

§52 Finite Fields

We have seen some examples of finite fields, i.e., fields with finitely many elements. In this paragraph, we want to discuss some properties of finite fields.

In modern times, it is customary to treat finite fields after the presentation of Galois theory. Our approach to finite fields will be more elementary and more concrete than usual. We hope this will prepare the way to a better understanding of Galois theory. See also Example 54.18(c) and Theorem 54.26.

We begin by restricting the order of a finite field to prime powers.

52.1 Lemma: *Let q be a natural number and K a field with q elements. Then $q = p^n$ for some prime number p and for some natural number n .*

Proof: Let K be a field with q elements. The prime subfield of K cannot be (isomorphic to) \mathbb{Q} , for then K would contain infinitely many elements. Hence the prime subfield of K is (isomorphic to) \mathbb{F}_p for some prime number p . We consider K as an \mathbb{F}_p -vector space. The dimension of K over \mathbb{F}_p must be finite, say $|K:\mathbb{F}_p| = n \in \mathbb{N}$. Let $\{k_1, k_2, \dots, k_n\}$ be an \mathbb{F}_p -basis of K . Then K consists of the elements

$$a_1 k_1 + a_2 k_2 + \cdots + a_n k_n$$

as a_1, a_2, \dots, a_n run independently through \mathbb{F}_p , and

$$a_1 k_1 + a_2 k_2 + \cdots + a_n k_n \neq b_1 k_1 + b_2 k_2 + \cdots + b_n k_n$$

whenever $(a_1, a_2, \dots, a_n) \neq (b_1, b_2, \dots, b_n)$. Hence there are p possible choices for each of a_1, a_2, \dots, a_n and there are precisely $pp \dots p = p^n$ elements in K .

Thus the condition $q = p^n$ is a necessary condition for the existence of a field with q elements. One of our main goals in this paragraph is to show that it is also a sufficient condition.

By the proof of Lemma 52.1, we know that a field with p^n elements is of characteristic p . We prove two lemmas about (not necessarily finite) fields of prime characteristic.

52.2 Lemma: *Let K be a field of characteristic $p \neq 0$. Then*

$$(a + b)^p = a^p + b^p \quad \text{and} \quad (ab)^p = a^p b^p$$

for all $a, b \in K$.

Proof: We use the binomial theorem (Theorem 29.16). Here p is a prime number and the binomial coefficients $\binom{p}{k}$ are divisible by p when $k = 1, 2, \dots, p - 1$: note that $p!$ is divisible by p , so $k!(p - k)!\binom{p}{k}$ is divisible by p , but $k!(p - k)!$ is relatively prime to p , so p divides $\binom{p}{k}$ by Theorem 5.12. Then, for any $a, b \in K$, we have

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p = a^p + \sum_{k=1}^{p-1} 0 + b^p = a^p + b^p$$

since $p \mid \binom{p}{k}$ and $\text{char } K = p$ imply that $\binom{p}{k} a^{p-k} b^k = 0$ for $k = 1, 2, \dots, p - 1$. This proves $(a + b)^p = a^p + b^p$. The claim $(ab)^p = a^p b^p$ follows from Lemma 8.14(1). \square

Lemma 52.2 states that the mapping $\sigma: K \rightarrow K$ is a field homomorphism

$$a \rightarrow a^p$$

(clearly $1^p = 1 \neq 0$). By induction on m , we obtain

$$(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_2^p + \cdots + a_m^p$$

for any m elements a_1, a_2, \dots, a_m of a field of prime characteristic p .

52.3 Lemma: *Let K be a field of characteristic $p \neq 0$ and $n \in \mathbb{N}$. Then,*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

for any $a, b \in K$.

Proof: We make induction on n . The claim is established for $n = 1$ in Lemma 52.2. If the assertion is true for $n = k$, then, for any $a, b \in K$,

$$(a + b)^{p^{k+1}} = [(a + b)^{p^k}]^p = [a^{p^k} + b^{p^k}]^p = (a^{p^k})^p + (b^{p^k})^p = a^{p^{k+1}} + b^{p^{k+1}}$$

and it is true for $n = k + 1$ also. Hence it is true for all $n \in \mathbb{N}$. \square

52.4 Lemma: Let $q \in \mathbb{N}$ and let K be a field with q elements.

(1) $a^{q-1} = 1$ for all $a \in K^\times$.

(2) $a^q = a$ for all $a \in K$.

(3) $x^q - x = \prod_{a \in K} (x - a)$ in $K[x]$.

(4) Let $f(x)$ be a nonzero polynomial of degree d in $K[x]$. If $f(x) \mid (x^q - x)$ in $K[x]$, then $f(x)$ has exactly d roots in K , and these roots are pairwise distinct.

Proof: (1) K^\times is a multiplicative group of order $|K^\times| = |K \setminus \{0\}| = q - 1$. Hence $a^{q-1} = 1$ for any $a \in K^\times$.

(2) This follows from (1) if $a \neq 0$ and from $0^q = 0$ if $a = 0$.

