3.E Finite Fields

In this section we study finite fields and their field extensions.

Let K be a finite field. Then the characteristic of K is a prime number p and $\mathbb{F}_p := \mathbb{Z}/\mathbb{Z}p$ is a prime field of K. Moreover, K is a finite dimensional vector space over $\mathbb{F}_p$ and therefore $K \cong \mathbb{F}_p^n$ (as $\mathbb{F}_p$-vector spaces) where $n = \mathrm{Dim}_{\mathbb{F}_p} K = [K : \mathbb{F}_p]$, in particular,

$\mathrm{Card}\, K = \mathrm{Card}\, \mathbb{F}_p^n = (\mathrm{Card}\, \mathbb{F}_p)^n = p^n$. Therefore: cardinality of a finite field is a power of a prime number.

Next we obtain some field theoretic information about K by investigating the group structure of the multiplicative group $K^* = K \setminus \{0\}$ of K.

3.E.1 Lemma Let $G \subseteq K^*$ be a finite subgroup of any field K. Then G is cyclic.

Proof Let $n = \mathrm{card}\, G$ and $m = \exp(G)$[1]. Then $m | n$ and $x^m = 1$ for every $x \in G$

---

[1] Exponent of a finite group:

Let G be a finite group. Then the $\mathrm{lcm}\{\mathrm{ord}\, g \mid g \in G\} \in \mathbb{N}$ is called the exponent of G and is denoted by $\exp(G)$. For example, $\exp(S_3) = 6$, $\exp(\mathbb{Z}_n) = n$. Therefore $G \subseteq$

Let G be a finite abelian group of exponent $m = \exp(G)$. Then there is an element $x \in G$ of order m.† Moreover, G is cyclic if and only if $\mathrm{Card}\, G = \exp(G)$.

† In particular, $\exp(G)$ divides $\mathrm{Card}\, G$.

$V(X^m-1)$ = the zero set of the polynomial X^m-1 in K and hence $n = \mathrm{Card}\, G \leq \mathrm{Card}\left(V(X^m-1)\right) \leq \deg(X^m-1) = m$. This proves that $\mathrm{Card}\, G = n = m = \exp(G)$ and hence G is cyclic (see the footnote 1).

3.E.2 Corollary Let K be a finite field. Then K^* is a cyclic group.

3.E.3 Remark It is interesting to note that the converse of 3.E.2 is also true, i.e. if the multiplicative group K^* of a field K is cyclic, then K is finite.
For this it is enough to check that the multiplicative groups $\mathbb{Q}^*$ and $k(X)^*$, where k is any field, are no cyclic. This follows from the fact that the integral domains $\mathbb{Z}$ and $k[X]$ are factorial and have infinite many prime elements.

3.E.4 Example Let $m \in \mathbb{N}^*$. An element of the multiplicative group $(\mathbb{Z}_m)^\times$ of units in $\mathbb{Z}_m$ is called a primitive root[2] modulo m if it generates the group $(\mathbb{Z}_m)^\times$.
Note the following very interesting theorem:
Theorem (Gauss) For $m \in \mathbb{N}^*$, the group $(\mathbb{Z}_m)^\times$ of units modulo m is cyclic if and only if $m \in \{1, 2, 4, p^r, 2p^r \mid r \in \mathbb{N}^*$ and p is a prime number$\}$.
There is no simple way to find a primitive root modulo p in terms of p. For example, 2 is a primitive root modulo 5,

---

[2] The term "root" is used since these elements are solutions of the pure equations X^n-1

but 2 is not a primitive root modulo 7. 3 is a primitive root modulo 7.

An easy consequence of 3.E.2 is the ~~primitive element~~ (theorem for finite field)

3.E.5 Corollary (primitive element theorem) Let k be a finite field and let $K|k$ be a finite field extension. Then K is a simple extension of k, i.e. $K = k(\alpha)$ for some $\alpha \in K$.

Proof The field K is finite, since $K|k$ is finite. The group K^* is cyclic by 3.E.2. Let $\alpha \in K^*$ be a generator of K^*. Then every non-zero element of K is a power of α, in particular, $K = k(\alpha)$.

