbb{F}_{p^n}$ has $\phi(p^n - 1)$ primitive roots, where ϕ is the Euler ϕ-function.

(b) Prove that every primitive polynomial for $\mathbb{F}_{p^n}$ has degree n.

(c) Prove that the product of the primitive polynomials for $\mathbb{F}_{p^n}$ is $\Phi_{p^n-1}(x)$.

Proof. (a) Let γ a generator of the cyclic group $\mathbb{F}_{p^n}^*$, with cardinality $p^n - 1$. Then $\gamma^k, 0 \leq k < p^n - 1$, is a generator of the same group if and only if $k \wedge n = 1$, so $\mathbb{F}_{p^n}$ has $\phi(p^n - 1)$ primitive roots.

(b) Let α be a primitive root of $\mathbb{F}_{p^n}$. As $F_{p^n} = \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}$, then $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ (in other words, a primitive root of $\mathbb{F}_{p^n}$ is a primitive element of the extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$).

Let f be a primitive polynomial. By definition, f is the minimal polynomial of a primitive root α. Then

$$\deg(f) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Every primitive polynomial for $\mathbb{F}_{p^n}$ has degree n.

(c) By definition of the cyclotomic polynomials (and Proposition 11.2.6),

$$\Phi_{p^n-1}(x) = \prod_{o(\alpha)=p^n-1} (x-\alpha),$$

where we write $o(\alpha)$ the order of α in the group $\mathbb{F}_{p^n}^*$.

So the roots of $\Phi_{p^n-1}(x)$ are the primitive roots of $\mathbb{F}_{p^n}$.

Let f be a primitive polynomial for $\mathbb{F}_{p^n}$. By definition , f is the minimal polynomial of some primitive root α of $\mathbb{F}_{p^n}$. Since $\Phi_{p^n-1}(\alpha) = 0$, f divides $\Phi_{p^n-1}(x)$.

Conversely, let $f \in \mathbb{F}_p[x]$ be an irreducible factor of $\Phi_{p^n-1}(x)$. Let α be a root of $f(x)$ in some extension of $\mathbb{F}_{p^n}$. Since $f(x) \mid \Phi_{p^n-1}(x)$ and $\Phi_{p^n-1}(x) \mid x^{p^n-1} - 1$, then $\alpha^{p^n-1} = 1$, $\alpha^{p^n} = \alpha$, therefore $\alpha \in \mathbb{F}_{p^n}$. Moreover α is a root of $\Phi_{p^n-1}(x)$, so α is a primitive root of $\mathbb{F}_{p^n}$, thus f is a primitive polynomial for $\mathbb{F}_{p^n}$.

So the irreducible factors of $\Phi_{p^n-1}(x)$ in $\mathbb{F}_p[x]$ are all primitive polynomials for $\mathbb{F}_{p^n}$. Since $\Phi_{p^n-1}(x)$ is a separable polynomial, $\Phi_{p^n-1}(x)$ is squarefree, so $\Phi_{p^n-1}(x)$ is the product of its monic irreducible factors:

$$\text{the product of the primitive polynomials for } \mathbb{F}_{p^n} \text{ is } \Phi_{p^n-1}(x).$$

Note: this is consistent with Theorem 11.2.7. Indeed, $\Phi_{p^n-1}(x)$ is the product of irreducible polynomials in $\mathbb{F}_p[x]$ of degree m, where m is the minimum of the integers k such that $d = p^n - 1 \mid p^k - 1$, so $m = n$ (the order of p modulo $p^n - 1$ is n). Here we have proved that these factors are the primitive polynomials for $\mathbb{F}_{p^n}$. □

Ex. 11.2.16 *Consider the trinomial $f = x^r + x^s + 1 \in \mathbb{F}_2[x]$, where $r > s > 0$ and r is prime. Prove that f is irreducible over $\mathbb{F}_2$ if and only if $f \mid x^{2^r} - x$. If in addition r is large and f is primitive in the sense of Exercise 15, then we can use f to make a pseudo-random number generator that take a long time to repeat itself. For example, $x^{43112609} + x^{21078848} + 1$ is a primitive trinomial of large degree. See [3] (R.P.Brent and P. Zimmermann, The great trinomial hunt) for more details.*

Proof. • Suppose that f is irreducible over $\mathbb{F}_2$. Then $F = \mathbb{F}_2[x]/\langle f\rangle$ is a field with 2^r elements, so $F \simeq \mathbb{F}_{2^r}$. Then $\alpha = x + \langle f\rangle \in F$ is a root of f in F, and $F \simeq \mathbb{F}_{2^r}$, therefore $\alpha^{2^r} = \alpha$, so α is a root of $x^{2^r} - x$. Since f is the minimal polynomial of α over $\mathbb{F}_2$, $f \mid x^{2^r} - x$.

• Conversely, suppose that $f \mid x^{2^r} - x$.

