

## ALGEBRA II

## CONTENTS

|  |    |
|--|----|
| 1. Results from elementary number theory                             | 3  |
| 2. Groups  | 4  |
| 2.1. Definition, Subgroup, Order of an element                       | 4  |
| 2.2. Equivalence relation, Lagrange's theorem, Cyclic group          | 9  |
| 2.3. Homomorphism, Factor group, First isomorphism theorem           | 12 |
| 3. Rings and fields  | 15 |
| 3.1. Ring, Integral domain, Field, Characteristic                    | 15 |
| 3.2. Subring, Ideal, Residue class ring, Finite field $\mathbb{F}_p$ | 17 |
| 4. Polynomials   | 20 |
| 4.1. Divisibility in $F[x]$  | 22 |
| 4.2. Residue class ring $F[x]/(f)$                                   | 25 |
| 5. Field extensions  | 27 |
| 6. Finite fields   | 33 |
| 7. A brief introduction to the error correcting block codes          | 38 |
| 7.1. Cyclic codes  | 43 |

## 1. RESULTS FROM ELEMENTARY NUMBER THEORY

Recall the *division algorithm*: for  $a, d \in \mathbb{Z}$  ( $d \neq 0$ ), there exist unique  $q, r \in \mathbb{Z}$  such that

$$a = qd + r, \quad 0 \leq r < |d|$$

If the remainder  $r = 0$  we say that  $d$  *divides*  $a$  (or is a *factor* of  $a$ ) and write  $d \mid a$ . We use the notation  $a \bmod d$  for the remainder  $r$ .

An integer  $p > 1$  is a *prime number* if it has only the trivial factors  $\pm 1, \pm p$ .

**Theorem 1.1** (Fundamental Theorem of Arithmetics). *Let  $n > 1$  be an integer. There exist unique prime numbers  $p_1, \dots, p_t$  such that  $n = p_1 p_2 \cdots p_t$ .*

**Theorem 1.2.**

- (1)  $a \mid a \quad \forall a \in \mathbb{N}$ .
- (2)  $a \mid b$  and  $b \mid a \Rightarrow a = \pm b \quad \forall a, b \in \mathbb{N}$ .
- (3)  $a \mid b$  and  $b \mid c \Rightarrow a \mid c \quad \forall a, b \in \mathbb{N}$  and  $c \in \mathbb{Z}$ .
- (4)  $c \mid a$  and  $c \mid b \Rightarrow c \mid (au + bv) \quad \forall a, b, u, v \in \mathbb{Z}$  and  $c \in \mathbb{N}$ .

**Definition 1.1.** Let  $a, b \in \mathbb{Z}$  ( $b \neq 0$ ). Integer  $d$  is a *common factor* of  $a$  and  $b$  if it is a factor of  $a$  and  $b$ . The *greatest common divisor*  $\gcd(a, b)$  of  $a$  and  $b$  is the greatest element in the set of common factors of  $a$

The greatest common divisor  $\gcd(a, b)$  can be calculated by the *Euclidean algorithm*:

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots & \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Here, the last nonzero remainder  $r_n = \gcd(a, b)$ .

**Theorem 1.3.** *Let  $a, b \in \mathbb{Z}$  ( $b \neq 0$ ). There exists  $u, v \in \mathbb{Z}$  such that  $\gcd(a, b) = au + bv$ .*

**Definition 1.2.** Let  $a, b, n \in \mathbb{Z}$  ( $n > 0$ ). If  $n$  is a factor of  $a - b$  we say that  $a$  is congruent to  $b$  modulo  $n$  if  $a \equiv b \pmod{n}$ .

**Theorem 1.4.** Let  $a, b, c, d, n \in \mathbb{Z}$  ( $n > 0$ ). Then

- (1)  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ .
- (2)  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$ .
- (3)  $\gcd(a, n) = 1$  and  $ab \equiv ac \pmod{n} \Rightarrow b \equiv c \pmod{n}$ .
- (4)  $a \equiv b \pmod{n} \Leftrightarrow a \bmod n = b \bmod n$ .

**Theorem 1.5.** Let  $a, b, n \in \mathbb{Z}$  ( $n > 0$ ). The congruence

$$(1) \quad ax \equiv b \pmod{n}$$

is solvable if and only if  $\gcd(a, n) \mid b$ . The solutions of (1) in the interval  $[0, n - 1]$  are

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \dots, x_0 + (d - 1)\frac{n}{d},$$

where  $d = \gcd(a, n)$ , and  $x_0$  is the unique solution of

$$(2) \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

in the interval  $[0, n/d - 1]$ .

Moreover, any solution of (1) is congruent to  $x_0 + k\frac{n}{d}$  for some  $k \in \{0, \dots, d - 1\}$ .