(3) Any element a of K is a root of the polynomial $x^q - x \in K[x]$ by part

(2). Thus both $x^q - x$ and $\prod_{a \in K} (x - a)$ are monic polynomials, in $K[x]$, of degree q having all the q elements of K as roots. If $x^q - x$ were not equal

to $\prod_{a \in K} (x - a)$, then $(x^q - x) - \prod_{a \in K} (x - a)$ would be a nonzero polynomial of degree less than q having at least q distinct roots, contrary to

Theorem 35.7. So $x^q - x = \prod_{a \in K} (x - a)$

(4) We put $x^q - x = f(x)g(x)$, with $g(x) \in K[x]$. Then $\deg g(x) = q - d$. The roots of $x^q - x$ are pairwise distinct by part (3) and, since any root of $f(x)$ is also a root of $x^q - x$, we see that the roots of $f(x)$, too, are pairwise distinct. Likewise the roots of $g(x)$ are pairwise distinct. Now $g(x)$ has at most $q - d$ roots in K (Theorem 35.7). If $f(x)$ had r roots in K and $r < d$, then $x^q - x = f(x)g(x)$ would have at most $r + (q - d) < q$ roots in K , contrary to the fact that all q elements of K are roots of $x^q - x$. Thus $f(x)$ has at least d roots in K . But it can have at most d roots in K by Theorem 35.7. Hence $f(x)$ has exactly d roots in K . \square

52.5 Lemma: Let L/K be a field extension and assume that K has q elements, $q \in \mathbb{N}$. Let b be an element of L . Then $b \in K$ if and only if $b^q = b$.

Proof: $b \in K$ if and only if b is a root of $\prod_{a \in K} (x - a)$, so if and only if b is a root of $x^q - x$, so if and only if $b^q = b$. \square

The last two lemmas will now be employed to get information about the subfields of a finite field. If $K_1 \subseteq K_2$ are finite fields, with p^{m_1} and p^{m_2} elements, respectively, then K_1^\times is a subgroup of K_2^\times , hence $p^{m_1} - 1 = |K_1^\times|$ divides $|K_2^\times| = p^{m_2} - 1$ by Lagrange's theorem. We proceed to show that this happens if and only if m_1 divides m_2 .

52.6 Lemma: Let $m, n \in \mathbb{N}$ and put $d = (m, n)$.

(1) For any $k \in \mathbb{N}$, we have $(k^m - 1, k^n - 1) = k^d - 1$.

(2) If K is any field and x an indeterminate over K , then, in the unique factorization domain $K[x]$, we have $(x^m - 1, x^n - 1) \approx x^d - 1$.

Proof: (1) We put $e = (k^m - 1, k^n - 1)$. Since

$$k^m - 1 = (k^d - 1)((k^d)^{(m/d)-1} + (k^d)^{(m/d)-2} + \dots + k^d + 1),$$

we have $k^d - 1 | k^m - 1$. Likewise $k^d - 1 | k^n - 1$ and so $k^d - 1 | e$. On the other hand, $k^m \equiv 1 \pmod{e}$, so $\bar{k}^m = \bar{1}$ in \mathbb{Z}_e^\times , so $o(\bar{k}) | m$. Likewise $o(\bar{k}) | n$, so $o(\bar{k}) | d$, so $\bar{k}^d = \bar{1}$ in \mathbb{Z}_e^\times , so $k^d \equiv 1 \pmod{e}$, so $e | k^d - 1$. From $k^d - 1 | e$ and $e | k^d - 1$, we obtain $e = k^d - 1$, as claimed.

(2) We put $f(x) = (x^m - 1, x^n - 1)$. Since

$$x^m - 1 = (x^d - 1)((x^d)^{(m/d)-1} + (x^d)^{(m/d)-2} + \dots + x^d + 1),$$

we have $x^d - 1 | x^m - 1$ in $K[x]$. Likewise $x^d - 1 | x^n - 1$ and so $x^d - 1 | f(x)$. On the other hand, $f(x) | x^m - 1$, so $(x + (f))^m = x^m + (f) = 1 + (f)$ in $K[x]/(f(x))$, hence $x + (f)$ is a unit in $K[x]/(f)$ and the order of $x + (f) \in (K[x]/(f))^\times$ is divisible by m , likewise by n , and therefore by d . Thus $x^d + (f) = (x + (f))^d = 1 + (f)$, and $f(x) | x^d - 1$ in $K[x]$. From $x^d - 1 | f(x)$ and $f(x) | x^d - 1$, we get $f(x) \approx x^d - 1$, as claimed.

\square

52.7 Lemma: Let $m, n, p \in \mathbb{N}$ and let K be a field and x an indeterminate over K .

(1) For any $k \in \mathbb{N}$, we have $k^m - 1 | k^n - 1$ if and only if $m | n$.

(2) In the polynomial ring $K[x]$, we have $x^m - 1 | x^n - 1$ if and only if $m | n$.

(3) In the polynomial ring $K[x]$, we have $x^{p^m} - x | x^{p^n} - x$ if and only if $m | n$.

Proof: (1) $k^m - 1 | k^n - 1$ if and only if $(k^m - 1, k^n - 1) = k^m - 1$, so if and only if $k^{(m,n)} - 1 = k^m - 1$, so if and only if $(m, n) = m$, so if and only if $m | n$.

(2) $x^m - 1 | x^n - 1$ in $K[x]$ if and only if $(x^m - 1, x^n - 1) \approx x^m - 1$, so if and only if $x^{(m,n)} - 1 \approx x^m - 1$, so if and only if $x^{(m,n)} - 1 = x^m - 1$, so if and only if $(m, n) = m$, so if and only if $m | n$.