Since $x^{2^r} - x$ is a separable polynomial over $\mathbb{F}_2$, f is also separable. Thus

$$f = f_1 f_2 \cdots f_k,$$

where $f_1, \ldots, f_k$ are monic irreducible polynomials such that $\gcd(f_i, f_j) = 1$ if $i \neq j$. We want to prove that $k = 1$. By Exercise 10 (Chinese Remainder Theorem),

$$\mathbb{F}_2[x]/\langle f\rangle \simeq \mathbb{F}_2[x]/\langle f_1\rangle \times \cdots \mathbb{F}_2[x]/\langle f_k\rangle.$$

Since $R_i = \mathbb{F}_2[x]/\langle f_i\rangle$ is a field with 2^{d_i} elements ($1 \leq i \leq k$), where $d_i = \deg(f_i)$, then $R_i \simeq \mathbb{F}_{2^{d_i}}$, and $d_1 + \cdots + d_k = \deg(f_1) + \cdots + \deg(f_k) = \deg(f) = r$. Thus

$$\mathbb{F}_2[x]/\langle f\rangle \simeq \mathbb{F}_{2^{d_1}} \times \cdots \times \mathbb{F}_{2^{d_k}}, \qquad d_1 + \cdots + d_k = r.$$

Let g_i a generator of $(\mathbb{F}_{2^{d_i}})^*$ for $i = 1, \ldots, k$. Then $g_i^{2^{d_i}-1} = 1$.

Write $\psi : \mathbb{F}_2[x]/\langle f\rangle \to \mathbb{F}_{2^{d_1}} \times \cdots \times \mathbb{F}_{2^{d_k}}$ the previously constructed ring isomorphism. There exists a coset $\beta \in \mathbb{F}_2[x]/\langle f\rangle$ such that $\psi(\beta) = (g_1, \ldots, g_k)$.

Let $\alpha = x + \langle f\rangle$ be the coset of x. Then $f(\alpha) = 0$, and since $f \mid x^{2^r} - x$, $\alpha^{2^r} = \alpha$.

Moreover, $\beta = h(\alpha)$, where $h \in \mathbb{F}_2[x], \deg(h) < r$. Since the characteristic is 2,

$$\beta^{2^r} = h(\alpha)^{2^r} = h(\alpha^{2^r}) = h(\alpha) = \beta.$$

By the isomorphism ψ, $\psi(\beta)^{2^r} = \psi(\beta)$, thus $(g_1, \ldots, g_k)^{2^r} = (g_1, \ldots, g_k)$, so $g_1^{2^r} = g_1, \ldots, g_k^{2^r} = g_k$, with $g_i \neq 0$ in the field R_i, so

$$g_1^{2^r-1} = 1, \ldots, g_k^{2^r-1} = 1.$$

Since the order of g_i is $2^{d_i} - 1$,

$$2^{d_1} - 1 \mid 2^r - 1, \ldots, 2^{d_k} - 1 \mid 2^r - 1.$$

Recall that $2^n - 1 \mid 2^m - 1$ implies $n \mid m$. Indeed, write $m = nq + s, 0 \leq s < n$. Then $2^m \equiv 1 \pmod{2^n - 1}$ (and $2^n \equiv 1 \pmod{2^n - 1}$), so $1 \equiv 2^m = (2^n)^q 2^s \equiv 2^s \pmod{2^n - 1}$, thus $2^n - 1 \mid 2^s - 1, 0 \leq s < n$, therefore $s = 0$, so $n \mid m$.

Consequently,

$$d_1 \mid r, \ldots, d_k \mid r.$$

But r is prime! So $d_i = 1$ or $d_i = r$ for all $i = 1, \ldots, k$.

Since $d_1 + \cdots + d_k = r$ with $d_i > 0$, if there is an index i such that $d_i = r$, then $k = 1$. In this case $f = f_1$ is irreducible.

It remains the case where $d_i = 1$ for all $i = 1, \ldots, k$. Then $f_i = x - a_i, a_i \in \mathbb{F}_2$, so

$$f = (x - a_1) \cdots (x - a_k), \quad a_i \in \mathbb{F}_2$$

splits completely over $\mathbb{F}_2$. But this is impossible, since $f = x^r + x^s + 1$ has no root in $\mathbb{F}_2$. Therefore f is irreducible over $\mathbb{F}_2$.

□

Ex. 11.2.17 *In section 4.2 we use the Schönemann-Eisenstein criterion to prove that $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$, where p is prime. Here is a very different proof. We know that primitive roots modulo p exist. By Dirichlet's theorem on primes in arithmetic progression, it follows that there is a prime l such that $[l] \in (\mathbb{Z}/p\mathbb{Z})^*$ has order $p - 1$. Prove that $\Phi_p(x)$ is irreducible modulo l and conclude that it is irreducible over $\mathbb{Q}$. This argument is due to Schönemann in 1845 (see [5]).*

Proof. Let $[g]$ a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. By Dirichlet's Theorem, since $\gcd(g, p) = 1$, there is some integer k such that $l = g + kp$ is prime, and $[l] = [g]$ has order $p - 1$.

Let $\overline{\Phi}_p(x)$ the reduction modulo l of Φ_p. By Theorem 11.2.7, $\overline{\Phi}_p(x)$ is the product of $\phi(p)/m = (p-1)/m$ irreducible polynomials in $\mathbb{F}_l[x]$ of degree m, where m is the order of $[l] \in (\mathbb{Z}/p\mathbb{Z})^*$, which is $p - 1$. So $m = p - 1$, and $\overline{\Phi}_p(x)$ is irreducible over $\mathbb{F}_l$.

Since Φ_p is monic, any decomposition $\Phi_p(x) = u(x)v(x)$ with $u, v \in \mathbb{Z}[x], \deg(u) < p - 1, \deg(v) < p - 1$ would give a decomposition $\overline{\Phi}_p(x) = \overline{u}(x)\overline{v}(x)$ in $\mathbb{F}_l[x]$, where $\deg(\overline{\Phi}_p(x)) = p - 1, \deg(\overline{u}(x)) < p - 1, \deg(\overline{v}(x)) < p - 1$. Since $\overline{\Phi}_p(x)$ is irreducible over $\mathbb{F}_l$, this is impossible, so $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. □