Using group theoretic properties of finite groups, we ve the structure theorem of finite fields.

3.E.6 Theorem Let K be a finite field of characteristic p and $n := \mathrm{Dim}_{\mathbb{F}_p} K$, i.e. $|K| = p^n$. Then K is the splitting field of the separable polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. In particular, $K|\mathbb{F}_p$ is Galois. More-over, the Frobenius automorphism $\sigma : K \longrightarrow K$, $x \longmapsto x^p$, generates the Galois group $\mathrm{Gal}(K|\mathbb{F}_p)$. In particular, the field extension $K|\mathbb{F}_p$ is cyclic of degree $n = \mathrm{Dim}_{\mathbb{F}_p} K$.

Proof Since $|K| = p^n$, $|K^*| = p^n - 1$ and hence $x^{p^n-1} = 1$ for every $x \in K^*$. Therefore $x^{p^n} - x = 0$ for every $x \in K$, i.e. $K \subseteq V(X^{p^n} - X)$ = the zero set of the polynomial $X^{p^n} - X$ in K and hence $K = V(X^{p^n} - X)$, since $\mathrm{card}\,(V(X^{p^n} - X)) \leq \deg X^{p^n} - X = p^n$.

This proves that K is the splitting field of the polynomial $X^{p^n}-X$ over $\mathbb{F}_p$, in particular, K is normal over $\mathbb{F}_p$. Since the derivative $(X^{p^n}-X)' = p^n X^{p^n-1}-1 = -1$ has no zero in K, the polynomial $X^{p^n}-X$ has no repeated zeros and hence $X^{p^n}-X$ is separable over $\mathbb{F}_p$. Therefore the extension $K=\mathbb{F}_p(x)$ is separable and hence Galois over $\mathbb{F}_p$. Further, the map $\sigma: K \longrightarrow K$, $x \longmapsto x^p$ is surjective and hence bijective (since K is finite). Since $(x+y)^p = x^p+y^p$ for all $x,y\in K$ ($\operatorname{char} K = p$), σ is an automorphism of K over $\mathbb{F}_p$. Moreover, the order of $\sigma \in \operatorname{Gal}(K|\mathbb{F}_p) = n$, since $\sigma^n(x) = x^{p^n} = x$ for every $x\in K$ and $\sigma^r \neq \mathrm{id}_K$ for every $r<n$; otherwise $\sigma^r(x) = x^{p^r} = x$ for every $x \in K$, i.e. $K \subseteq V(X^{p^r}-X)$, in particular, $|K| \leq p^r < p^n$ a contradiction. Now, since $|\operatorname{Gal}(K|\mathbb{F}_p)| = [K:\mathbb{F}_p] = n = \operatorname{ord}\sigma$, it follows that $\operatorname{Gal}(K|\mathbb{F}_p)$ is cyclic and generated by σ.

3.E.7 Corollary Any two finite fields of the same cardinality are isomorphic.

Proof Let K and K' be finite fields with cardinality p^n, $n\in\mathbb{N}^*$, p is a prime number. Then $\operatorname{char} K = \operatorname{char} K' = p$ and both $K|\mathbb{F}_p$ and $K'|\mathbb{F}_p$ are splitting fields of $X^{p^n}-X$ over $\mathbb{F}_p$. Therefore K and K' are isomorphic over $\mathbb{F}_p$. (Direct proof: $K=\mathbb{F}_p(x)$ for some $x\in K$ by 3.E.5. Let $\mu_x \in \mathbb{F}_p[X]$ be the minimal polynomial of x over $\mathbb{F}_p$. Then μ_x divides $X^{p^n}-X$ in $\mathbb{F}_p[X]$ and hence there exist $y\in K'$ which is a zero of μ_x (since $X^{p^n}-X$ factors into linear factors over K'). Then the kernel of the $\mathbb{F}_p$-algebra homomorphism $\mathbb{F}_p[X] \longrightarrow K'$ defined by $X \longmapsto y$ contains

μ_x, since $\mu_x(y)=0$ and hence equal to $\mathbb{F}_p[X]/\mu_x$, since μ_x is irreducible in $\mathbb{F}_p[X]$ and hence generate a maximal ideal in $\mathbb{F}_p[X]$. Therefore we have an injective $\mathbb{F}_p$-algebra homomorphism

$$K=\mathbb{F}_p(x) = \mathbb{F}_p[X] \big/ \mathbb{F}_p[X]\mu_x \xrightarrow{\varphi} K'$$

Now, since $|K|=|K'|$, φ is an isomorphism.