(3) We have $x^{p^m} - x | x^{p^n} - x$ if and only if $x^{p^{m-1}} - 1 | x^{p^{n-1}} - 1$, so if and only if $p^m - 1 | p^n - 1$ by part (2), so if and only if $m | n$ by part (1). \square

52.8 Theorem: Let K be a field with p^n elements (p prime). Then K has a subfield with p^m elements if and only if $m | n$. In this case, there is exactly one subfield of K with p^m elements. This subfield is

$$\{a \in K: a^{p^m} = a\}.$$

Proof: As noted earlier, if K has a subfield H with p^m elements, then H^\times is a subgroup of K^\times , so $p^m - 1 = |H^\times|$ divides $|K^\times| = p^n - 1$ by Lagrange's theorem. From $p^m - 1 | p^n - 1$, we get $m | n$ by Lemma 52.7(1).

Suppose now $m | n$. We want to show that K has a subfield with p^m elements. Lemma 52.5 leads us to consider the set of all elements a in K satisfying $a^{p^m} = a$. So we put $K_1 = \{a \in K: a^{p^m} = a\}$. Then K_1 is not empty and, for any $a, b \in K_1$, we have

$$(a + b)^{p^m} = a^{p^m} + a^{p^m} = a + b, \quad \text{so } a + b \in K_1 \quad (\text{Lemma 52.3}),$$

$$(-b)^{p^m} = (-1b)^{p^m} = (-1)^{p^m} b^{p^m} = (-1)b, \quad \text{so } -b \in K_1 \quad (\text{even when } p = 2),$$

$$(ab)^{p^m} = a^{p^m} b^{p^m} = ab, \quad \text{so } ab \in K_1,$$

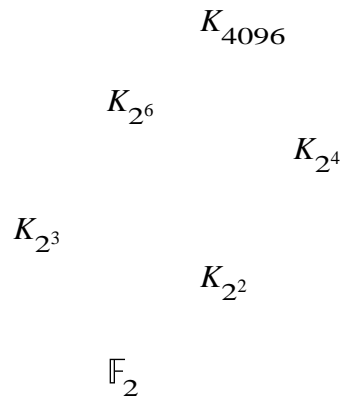
$$(1/b)^{p^m} = 1/b^{p^m} = 1/b, \quad \text{so } 1/b \in K_1 \quad (\text{if } b \neq 0).$$

Thus K_1 is a subfield of K . We now show that K_1 has exactly p^m elements. Since $m | n$, we have $x^{p^m} - x | x^{p^n} - x$ in $K[x]$ (Lemma 52.7(3)). Thus the

polynomial $x^{p^m} - x$ has exactly p^m roots (and these are pairwise distinct). (Lemma 52.4(4)) and the roots of $x^{p^m} - x$ are precisely the elements in K_1 . Hence K_1 has indeed p^m elements.

This proves that K has a subfield K_1 with p^m elements whenever $m|n$. Moreover, there is only one subfield with p^m elements, for if K_2 is a subfield of K and $|K_2| = p^m$, then any element b of K_2 satisfies $b^{p^m} = b$ by Lemma 52.5, so $K_2 \subseteq K_1$, so $K_2 = K_1$. The proof is complete. \square

As an illustration of Theorem 52.8, assume that K_{4096} is a field with $4096 = 2^{12}$ elements. Then all subfields of K_{4096} are as the figure below, where K_q denotes a field with q elements.



In particular, assuming the existence of a field with 4096 elements, we can conclude the existence of a field with $2^1, 2^2, 2^3, 2^4, 2^6$ elements, too. However, we do not know whether a field with 4096 elements really exists, so the foregoing argument is very weak. It is in fact true that there is a field with p^n elements, for any prime number p and for any natural number n . We wish to prove this assertion. We need some results from elementary number theory.

*
* *

In the following, we use the notation $\sum_{d|n} a_d$. This means that $n \in \mathbb{N}$ and that we take a sum of terms a_d as d ranges through the positive divisors

of n , including 1 and n . For instance $\sum_{d|12} a_d = a_1 + a_2 + a_3 + a_4 + a_6 + a_{12}$ and

$\sum_{d|15} a_d = a_1 + a_3 + a_5 + a_{15}$. We clearly have $\sum_{d|n} a_d = \sum_{d|n} a_{n/d}$. The notations $\prod_{d|n} a_d$ and $\bigcup_{d|n} S_d$ will have similar meanings.

52.9 Lemma: Let φ be Euler's function. Then, for any natural number n ,

$$\sum_{d|n} \varphi(d) = n.$$

Proof: For any $k \in \mathbb{N}$, $\varphi(k)$ is defined to be the number of positive integers less than (on equal to) k that are relatively prime to k . The greatest common divisor of any integer in $\{1, 2, \dots, n\}$ with n is a positive divisor d of n . Hence we have

$$\{1, 2, \dots, n\} = \bigcup_{d|n} S_d \quad \text{where } S_d = \{k \in \mathbb{N}: k \leq n \text{ and } (k, n) = d\}.$$