**Remark 1.1.** We show how Euclidean algorithm can be used to find the solution  $x_0$  of (2). Since  $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$ , Theorem 1.3 implies that

$$\frac{a}{d}u + \frac{n}{d}v = 1$$

for some  $u, v \in \mathbb{Z}$ . Multiply both sides by  $\frac{b}{d}$  to get

$$\frac{a}{d}(u\frac{b}{d}) \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

It now follows from Theorem 1.4 (4) that  $x_0$  is equal to the remainder  $u\frac{b}{d} \bmod \frac{n}{d}$ .

## 2. GROUPS

### 2.1. Definition, Subgroup, Order of an element.

**Definition 2.1.** Let  $S$  be a set and let  $S \times S = \{(a, b) \mid a, b \in S\}$  (the set of ordered pairs  $(a, b)$  with  $a, b \in S$ ). A function  $S \times S \rightarrow S$  is called a *binary operation on  $S$* .

**Definition 2.2.** Let  $G$  be a non-empty set and  $*$  a binary operation on  $G$ . The pair  $(G, *)$  is called a *group* if the following three properties hold:

(1)  $*$  is *associative*, that is, for any  $a, b, c \in G$ ,

$$a * (b * c) = (a * b) * c.$$

(2) There is an *identity* (or *unity*) *element*  $e$  in  $G$  such that for all  $a \in G$ ,

$$a * e = e * a = a.$$

(3) For each  $a \in G$ , there exists an *inverse element*  $a^{-1}$  in  $G$  such that

$$a * a^{-1} = a^{-1} * a = e.$$

If the group also satisfies

(4) For all  $a, b \in G$ ,

$$a * b = b * a,$$

then the group is called *abelian* or (*commutative*).

From now on we usually write  $G$  instead of  $(G, *)$  and use multiplicative notation  $ab$  instead of  $a*b$ . Sometimes, especially when  $G$  is abelian, we use additive notation  $a + b$  instead of  $a * b$ . Respectively, we call  $G$  multiplicative or additive. If  $G$  is additive we write  $-a$  instead of  $a^{-1}$ .

**Remark 2.1.** It is easy to see that there is only one identity element in  $G$  and only one inverse  $a^{-1}$  for each  $a$  in  $G$ .

**Example 2.1.**  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ , and  $(\mathbb{C}, +)$  are abelian groups as well as  $(\mathbb{R}^*, \cdot)$  and  $(\mathbb{C}^*, \cdot)$ . The set of all invertible  $n \times n$  matrices with entries in  $\mathbb{R}$  is a non-abelian group with respect of matrix product.

For  $n \in \mathbb{N}$  and  $a \in G$  we define the  $n$ th *power*  $a^n$  of  $a$  by setting  $a^n = \overbrace{aa \cdots a}^{n \text{ times}}$ . Moreover, we set  $a^0 = e$  and  $a^{-n} = (a^{-1})^n$ .

It is easy to see that

$$(3) \quad \begin{aligned} a^n a^m &= a^{n+m}, \\ (a^n)^m &= a^{nm}, \end{aligned}$$

for all  $n, m \in \mathbb{Z}$ .

If we use the notation  $+$  on  $G$ , we write  $na$ , the  $n$ th *multiple* of  $a$ , instead of  $a^n$ . Now  $na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$ , if  $n \in \mathbb{N}$ . Moreover, we set  $0a = e$  and  $(-n)a = n(-a)$ .

Now we have,

$$\begin{aligned}na + ma &= (n + m)a, \\ m(na) &= (mn)a,\end{aligned}$$

for all  $n, m \in \mathbb{Z}$ .

**Definition 2.3.** A group  $G$  is *cyclic* if there is an element  $g$  in  $G$  such that

$$G = \{g^j \mid j \in \mathbb{Z}\}.$$

Such an element is a *generator* of  $G$  and we write  $G = \langle g \rangle$ .

**Remark 2.2.** Property (3) implies that any cyclic group is abelian.

**Example 2.2.** The generators of the additive group  $\mathbb{Z}$  are 1 and  $-1$ .

Consider next some groups with finite number of elements.

**Definition 2.4.** A group is called *finite* (resp. *infinite*) if it contains finitely (resp. infinitely) many elements. The number of elements in a finite group is called its *order*. We write  $|G|$  for the order of the finite group  $G$ .

Let  $a, n \in \mathbb{Z}$  ( $n > 0$ ). The *residue class*  $\bar{a}$  of  $a$  modulo  $n$  is the set

$$\bar{a} := \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}.$$

Each element in  $\bar{a}$  is called a *representative* of  $\bar{a}$ .

