Appendix A

Finite Fields

As a corollary of the Euclidean algorithm we saw that the integers modulo a prime number p form a field, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. (For a simple direct proof observe that multiplying by a nonzero element is injective.) The fields $\mathbb{F}_p$ play an important role in the theory of finite fields.

The purpose of this appendix is to determine all finite fields.

A.1 Prime Fields

For an arbitrary ring R (with 1) and an integer n the product $n \cdot 1 \in R$ has a natural definition as sum $1 + \cdots + 1$ of n exemplars of 1, if $n > 0$, as 0, if $n = 0$, and as $-|n| \cdot 1$, if $n < 0$. This makes R an algebra over $\mathbb{Z}$ and defines a canonical ring homomorphism

$$\alpha \colon \mathbb{Z} \longrightarrow R, \ \ \alpha(n) = n \cdot 1.$$

The kernel of α is an ideal $m\mathbb{Z}$ with $m \geq 0$. If $m = rs$, then $\alpha(r)\alpha(s) = 0$ in R. Thus if R is an integral domain (say a field), then $m = p$ is a prime number or 0, and is called the **characteristic** of R. If K is a finite field, then $p > 0$ (else α would be injective), and the Homomorphy Theorem yields a natural embedding $\mathbb{F}_p \hookrightarrow K$. Usually one identifies the field $\mathbb{F}_p$ with its image in K and calls it the **prime field** of K.

Remarks

1. If K is a field of characteristic $p > 0$, then $pa = 0$ for all $a \in K$, since $pa = (p \cdot 1) \cdot a = 0 \cdot a$.

2. With the same assumptions $(a + b)^p = a^p + b^p$ for all $a, b \in K$. For by the Binomial Theorem

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

Since p divides all binomial coefficients $\binom{p}{i}$ for $0 < i < p$ the sum is 0. In particular the map $a \mapsto a^p$ is a ring homomorphism of K into itself with kernel 0, hence injective. If K is finite, it is an automorphism.

Now let K be a finite field of characteristic p with $q = \#K$ elements. Then K is a finite dimensional vector space over $\mathbb{F}_p$. If $e = \dim K$, then K as a vector space is isomorphic with $\mathbb{F}_p^e$. Hence $q = p^e$.

We have proved:

Theorem 4 *Let K be a finite field, and q the number of its elements. Then there is a prime number p and an exponent e such that $q = p^e$. Furthermore K has characteristic p and contains the prime field $\mathbb{F}_p$ (up to isomorphism).*

A.2 The Multiplicative Group of a Finite Field

This is a standard result of Algebra:

Proposition 9 *Let K be a field, and $G \leq K^\times$ a finite subgroup with $\#G = n$ elements. Then G is cyclic and consists of the n-th roots of unity in K.*

Proof. For $a \in G$ always $a^n = 1$. Hence G is contained in the set of roots of the polynomial $T^n - 1 \in K[T]$. Hence K has exactly n different n-th roots of unity, and G consists exactly of these. Now let m be the exponent of G, in particular $m \leq n$. The following Lemma 2 yields: All $a \in G$ are m-th roots of unity whose number—as roots of the polynomial $T^m - 1$—is at most m. Therefore also $n \leq m$, hence $n = m$, and G has an element of order n. $\diamond$

Lemma 2 *Sei G be an abelian group.*

(i) *Let $a, b \in G$, $\operatorname{ord} a = m$, $\operatorname{ord} b = n$, where m, n are finite and coprime. Then $\operatorname{ord} ab = mn$.*

(ii) *Let $a, b \in G$, $\operatorname{ord} a$, $\operatorname{ord} b$ finite, $q = \operatorname{lcm}(\operatorname{ord} a, \operatorname{ord} b)$. Then there is a $c \in G$ with $\operatorname{ord} c = q$.*

(iii) *Let $m = \max\{\operatorname{ord} a | a \in G\}$, the exponent of G, be finite. Then $\operatorname{ord} b \mid m$ for all $b \in G$.*

Proof. (i) Let $k := \operatorname{ord}(ab)$. From $(ab)^{mn} = (a^m)^n \cdot (b^n)^m = 1$ it follows that $k|mn$. Since $a^{kn} = a^{kn} \cdot (b^n)^k = (ab)^{kn} = 1$ also $m|kn$, hence $m|k$, and likewise $n|k$, hence $mn|k$.

(ii) Let p^e be a prime power with $p^e|q$, say $p^e|m := \operatorname{ord} a$. Then a^{m/p^e} has order p^e. If $q = p_1^{e_1} \cdots p_r^{e_r}$ is the prime decomposition with different primes p_i, then there are $c_i \in G$ with $\operatorname{ord} c_i = p_i^{e_i}$. By (i) $c = c_1 \cdots c_r$ has order q.