Counting the number of elements, we get $n = |\{1, 2, \dots, n\}| = \sum_{d|n} |S_d|$. Here

$$\begin{aligned} S_d &= \{k \in \mathbb{N}: k \leq n \text{ and } (k, n) = d\} \\ &= \{k \in \mathbb{N}: d|k, k \leq n \text{ and } (k, n) = d\}. \\ &= \{k \in \mathbb{N}: k = db \text{ for some } b \in \mathbb{N}, k \leq n \text{ and } (k, n) = d\} \\ &= \{db \in \mathbb{N}: db \leq n \text{ and } (db, n) = d\} \\ &= \{db \in \mathbb{N}: db \leq n \text{ and } (db, d \frac{n}{d}) = d\} \\ &= \{db \in \mathbb{N}: 1 \leq b \leq \frac{n}{d} \text{ and } (b, \frac{n}{d}) = 1\}. \end{aligned}$$

Thus $|S_d|$ is the number of positive integers b such that $1 \leq b \leq n/d$ and $(b, (n/d)) = 1$, and this number is $\varphi(n/d)$ by definition. We then obtain

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d). \quad \square$$

For ease in formulation of the next lemma, we introduce some terminology. Let $m \in \mathbb{N}$. A *complete residue system mod m* is defined to be a set

of m integers such that one and only one of them is congruent to each one of $1, 2, \dots, m$. Thus a complete residue system mod m is a set $\{r_1, r_2, \dots, r_m\} \subseteq \mathbb{Z}$ such that the residue classes mod m of r_1, r_2, \dots, r_m make up \mathbb{Z}_m . In particular, r_i are then mutually incongruent mod m (and, *a fortiori*, mutually distinct). If r_1, r_2, \dots, r_m are integers mutually incongruent mod m , then $\{r_1, r_2, \dots, r_m\}$ is a complete residue system mod m . Also, if any integer is congruent, modulo m , to one of the integers r_1, r_2, \dots, r_m , then $\{r_1, r_2, \dots, r_m\}$ is a complete residue system mod m .

A *reduced residue system mod m* is defined to be a set of $\varphi(m)$ integers such that one and only one of them is congruent to each one of the integers among $1, 2, \dots, m$ that are relatively prime to m . Thus a reduced residue system mod m is a set $\{a_1, a_2, \dots, a_{\varphi(m)}\} \subseteq \mathbb{Z}$ such that the residue classes mod m of $a_1, a_2, \dots, a_{\varphi(m)}$ make up \mathbb{Z}_m^\times . In particular, a_i are then mutually incongruent mod m (and, *a fortiori*, mutually distinct). If $a_1, a_2, \dots, a_{\varphi(m)}$ are integers relatively prime to m and mutually incongruent mod m , then $\{a_1, a_2, \dots, a_{\varphi(m)}\}$ is a reduced residue system mod m . Also, if any integer that is relatively prime to m is congruent, modulo m , to one of the integers $a_1, a_2, \dots, a_{\varphi(m)}$, then $\{a_1, a_2, \dots, a_{\varphi(m)}\}$ is a reduced residue system mod m .

52.10 Lemma: Let φ be Euler's function. Let $m, n \in \mathbb{N}$ and $(m, n) = 1$.

(1) If $\{r_1, r_2, \dots, r_m\} \subseteq \mathbb{Z}$ is a complete residue system mod m and if $\{s_1, s_2, \dots, s_n\} \subseteq \mathbb{Z}$ is a complete residue system mod n , then

$$\{ms_i + nr_j : i = 1, 2, \dots, m, j = 1, 2, \dots, n\} \subseteq \mathbb{Z}$$

is a complete residue system mod mn .

(2) If $\{a_1, a_2, \dots, a_{\varphi(m)}\} \subseteq \mathbb{Z}$ is a reduced residue system mod m and if $\{b_1, b_2, \dots, b_{\varphi(n)}\} \subseteq \mathbb{Z}$ is a reduced residue system mod n , then

$$\{ma_i + nb_j : i = 1, 2, \dots, \varphi(m), j = 1, 2, \dots, \varphi(n)\} \subseteq \mathbb{Z}$$

is a reduced residue system mod mn .

(3) $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof: (1) It will be sufficient to show that any two distinct of the mn numbers $ms_i + nr_j$ are incongruent modulo mn . Indeed, if

$$ms_i + nr_j \equiv ms_{i'} + nr_{j'} \pmod{mn},$$

then $ms_i + nr_j \equiv ms_{i'} + nr_{j'} \pmod{m}$ and $ms_i + nr_j \equiv ms_{i'} + nr_{j'} \pmod{n}$
 $nr_j \equiv nr_{j'} \pmod{m}$ and $ms_i \equiv ms_{i'} \pmod{n}$

$$\begin{aligned}
r_j &\equiv r_{j'} \pmod{m} \text{ and } s_i \equiv s_{i'} \pmod{n} \\
r_j &= r_{j'} \text{ and } s_i = s_{i'} \\
ms_i + nr_j &= ms_{i'} + nr_{j'}
\end{aligned}$$

(2) Let us take a complete residue system $\{r_1, r_2, \dots, r_m\} \pmod{m}$ such that $\{a_1, a_2, \dots, a_{\varphi(m)}\} \subseteq \{r_1, r_2, \dots, r_m\}$ and a complete residue system $\{s_1, s_2, \dots, s_n\} \pmod{n}$ such that $\{b_1, b_2, \dots, b_{\varphi(n)}\} \subseteq \{s_1, s_2, \dots, s_n\}$. We have $\{a_1, a_2, \dots, a_{\varphi(m)}\} = \{r_j : j = 1, 2, \dots, m, (r_j, m) = 1\}$ and $\{b_1, b_2, \dots, b_{\varphi(n)}\} = \{s_i : i = 1, 2, \dots, n, (s_i, n) = 1\}$. Now $\{ms_i + nr_j : j = 1, 2, \dots, m, i = 1, 2, \dots, n\}$ is a complete residue system mod mn . So it will be sufficient to show that $ms_i + nr_j$ is relatively prime to mn if and only if $(s_i, n) = 1$ and $(r_j, m) = 1$.