3.E.8 Corollary Let $K|k$ be a finite extension of finite fields. Then $K|k$ is Galois and the Galois group $\mathrm{Gal}(K|k)$ is cyclic. Moreover, if $\mathrm{Char}\, k = p$ and $|k|=p^n$, then $\mathrm{Gal}(K|k)$ is generated by the automorphism $\tau: K \longrightarrow K$, $x \longmapsto x^{p^n}$.

Proof Suppose that $\mathrm{Dim}_{\mathbb{F}_p} K = m$. Then $\mathrm{Gal}(K|\mathbb{F}_p)$ is a cyclic group of order m generated by the Frobenius automorphism $\sigma: K \longrightarrow K$, $x \longmapsto x^p$, in particular, the order of σ is m. Since $\mathrm{Gal}(K|k)$ is a subgroup of the group $\mathrm{Gal}(K|\mathbb{F}_p)$, it is cyclic of order r, where $m=[K:\mathbb{F}_p] = n\cdot r$; moreover, $\sigma^n: K \longrightarrow K$, $x \longmapsto x^{p^n}$ is a generator of $\mathrm{Gal}(K|k)$, since $|k|=p^n$. This proves that $r=[K:k]=\mathrm{Gal}(K|k)$ and hence $K|k$ is Galois.

We now show that for each $n\in\mathbb{N}^*$ there is a unique (upto isomorphism) finite field of cardinality p^n.

3.E.9 Theorem For each $n\in\mathbb{N}^*$, there is a unique subfield of $\overline{\mathbb{F}_p}$ (= algebraic closure of $\mathbb{F}_p$) of cardinality p^n. If K and L are subfields of $\overline{\mathbb{F}_p}$ of cardinalities p^m and p^n respectively, then $K \subseteq L$ if and only if m divides n.

Moreover, in this case L is Galois over K and the Galios group $\mathrm{Gal}(L|K)$ is generated by $\tau = \sigma^m$, when $\sigma : L \longrightarrow L$, $x \longmapsto x^p$ is the Frobenius automorphism of L.

Proof Let $n \in \mathbb{N}^*$ and $K := V_{\overline{\mathbb{F}}_p}(X^{p^n} - X)$ = the set of all zeros of the polynomial $X^{p^n} - X$ in $\overline{\mathbb{F}}_p$. Note that $X^{p^n} - X$ has p^n distinct zeros in $\overline{\mathbb{F}}_p$, since its derivative $pX^{p^n-1} - 1 = -1$ has no zero. Further, $K = \mathrm{Fix}(\sigma^n)$ is the set of all fixed points $\{x \in \overline{\mathbb{F}}_p \mid \sigma^n(x) = x\}$, where $\sigma : \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$, $x \longmapsto x^p$ is the Frobenius automorphism of $\overline{\mathbb{F}}_p$ (σ is surjective, since $\overline{\mathbb{F}}_p$ is algebraically closed). Therefore K is a unique subfield of $\overline{\mathbb{F}}_p$ of cardinality p^n.

Let K and L be subfields of $\overline{\mathbb{F}}_p$ of cardinalities p^m and p^n, respectively. First, suppose that $K \subseteq L$. Then $|L| = |K|^d$, where $d = \mathrm{Dim}_K L$ (L is a d-dimensional K-vector space) and hence $p^n = p^{md}$. Therefore $n = md$, i.e. m divides n. Conversely, suppose that $m | n$, i.e. $n = md$ for some $d \in \mathbb{N}$. Then $p^n = p^{md} = (p^m)^d$

$$K = V_{\overline{\mathbb{F}}_p}(X^{p^n} - X) \subseteq V_{\overline{\mathbb{F}}_p}(X^{p^m} - X) = L.$$

Now, by 3.E.8 $L|K$ is a Galois extension and the Galois group $\mathrm{Gal}(L|K)$ is generated by the automorphism $\tau : L \longrightarrow L$, $x \longmapsto x^{p^n}$

Theorems 3.E.6 and 3.E.9 can be used to determine the splitting field of a polynomial $f \in k[X]$ over a finite field k.