(iii) Let $\operatorname{ord} b = n$. Then there is a $c \in G$ with $\operatorname{ord} c = \operatorname{lcm}(m, n)$. Thus $\operatorname{lcm}(m, n) \le m$, hence $= m$, hence $n|m$. $\diamond$

Theorem 5 *Let K be a finite field, $\#K = q$. Then the multiplicative group $K^\times$ is cyclic of order $q - 1$, and $a^{q-1} = 1$ for all $a \in K^\times$. Moreover $a^q = a$ for all $a \in K$. In particular K consists exactly of the roots of the polynomial $T^q - T \in \mathbb{F}_p[T]$.*

An element $a \in K$, K finite, is called **primitive** if it generates the multiplicative group $K^\times$.

A.3 Irreducible Polynomials and Field Extensions

Given two fields $L \supseteq K$ with $n = \operatorname{Dim}_K L < \infty$ we call L a finite field extension of K, and n its degree.

There is a common way of constructing field extensions: Let $f \in K[T]$ be an irreducible polynomial of degree n.

> The definition of "irreducible" is: f is not constant, and if $f = gh$ for $g, h \in K[T]$, then g or h is constant.

We'll show that $L = K[T]/fK[T]$ is a field extension of degree n.

First $K \subseteq K[T]$ as the set of constant polynomials, and $K \cap fK[T] = 0$. Therefore the natural homomorphism $K[T] \to L$ induces an injection $K \hookrightarrow L$, that allows us to identify K as a subfield of L.

Next we want to show that L is a field. We start with the division algorithm of polynomials. For a convenient handling of the zero polynomial in this context we assign it the degree $-\infty$. Thus $\deg r < 0$ is equivalent with $r = 0$.

Proposition 10 *Let K be a field, and let $f, g \in K[T]$, $g \neq 0$. Then there are uniquely determined polynomials $q, r \in K[T]$ such that $f = q \cdot g + r$ and $\deg r < \deg g$.*

Proof. Uniqueness: If $f = \tilde{q} \cdot g + \tilde{r}$ with $\deg \tilde{r} < \deg g$, then

$$0 = (\tilde{q} - q) \cdot g + \tilde{r} - r,$$

$$(q - \tilde{q}) \cdot g = \tilde{r} - r.$$

The degree of the right-hand side is $< \deg g$. If we assume that $q \neq \tilde{q}$, then the left-hand side has degree $\ge \deg g$ because the degree of a product is the sum of the degrees, contradiction. Hence $q = \tilde{q}$, and consequently also $r = \tilde{r}$.

Existence: We use the following Lemma 3 to conclude that we get a correct algorithm by the instructions:

Initialization: Put $r := f$, $q := 0$. (Then $f = qg + r$.)

Division loop: While $\deg r \geq \deg g$, replace q by $q + s$ and r by $r - sg$ with $\deg(r - sg) < \deg r$. (Then $\deg r$ decreases while the condition $f = qg + r$ is preserved.)

At the exit of the loop we have the sought-after polynomials. $\diamond$

Lemma 3 *Let $n \geq m$ and $f = a_nT^n + \cdots a_0$, $g = b_mT^m + \cdots + b_0$ with leading coefficients $a_n, b_m \neq 0$. Then $\deg(f - qg) < \deg f$ for*

$$q = \frac{a_n}{b_n} \cdot T^{n-m}.$$

Proof. The leading term of f cancels out. $\diamond$

As for integers this algorithm leads to an Euclidean algorithm. Here we only need a theoretical consequence. Define a **principal ring** to be a ring R all of whose ideals are principal, that is of the form aR (we consider commutative rings only). We already know a principal ring: $\mathbb{Z}$.

Proposition 11 *The polynomial ring $K[T]$ over a field K is principal.*

Proof. Let $\mathfrak{a} \trianglelefteq K[T]$ be an ideal. We may assume $\mathfrak{a} \neq 0$. Choose $g \in \mathfrak{a}$ of minimal degree ≥ 0, and $f \in \mathfrak{a}$ arbitrary. Division yields $r = f - qg \in \mathfrak{a}$ with a smaller gegree. This is possible only if $r = 0$, hence $f = qg \in gK[T]$. Therefore $\mathfrak{a} = gK[T]$. $\diamond$

An ideal $\mathfrak{m} \trianglelefteq R$ of a ring R is called maximal if it is maximal in the ordered set of *proper* ideals $\mathfrak{a} \neq R$. An ideal $\mathfrak{m}$ is maximal if and only if the residue class ring $R/\mathfrak{m}$ has only two ideals: the zero ideal $\mathfrak{m}/\mathfrak{m}$, and the unit ideal $R/\mathfrak{m}$, that is if and only if it is a field.

Proposition 12 *Let $f \in K[T]$ be irreducible and have degree n. Then $L = K[T]/fK[T]$ is a field extension of K of degree n.*

Proof. First L is a field since $fK[T]$ is a maximal ideal: If $fK[T] \subseteq \mathfrak{a} \triangleleft K[T]$, then the ideal $\mathfrak{a}$ also is principal $= gK[T]$. As a member of this ideal $f = gh$, and the irreducibility forces $h \in K$. Hence $fK[T] = gK[T] = \mathfrak{a}$.