If $(s_i, n) > 1$, then (s_i, n) divides both $ms_i + nr_j$, and mn , so (s_i, n) divides $(ms_i + nr_j, mn)$ and $(ms_i + nr_j, mn) > 1$. Likewise $(r_j, m) > 1$ implies that $(ms_i + nr_j, mn) > 1$.

On the other hand, if $(s_i, n) = 1$ and $(r_j, m) = 1$, then $(ms_i + nr_j, mn) = 1$. For otherwise $(ms_i + nr_j, mn)$ would be divisible by a prime number p . Then we would have $p|mn$, so $p|m$ or $p|n$. Without loss of generality, assume $p|m$. Also $p|ms_i + nr_j$, so $p|nr_j$. Since $p|m$ and $(m, n) = 1$, we would get $(p, n) = 1$. Then $p|nr_j$ and $(p, n) = 1$ would give $p|r_j$ and p would divide (r_j, m) , contrary to $(r_j, m) = 1$. So $(s_i, n) = 1$ and $(r_j, m) = 1$ implies $(ms_i + nr_j, mn) = 1$.

(3) From part (2), we learn that a reduced residue system modulo mn has $\varphi(m)\varphi(n)$ elements. Hence $\varphi(mn) = \varphi(m)\varphi(n)$ whenever m and n are relatively prime. \square

It follows by induction on k that $\varphi(m_1 m_2 \dots m_k) = \varphi(m_1)\varphi(m_2)\dots\varphi(m_k)$ for all natural numbers m_1, m_2, \dots, m_k that are pairwise relatively prime. In particular, if $n \in \mathbb{N}$ and $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is the canonical decomposition of n into prime numbers, then $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\dots\varphi(p_k^{a_k})$.

Now it is easy to find $\varphi(p^a)$ in closed form if p is prime: among the p^a integers $1, 2, \dots, p^a$, exactly p^{a-1} of them, namely

$$p1, p2, \dots, pp^{a-1}$$

are not relatively prime to p , so exactly $p^a - p^{a-1}$ of them are relatively prime to p . This means $\varphi(p^a) = p^a - p^{a-1}$. We can also write $\varphi(p^a)$

$$= p^a \left(1 - \frac{1}{p}\right).$$

Therefore, if $n \in \mathbb{N}$, $n > 1$ and $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is the canonical decomposition of n into prime numbers, then

$$\begin{aligned} \varphi(n) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) \\ &= p_1^{a_1-1} p_2^{a_2-1} \dots p_k^{a_k-1} (p_1 - 1)(p_2 - 1) \dots (p_k - 1) \\ &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Expanding the last expression, we find

$$\begin{aligned} \varphi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \dots + \frac{n}{p_k}\right) &+ \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \dots + \frac{n}{p_{k-1} p_k}\right) + \dots + \\ &(-1)^k \left(\frac{n}{p_1 p_2 \dots p_k}\right). \end{aligned}$$

Thus $\varphi(n)$ is equal to a sum of terms of the form $\mp \frac{n}{d}$, where d is a product of distinct prime divisors of n , and the sign is $+$ or $-$ according as the number of prime divisors is even or odd. Thus we can write

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

where $\mu(d) = 0$ if d is divisible by the square of some prime number, and, if d is not divisible by the square of any prime number, $\mu(d) = 1$ or -1 according as the number of (distinct) prime divisors of d is even or odd. This leads us to the function named after A. F. Möbius (1790-1868).

52.11 Definition: The function $\mu: \mathbb{N} \rightarrow \mathbb{Z}$, where

$$\mu(1) = 1,$$

$$\mu(n) = (-1)^r \text{ if } n \text{ is the product of } r \text{ distinct prime numbers,}$$

$$\mu(n) = 0 \text{ otherwise, i.e., if } n \text{ is divisible by the square of a}$$

prime number,

is called the *Möbius function*.

For example, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$,

$$\mu(6) = 1, \quad \mu(7) = -1, \quad \mu(8) = 0, \quad \mu(9) = 0, \quad \mu(10) = 1.$$

The two formulas $n = \sum_{d|n} \varphi(d)$ and $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ are equivalent. This is a special case of a formula known as Möbius inversion formula that connects a divisor sum $\sum_{d|n} a_d$ with the a_d . To establish this formula, we need a lemma.

52.12 Lemma: *Let μ be the Möbius function and $n \in \mathbb{N}$. Then $\sum_{d|n} \mu(d)$ is equal to 1 in case $n = 1$ and to 0 in case $n > 1$.*

Proof: If $n = 1$, then $\sum_{d|n} \mu(d) = \sum_{d|1} \mu(d) = \mu(1) = 1$.