3.E.10 Corollary Let k be a finite field and let $f \in k[X]$ be a monic irreducible polynomial over k of degree n

Then:

(1) Let $\alpha \in \overline{k}$ be a zero of f in the algebraic closure $\overline{k}$ of k. Then $k(\alpha)$ is a splitting field of f over k, i.e. the polynomial f splits into linear factors over $k(\alpha)$. In particular, if K is a splitting field of f over k, then $[K : k] = n =$ degree of f.

(2) If $|k| = q$, then $V_{\overline{k}}(f) = \{\alpha^{q^r} \mid r \in \mathbb{N}^*\}$.

Proof Let K be a splitting field of f over k. Then $\alpha \in K$ and $k(\alpha) \cong k[X]/(f)$ (since f is irreducible over k) is a field extension of degree $[k(\alpha) : k] =$ degree of $f = n$. Therefore by 3.E.8 $k(\alpha)|k$ is a Galois extension, in particular, $f = \mu_{\alpha,k}$ splits over k and hence $K = k(\alpha)$ is a splitting field of f over k. This proves (1). For a proof of (2), note that (by 3.E.8) the Galois group $\mathrm{Gal}(k(\alpha)|k)$ is generated by the k-automorphism $\tau : k(\alpha) \longrightarrow k(\alpha)$, $x \longmapsto x^q$. Therefore each zero of f is then of the form $\tau^r(\alpha) = \alpha^{q^r}$ for some $r \in \mathbb{N}^*$ (see   ) and hence $V_{\overline{k}}(f) = \{\alpha^{q^r} \mid r \in \mathbb{N}^*\}$.

3.E.11 Examples

(1) Let $f = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ and let $\alpha \in \overline{\mathbb{F}_2}$ be a zero of f. Note that f has no zero in $\mathbb{F}_2$ and hence f is irreducible over $\mathbb{F}_2$. Therefore $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Further, the field $k(\alpha)$ is the splitting field of f over $\mathbb{F}_2$ and the zeros of f are $\alpha, \alpha^2, \alpha^4$ by 3.E.10. Since $f(\alpha) = 0$, $\alpha^3 = \alpha^2 + 1$ and so $\alpha^4 = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$. Therefore in terms of the basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{F}_2(\alpha)|\mathbb{F}_2$, the zeros of f are α, α^2 and $1 + \alpha + \alpha^2$; this shows explicitly that $\mathbb{F}_2(\alpha)$ is the splitting field of f over $\mathbb{F}_2$.

(2) Let $f = X^4 + X + 1 \in \mathbb{F}_2[X]$. Then $f' = 1$ and hence f has no multiple zeros. Further, f has no zeros in $\mathbb{F}_2$ and f is not divisible by the unique irreducible quadratic $X^2+X+1 \in \mathbb{F}_2[X]$. Therefore f is irreducible over $\mathbb{F}_2$. If $\alpha \in \overline{\mathbb{F}_2}$ is a zero of f, then $\alpha^4 = \alpha+1$, and hence by 3.E.10, the zeros of f are $\alpha, \alpha+1, \alpha^2$ and α^2+1.

(3) Let p be an odd prime and let $f = X^2+1 \in \mathbb{F}_p[X]$. Then f is reducible over $\mathbb{F}_p \iff p \equiv 1 \pmod 4$. For, if $\alpha \in \mathbb{F}_p$ is a zero of f, then $\alpha^2 = -1$ and so the order of α in $(\mathbb{F}_p)^*$ is 4. Therefore by Lagrange's theorem $4 \mid |\mathbb{F}_p^*|$ $p-1$, i.e. $p \equiv 1 \pmod 4$. Conversely, if $4 \mid p-1$, then there is an element $\alpha \in \mathbb{F}_p^*$ of order 4, since $\mathbb{F}_p^*$ is a cyclic group of order $p-1$. Then $\alpha^4 = 1$ and $\alpha^2 \neq 1$. This forces $\alpha^2 = -1$ and so α is a zero of f.