Furthermore L as a vector space is spanned by the residue classes $t_i = T^i \bmod f$. The equation $f \bmod f = 0$ displays t^n as a linear combination of $t_0, \ldots, t_{n-1}$. By induction all t_i $(i \geq n)$ are linear combinations. Hence the dimension is $\leq n$. A linear combination $= 0$ of $t_0, \ldots, t_{n-1}$ would define a polynomial $g \equiv 0 \pmod f$ of degree $\leq n - 1$. Hence all its coefficients must be 0. Thus the dimension is $= n$. $\diamond$

An isomorphism of field extensions of K is an isomorphism of fields that fixes all elements of K. By $K[a]$ for $a \in L \supseteq K$ we denote the smallest subring of L that contains K and a. It consists of the polynomial expressions in a with coefficients in K. Note that in general these are not all different as elements of L.

Corollary 3 *Let $f \in K[T]$ be irreducible. Then in the field $L = K[T]/fK[T]$ the polynomial f has the root $t = T \bmod f$.*

If $M \supseteq K$ is a field extension containing a root a of f, then $K[a] \cong L$.

Proof. The natural homomorphism $K[T] \to L$ coincides with the substitution map $g \mapsto g(t)$. It maps f to 0, and that means that $f(t) = 0$.

The substitution map $K[T] \to M$, $g \mapsto g(a)$, is a homomorphism whose kernel contains $fK[T]$. By the Homomorphy Theorem it induces a homomorphism $\varphi\colon L \to M$. Since L is a field φ is injective, and the image of φ is $K[a]$. $\diamond$

This construction of field extensions generalizes one of the usual constructions of the complex numbers as $\mathbb{C} = \mathbb{R}[T]/(T^2+1)\mathbb{R}[T]$.

A.4 Splitting Fields

Continuing the considerations of the last section we are going to construct a field extension where a given polynomial f, not necessarily irreducible, splits into linear factors.

If f is reducible (i. e. not irreducible), then we split off a factor of smaller degree and successively arrive at a decomposition into irreducible polynomials. (Showing the uniqueness is easy but not needed here.) Therefore there is a field extension $L \supseteq K$ such that f has a root in L, hence a linear factor in $L[T] \supseteq K[T]$. Split this factor off and process the remaining polynomial in the same way until there remain only linear factors. A field extension $L \supseteq K$ where $f \in K[T]$ decomposes into linear factors is called **splitting field** of f. We just have shown the existence:

Proposition 13 *Every polynomial $f \in K[T]$ has a splitting field.*

Now let $L \supseteq K$ be an arbitrary field extension, and $a \in L$. Then

$$\mathfrak{a} = \{g \in K[T] \mid g(a) = 0\}$$

is an ideal of $K[T]$, hence a principal ideal $fK[T]$, where f has minimal degree in $\mathfrak{a} - \{0\}$ and is irreducible. (Otherwise a would be a root of a proper factor of f that also would belong to $\mathfrak{a}$.) Assume without restriction that the leading coefficient of f is 1. Then f is called **minimal polynomial** of a. Clearly its degree is $\dim_K K[a]$.

This said we return to finite fields. Let K be one of them with $q = p^e$ elements, p a prime number. Choose a primitive element $a \in K$. Then each element $\neq 0$ of K is a power of a, whence a forteriori a polynomial in a. Hence $K = \mathbb{F}_p[a]$. The minimal polynomial $f \in \mathbb{F}_p[T]$ of a divides $T^q - T$, and $K \cong \mathbb{F}_p[T]/f\mathbb{F}_p[T]$.

Consider an arbitrary field L of q elements. Then $L \supseteq \mathbb{F}_p$, and L is a splitting field of $T^q - T \in \mathbb{F}_p[T]$. In particular f has a root b in L. Hence $\mathbb{F}_p[b] \cong \mathbb{F}_p[T]/f\mathbb{F}_p[T] \cong K$, and because $\mathbb{F}_p[b]$ has q elements it must be the whole of L. Hence L is isomorphic with K: Up to isomorphism there is at most one field with q elements.

To show the existence we start with a splitting field K of $h = T^q - T \in \mathbb{F}_p[T]$. (We know there is one.) The derivative $h' = -1$ is constant $\neq 0$. Hence all roots of h in K are different. In particular there are q of them. They constitute a subfield of L: The sum of two roots a, b is again a root, $(a+b)^p = a^p + b^p = a + b$, likewise the product, and for $a \neq 0$ also $1/a$. We proved:

Theorem 6 (Galois **1830/**E. H. Moore **1893)** *For each prime power q there is up to isomorphism exactly one field with q elements.*

This result allows us to think of *the* field of q elements. We denote it by $\mathbb{F}_q$.