If $n > 1$ and $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is the canonical decomposition of n into prime numbers, then

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|p_1 p_2 \dots p_k} \mu(d) = \mu(1) + (\mu(p_1) + \mu(p_2) + \dots + \mu(p_k)) \\ &\quad + (\mu(p_1 p_2) + \mu(p_1 p_3) + \dots + \mu(p_{k-1} p_k)) \\ &\quad + (\mu(p_1 p_2 p_3) + \dots + \mu(p_{k-2} p_{k-1} p_k)) \\ &\quad + \dots \\ &\quad + \mu(p_1 p_2 \dots p_k) \\ &= 1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \binom{k}{3}(-1)^3 + \dots + \binom{k}{k}(-1)^k \\ &= (1 - 1)^k = 0. \end{aligned} \quad \square$$

52.13 Lemma (Möbius inversion formula): *Let K be a field and let $f: \mathbb{N} \rightarrow K$ be any function. Define the function F by declaring*

$$F(n) = \sum_{d|n} f(d).$$

for all $n \in \mathbb{N}$. Then $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$

for all $n \in \mathbb{N}$.

Proof: Let $n \in \mathbb{N}$. For any positive divisor d of n , we have

$$F\left(\frac{n}{d}\right) = \sum_{b|\frac{n}{d}} f(b),$$

$$\mu(d)F\left(\frac{n}{d}\right) = \sum_{b|\frac{n}{d}} \mu(d)f(b)$$

$$\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \sum_{b|\frac{n}{d}} \mu(d)f(b).$$

The last sum is over all ordered pairs (d,b) of positive divisors of n such that $db|n$. Hence it is also the sum over all ordered pairs (b,d) of positive divisors of n such that $bd|n$ and we get

$$\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{b|n} \sum_{d|\frac{n}{b}} \mu(d)f(b) = \sum_{b|n} f(b) \left(\sum_{d|\frac{n}{b}} \mu(d) \right) = f(n)$$

since $\sum_{d|\frac{n}{b}} \mu(d)$ is equal to 1 when $b = n$ and to 0 when b is a proper

divisor of n (Lemma 52.12).

□

52.14 Lemma: Let K be a field and let $f: \mathbb{N} \rightarrow K^\times$ be any function. Define the function $F: \mathbb{N} \rightarrow K^\times$ by declaring

$$F(n) = \prod_{d|n} f(d).$$

for all $n \in \mathbb{N}$. Then $f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} F(d)^{\mu(n/d)}$

for all $n \in \mathbb{N}$.

Proof: Let $n \in \mathbb{N}$. We have $F\left(\frac{n}{d}\right) = \prod_{b|\frac{n}{d}} f(b)$,

$$F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{b|\frac{n}{d}} f(b)^{\mu(d)}$$

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} \prod_{b|\frac{n}{d}} f(b)^{\mu(d)}$$

and so

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{b|n} \prod_{d|\frac{n}{b}} f(b)^{\mu(d)} = \prod_{b|n} \left(f(b)^{\sum_{d|(n/b)} \mu(d)} \right) = f(n) \quad \square$$

*

* *

We return to finite fields. We will prove that, for any prime number p and natural number n , there is a finite field with p^n elements and that any two finite fields with the same number of elements are isomorphic. We begin by discussing the decomposition of $x^{p^n} - x \in \mathbb{F}_p[x]$ into irreducible polynomials in the unique factorization domain $\mathbb{F}_p[x]$. It turns out that all irreducible factors of $x^{p^n} - x$ are distinct, and an irreducible polynomial in $\mathbb{F}_p[x]$ divides $x^{p^n} - x$ if and only if its degree divides n .

52.15 Theorem: *Let p be a positive prime number and let $F_d(x)$ be the product of all monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$ (if there is no monic irreducible polynomial of degree d in $\mathbb{F}_p[x]$, let $F_d(x)$ be the constant polynomial $1 \in \mathbb{F}_p[x]$). Then*

$$x^{p^n} - x = \prod_{d|n} F_d(x) \quad \text{in } \mathbb{F}_p[x].$$

Proof: All roots of $x^{p^n} - x$ are simple, because $x^{p^n} - x$ is relatively prime to its derivative -1 . So $x^{p^n} - x$ is not divisible by the square of any polynomial in $\mathbb{F}_p[x]$. In particular, $x^{p^n} - x$ is not divisible by the square of any of its irreducible factors in $\mathbb{F}_p[x]$.

Suppose $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial in $\mathbb{F}_p[x]$ and let $d = \deg f(x)$. We construct the field $\mathbb{F}_p(a)$ by adjoining a root a of $f(x)$ to \mathbb{F}_p . Now $f(x)$ is the minimal polynomial of a over \mathbb{F}_p , so $|\mathbb{F}_p(a) : \mathbb{F}_p| = \deg f(x) = d$ and $\mathbb{F}_p(a)$ is a field of p^d elements. Therefore $b^{p^d} = b$ for all $b \in \mathbb{F}_p(a)$

(Lemma 52.4(3)). We are to prove that $f(x)|x^{p^n} - x$ in $\mathbb{F}_p[x]$ if and only if $d|n$ in \mathbb{Z} .