3.E.12 Corollary Every finite field is perfect i.e. every algebraic extension of a finite field is separable.

Proof Let k be a finite field and let $\alpha \in \overline{k}$. Then $k(\alpha)|k$ is a finite extension of k and hence Galois by 3.E.8, in particular, $k(\alpha)$ is separable over k, i.e. α is separable over k.

To construct a finite field of cardinality p^n for a given $n \in \mathbb{N}^*$, we use irreducible polynomials over $\mathbb{F}_p$.
Note that if $f \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree n, then $\mathbb{F}_p[X]/(f)$ is a field extension of degree $=$ degree of $f = n$ over $\mathbb{F}_p$ and hence it has p^n elements.

Conversely, if K has p^n elements and if $K = \mathbb{F}_p(\alpha)$, then $\mu_{\alpha,\mathbb{F}_p}$ is irreducible polynomial of degree $[K:\mathbb{F}_p]=n$. Therefore finding finite fields is equivalent to finding irreducible polynomials in $\mathbb{F}_p[X]$. For example, $\mathbb{F}_2[X]/(X^2+X+1)$ is a field with 4 elements, $\mathbb{F}_5[X]/(X^4-7)$ is a field with $5^4=625$ elements.

The following proposition give a way for searching irreducible polynomials over $\mathbb{F}_p$.

3.E.13 Proposition Let $n \in \mathbb{N}^*$. Then $X^{p^n}-X$ factors over $\mathbb{F}_p$ into the product of all monic irreducible polymials over $\mathbb{F}_p$ of degree a divisor of n.

Proof Let K be a field of cardinality p^n. Then by 3.E.6 K is a splitting field of $X^{p^n}-X$ over $\mathbb{F}_p$, infact, $K = V_{\overline{\mathbb{F}_p}}(X^{p^n}-X)$. Let $\alpha \in K$ and $m := [\mathbb{F}_p(\alpha):\mathbb{F}_p]$. Then m divides $[K:\mathbb{F}_p]=n$ and $\mu_{\alpha,\mathbb{F}_p}$ divides $X^{p^n}-X$, since α is a zero of $X^{p^n}-X$. Conversely, if $m|n$ and $f \in \mathbb{F}_p[X]$ is a monic irreducible polynomial of degree m. Let k be the splitting field of f over $\mathbb{F}_p$ in the algebraic closure of $\overline{K}$. Let $\alpha \in \overline{K}$ be a zero of f. Then $k = \mathbb{F}_p(\alpha)$ by 3.E.10. Therefore $[k:\mathbb{F}_p]=m$ and so $k \subseteq K$ by 3.E.9, since $m|n$, in particular, $\alpha \in K$ and hence α is a zero of $X^{p^n}-X$. Now, since f is irreducible over $\mathbb{F}_p$, $f = \mu_{\alpha,\mathbb{F}_p}$ and hence f divides $X^{p^n}-X$ in $\mathbb{F}_p[X]$. Note that, since $X^{p^n}-X$ has no repeated zeros, it factors into distinct irreducible factors over $\mathbb{F}_p$. Therefore we have shown that the irreducible factors of $X^{p^n} - X$ are exactly the irreducible polynomials of degree a divisor of n.

3.E.13 Example The monic irreducible polynomials of degree 5 over $\mathbb{F}_2$ are determined by factoring

$$X^{2^5} - X = X(X+1)(X^5+X^3+1)(X^5+X^2+1) \cdot (X^5+X^4+X^3+X+1)(X^5+X^4+X^2+X+1) (X^5+X^4+X^3+X^2+X+1)(X^5+X^3+X^2+X+1).$$

This factorisation has 6 monic irreducible polynomia of degree 5 over $\mathbb{F}_2$. Similarly, the monic irreducible polynomials of degree 2, 3 or 6 over $\mathbb{F}_2$ can be found by factoring $X^{2^6} - X$ over $\mathbb{F}_2$. For example, X^6+X+1 is an irreducible factor of $X^{64}-X$. Therefore $\mathbb{F}_2[X]/(X^6+X+6)$ is a field with 64 elements.