Assume $d|n$. As $a \in \mathbb{F}_p(a)$, we have $a^{p^d} = a$, so a is a root of $x^{p^d} - x \in \mathbb{F}_p[x]$. But $f(x)$ is the minimal polynomial of a over \mathbb{F}_p , hence $f(x)|x^{p^d} - x$ in $\mathbb{F}_p[x]$. From $d|n$, it follows that $x^{p^d} - x | x^{p^n} - x$ (Lemma 52.7(3)), so $f(x)|x^{p^n} - x$.

Assume now $f(x)|x^{p^n} - x$. Then $f(x)g(x) = x^{p^n} - x$ for some $g(x) \in \mathbb{F}_p[x]$, and $f(a)g(a) = a^{p^n} - a = 0$. So a is a root of $x^{p^n} - x$. But then any element of $\mathbb{F}_p(a)$ is a root of $x^{p^n} - x$: if $b \in \mathbb{F}_p(a)$, say $b = f_0 + f_1a + f_2a^2 + \dots + f_{d-1}a^{d-1}$ with $f_0, f_1, f_2, \dots, f_{d-1} \in \mathbb{F}_p$, then we get

$$\begin{aligned} b^{p^n} &= (f_0 + f_1a + f_2a^2 + \dots + f_{d-1}a^{d-1})^{p^n} \\ &= f_0^{p^n} + f_1^{p^n}a^{p^n} + f_2^{p^n}(a^2)^{p^n} + \dots + (f_{d-1})^{p^n}(a^{d-1})^{p^n} \\ &= f_0 + f_1a + f_2a^2 + \dots + f_{d-1}a^{d-1} = b. \end{aligned}$$

Since the elements of $\mathbb{F}_p(a)$ coincide with the roots of $x^{p^d} - x$ (Lemma 52.4(3)), we see that any root of $x^{p^n} - x$ is also a root of $x^{p^d} - x$. Therefore $x^{p^d} - x$ divides $x^{p^n} - x$ and, by Lemma 52.7(3), d divides n . \square

52.16 Lemma: *Let p be a prime number and let N_d be the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$. Let $F_d(x)$ be the product of all the N_d monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$ (with the understanding $F_d(x) = 1$ in case $N_d = 0$; we prove presently that $N_d > 0$). For any $n \in \mathbb{N}$, we have*

$$(1) \quad p^n = \sum_{d|n} dN_d;$$

$$(2) \quad F_n(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(n/d)};$$

$$(3) \quad N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d;$$

$$(4) \quad N_n > 0.$$

Proof: (1) This follows from $x^{p^n} - x = \prod_{d|n} F_d(x)$ by equating the degrees of the polynomials on both sides.

(2) This follows from the same equation by Lemma 52.14 (with the function $F: \mathbb{N} \rightarrow \mathbb{F}_p(x)$ that maps $n \in \mathbb{N}$ to $F_n(x)$).

(3) This follows from part (1) by Möbius inversion formula (Lemma 52.13).

(4) $N_n \geq 0$ by its definition. Also, if $N_n = 0$, we get $\sum_{d|n} \mu\left(\frac{n}{d}\right)p^d = 0$ from

part (3) and, dividing both sides by the smallest p^d for which $\mu\left(\frac{n}{d}\right) \neq 0$,

say by p^{d_0} , we obtain an equation $-\mu\left(\frac{n}{d_0}\right) = \sum_{\substack{d|n \\ d \neq d_0}} \mu\left(\frac{n}{d}\right)p^{d-d_0}$, where the right

hand side is and the left hand side is not divisible by p , a contradiction. Hence $N_n > 0$. □

52.17 Theorem: *Let $n \in \mathbb{N}$ and let p be a prime number. Then there exists a finite field with p^n elements.*

Proof: By Lemma 52.16(4), there is an irreducible polynomial $f(x)$ of degree n in $\mathbb{F}_p[x]$. Let K be the field obtained by adjoining a root of $f(x)$ to \mathbb{F}_p . Then $|K:\mathbb{F}_p| = n$ and K is a field with p^n elements (Theorem 50.7). □

52.18 Theorem: *Let K be a field and let G be a finite subgroup of K^\times . Then G is cyclic. In particular, if K is a finite field, then K^\times is cyclic.*

Proof: Let $n = |G|$. The order of any element g in G is a divisor of n . Hence we have the disjoint union

$$G = \bigcup_{d|n} \{g \in G: o(g) = d\},$$

from which we obtain

$$n = |G| = \sum_{d|n} \psi(d),$$

where $\psi(d)$ is the number of elements in G of order d .

We claim that $\psi(d)$ is either 0 or $\phi(d)$. If there is no element in G of order d , then of course $\psi(d) = 0$. If there does exist an element g in G of order d , then all the d elements in the cyclic group $\langle g \rangle$ generated by g satisfy

$g^d = 1$. Hence they are roots of the polynomial $x^d - 1 \in K[x]$ and this polynomial has therefore at least d roots in K . On the other hand, it can have at most roots in K , thus it has exactly d roots in K , namely the elements in $\langle g \rangle$. Thus any element in G that has order d , which necessarily is a root of $x^d - 1$, is in the subgroup $\langle g \rangle$, and an element in $\langle g \rangle$ is of order d if and only if that element is a generator of $\langle g \rangle$. Thus the elements in G of order d coincide with the generators of $\langle g \rangle$. There are $\varphi(d)$ generators of $\langle g \rangle$, so there are $\varphi(d)$ elements in G of order d , i.e., $\psi(d) = \varphi(d)$, as claimed.

Since $\psi(d) \leq \varphi(d)$ for any positive divisor of n , we obtain $n = \sum_{d|n} \psi(d) \leq$

$\sum_{d|n} \varphi(d) = n$ and this gives $\psi(d) = \varphi(d)$ for all positive divisors d of n . In

particular, $\psi(n) = \varphi(n) > 0$: there is an element a in G of order n . Thus G is the cyclic group $\langle a \rangle$. \square

52.19 Theorem: *Let K be a field of p^n elements and let t be a generator of the cyclic group K^\times . Then*

(1) $K = \mathbb{F}_p(t)$.

(2) *The minimal polynomial of t over \mathbb{F}_p has degree n .*

(3) *If K_1 is any field of p^n elements, then the minimal polynomial t over \mathbb{F}_p has a root in K_1 .*

Proof: Since $0 \in \mathbb{F}_p(t)$ and since any nonzero element of K , being a power of t , is in $\mathbb{F}_p(t)$, we get $K \subseteq \mathbb{F}_p(t)$; thus $K = \mathbb{F}_p(t)$. This proves (1). Then the degree of the minimal polynomial of t over \mathbb{F}_p is equal to $|\mathbb{F}_p(t):\mathbb{F}_p| = |K:\mathbb{F}_p| = n$. This proves (2). Finally, since the degree of the minimal polynomial of t over \mathbb{F}_p is equal to n , hence a divisor of n , this polynomial is a divisor of $x^{p^n} - x$ (Theorem 52.15) and has n distinct roots in K_1 (Lemma 52.4(3)); in particular, there is a root of this polynomial in K_1 . This proves (3). \square

52.20 Theorem: *Any two finite fields with the same number of elements are isomorphic.*

Proof: Let K and K_1 be fields of p^n elements. Then K^\times is a cyclic group (Theorem 52.18). Let t be a generator of K^\times . Then $K = \mathbb{F}_p(t)$ by Theorem 52.19(1). Let $f(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of t over \mathbb{F}_p . Now $f(x)$ has a root c in K_1 (Theorem 52.19(3)). Let $\mathbb{F}_p(c) \subseteq K_1$ be the subfield of K_1 generated by c over \mathbb{F}_p . Then $n = \deg f(x) = |\mathbb{F}_p(c):\mathbb{F}_p| \leq |K_1:\mathbb{F}_p| = n$ yields $\mathbb{F}_p(c) = K_1$. We then get

$$K_1 = \mathbb{F}_p(c) \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p(t) = K$$

from Theorem 50.6. Hence $K_1 \cong K$. □

In view of this theorem, we identify all finite fields of the same number of elements. Thus there is a unique field of q elements ($q = p^n$), and this field will be henceforward denoted by \mathbb{F}_q :

Exercises

1. Find finite subgroups of \mathbb{C}^\times and show directly that they are cyclic.
2. Let E and K be finite fields, with $K \subseteq E$ and $|E:K| = 5$. Let $a \in K$. If there is no $b \in K$ such that $b^2 = a$, show that there is no $b \in E$ such that $b^2 = a$.
3. Let E and K be finite fields, with $K \subseteq E$ and let $|E:K| = n$. Let $a \in K$ be such that there is no $b \in K$ such that $b^2 = a$. Prove that, if n is odd, there is no $b \in E$ such that $b^2 = a$ and that, if n is even, there is a $b \in E$ such that $b^2 = a$.
4. Find all monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 2, 3 and 4. Verify Theorem 52.
5. Let p and q be distinct prime numbers. Find the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree q .
6. Let K be a field with p^n elements. Let $a \in K$ and put $f(x) = \prod_{k=0}^{n-1} (x - a^{p^k})$. Show that $f(x) \in \mathbb{F}_p[x]$. Conclude that $a + a^p + a^{p^2} + \cdots + a^{p^{n-1}} \in \mathbb{F}_p$. This sum $a + a^p + a^{p^2} + \cdots + a^{p^{n-1}}$ is called the *trace of a over \mathbb{F}_p* and is denoted by

$T_{K/\mathbb{F}_p}(a)$. Prove that $T_{K/\mathbb{F}_p}(a + b) = T_{K/\mathbb{F}_p}(a) + T_{K/\mathbb{F}_p}(b)$ and $T_{K/\mathbb{F}_p}(ca) = cT_{K/\mathbb{F}_p}(a)$ for all $a, b \in K$ and $c \in \mathbb{F}_p$ and show that there is an $a \in K$ with $T_{K/\mathbb{F}_p}(a) \neq 0$.

7. Keep the notation of Ex.6. Prove that $g(x) = x^p - x - a \in K[x]$ is either irreducible in $K[x]$ or is a product of p polynomials of degree one. Prove that the latter alternative holds if and only if $T_{K/\mathbb{F}_p}(a) = 0$.

8. Construct addition and multiplication tables for the finite fields $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9$ and \mathbb{F}_{16} .

9. Find a generator of the cyclic group K^\times when $K = \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{16}, \mathbb{F}_{27}$.

10. Prove that a root of $x^2 + 7x + 2 \in \mathbb{F}_{11}[x]$ is a generator of \mathbb{F}_{11}^\times .