3.E.14 Theorem (Normal basis theorem) Let $K|k$ be a finite extension of finite fields. Then there exists $x \in K$ such that $\{\varphi(x) \mid \varphi \in \mathrm{Gal}(K|k)\}$ is a k-basis of the k-vector space K.

Proof By 3.E.8 $K|k$ is Galois and the Galois group $\mathrm{Gal}(K|k)$ is cyclic of order $n = [K:k]$ and is generated by σ the Frobenius automorphism $\sigma : K \longrightarrow K$, $x \longmapsto x^q$, where $q = |k|$. Note that the minimal polynomial μ_σ of σ is of degree n and hence $\mu_\sigma = \chi_\sigma$ = the characteristic polynomial of σ ($\deg \chi_\sigma = \mathrm{Dim}_k K = n = \deg \mu_\alpha$). Therefore $\exists\, x \in K$ such that $\{x, \sigma(x), \ldots, \sigma^{n-1}(x)\}$ is a k-basis of the k-vector space K (by linear algebra[1])

[1] Let $f : V \longrightarrow V$ be a linear operator on a finite dimensional vector space over a field k. Then f is a cyclic operator i.e. there exist $x \in$ such that $\{x, f(x), \ldots, f^{n-1}(x)\}$ is a k-basis of V $\Longleftrightarrow$ $\chi_f = \mu_f$.

Exercises

1. Let K be a finite field of characteristic p. Describe the structure of the additive group $(K,+)$ of K.

2. (Fermat) If p is a prime number, then $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$.

3. Let K be a finite field of characteristic p. Show tha every element of K has a unique p-th root in K.

4. Let K be a finite field of characteristic p and let $|K| = q$. Then
   (a) Let $n \in \mathbb{N}^*$ be such that $p \nmid n$ and L be the splitting field of $X^n - 1$ over K. Then show that $[L:K]$ is the least integer such that $n \mid (p^r - 1)$.

   (b) Let $f \in K[X]$ be an irreducible polynomial over K. Then show that f divides $X^{p^n} - X$ in $K[X]$ if and only if $\deg f$ divides n.

5. For $n \in \mathbb{N}$, $n \geq 3$, show that $X^{2^n} + X + 1$ is reducibl over $\mathbb{F}_2$.

6. Every element in a finite field can be written as the sum of squares.

7. Let K be a finite field with q elements and let $L|K$ be a finite field extension. Further, let $\alpha \in L$

be a non-zero element of order d in L^*. Show that $[K(x):K] = \deg \mu_{x,K}$ = the order of the residue class $\overline{q}$ in the multiplicative group $(\mathbb{Z}/\mathbb{Z}d)^\times$.

8. Let K be a finite field with q elements and let $L|K$ be a finite field extension. Let $x \in L$ and $s = \deg \mu_{x,K} = [K(x):K]$. Show that s is the smallest positive natural number with $x = x^{q^s}$ and $\mu_{x,K} = \prod_{i=0}^{s-1} (X - x^{q^i})$ is the minimal polynomial over K. (<u>Hint</u>: The coefficients of the polynomial $g := \prod_{i=0}^{s-1} (X - x^{q^i})$ are invariant under a generator of the Galois group $\mathrm{Gal}(K(x)|K)$.)

9. Let K be a finite field with q elements. Show that there are exactly $q(q-1)/2$ monic quadratic polynomials in $K[X]$ which are irreducible.

10. Let K be a finite field with q elements. For $s \in \mathbb{N}^*$, let $r_q(s)$ denote the number of monic irreducible polynomials of degree s in $K[X]$. Show that

$$r_q(s) = \frac{1}{s} \sum_{d|s} \mu\left(\frac{s}{d}\right) q^d ,$$

where μ is the Möbius-function (<u>Hint</u>: Let $L|K$ be a field extension of degree s. If $d|s$ and if $f \in K[X]$ is irreducible of degree d, then f has exactly d zeros in L. Therefore $q^s = \sum_{d|s} d \cdot r_q(d)$. Now, apply the Möbius-inversion formula.)