**Lemma 2.1.** Let  $a, b, n \in \mathbb{Z}$  ( $n > 0$ ). Then

$$\bar{a} \equiv \bar{b} \pmod{n} \Leftrightarrow \bar{a} \cap \bar{b} \neq \emptyset \Leftrightarrow \bar{a} = \bar{b}.$$

*Proof.* The first equivalence is obvious since  $c \in \bar{a} \cap \bar{b} \Leftrightarrow a \equiv c \equiv b \pmod{n}$ .

The implication  $\bar{a} = \bar{b} \Rightarrow \bar{a} \cap \bar{b} \neq \emptyset$  is obvious too, and hence we only need to prove:  $\bar{a} \cap \bar{b} \neq \emptyset \Rightarrow \bar{a} = \bar{b}$ .

So, assume  $c \in \bar{a} \cap \bar{b}$ , and let  $d \in \bar{a}$ . Now  $d \equiv a \equiv c \equiv b \pmod{n}$  and therefore  $d \in \bar{b}$ . Hence,  $\bar{a} \subseteq \bar{b}$ . By the symmetry we also have  $\bar{b} \subseteq \bar{a}$ .  $\square$

**Theorem 2.1.** The set  $\mathbb{Z}_n := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$  of residue classes modulo  $n$  forms a partition of  $\mathbb{Z}$ , i.e.

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \overline{n-1},$$

where the residue classes are pairwise distinct.

*Proof.* Let  $m \in \mathbb{Z}$ . By the division algorithm  $m \equiv r \pmod{n}$ , with  $0 \leq r \leq n-1$ . Hence,  $m$  belongs to the union. Obviously the union is a subset of  $\mathbb{Z}$ .

The residue classes are pairwise distinct by the first equivalence in Lemma 2.1.  $\square$

Now define the two binary operations, the addition  $+$  and the multiplication  $\cdot$ , on  $\mathbb{Z}_n$  by setting

$$\begin{aligned}\bar{a} + \bar{b} &= \overline{a + b}, \\ \bar{a} \cdot \bar{b} &= \overline{ab},\end{aligned}$$

where  $a, b$  are any representatives of the respective sets  $\bar{a}$  and  $\bar{b}$ .

**Remark 2.3.** It is easy to see that  $+$  and  $\cdot$  are well-defined i.e.  $\bar{a} + \bar{b}$  and  $\bar{a} \cdot \bar{b}$  are independent of the choice of the representatives of  $\bar{a}$  and  $\bar{b}$ .

**Theorem 2.2.**  $(\mathbb{Z}_n, +)$  is a finite cyclic group.

*Proof.* (Sketch.) (1) The associativity follows from the definition of  $+$  on  $\mathbb{Z}_n$  and the associativity of  $+$  on  $\mathbb{Z}$ . (2) The identity element is  $\bar{0}$ . (3) The inverse  $-\bar{a}$  of  $\bar{a}$  is  $\overline{-a}$ . Hence  $(\mathbb{Z}_n, +)$  is a group. It is finite by the definition, and  $\bar{1}$  is a generator for it.  $\square$

**Example 2.3.** The group table of the additive group  $\mathbb{Z}_4$  is

|           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|
| $+$       | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

Next define the set  $\mathbb{Z}_n^*$  of prime classes modulo  $n$ :

$$\mathbb{Z}_n^* := \{\bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

**Theorem 2.3.**  $(\mathbb{Z}_n^*, \cdot)$  is a finite abelian group.

*Proof.* (Sketch.) (1) The associativity follows from the definition of  $\cdot$  on  $\mathbb{Z}_n$  and the associativity of  $\cdot$  on  $\mathbb{Z}$ . (2) The identity element is  $\bar{1}$ . (3) Let  $a \in \mathbb{Z}_n^*$ . Now  $\bar{a}\bar{x} = \bar{1}$  if and only if  $ax \equiv 1 \pmod{n}$  is solvable. By Theorem 1.5 the congruence is solvable if  $\gcd(a, n) = 1$ , and consequently  $\bar{a}^{-1}$  exists for each  $\bar{a} \in \mathbb{Z}_n^*$ . (4) Since

$$\overline{\bar{a}\bar{b}} = \overline{ab} = \overline{ba} = \overline{\bar{b}\bar{a}},$$

the multiplicative group  $\mathbb{Z}_n^*$  is abelian.  $\square$

**Example 2.4.** The group table of the multiplicative group  $\mathbb{Z}_8^*$  is

|           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|
| $\cdot$   | $\bar{1}$ | $\bar{3}$ | $\bar{5}$ | $\bar{7}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{3}$ | $\bar{5}$ | $\bar{7}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ | $\bar{7}$ | $\bar{5}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{7}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{7}$ | $\bar{7}$ | $\bar{5}$ | $\bar{3}$ | $\bar{1}$ |

This group of order 4 is not cyclic, since  $\bar{a}^2 = \bar{1}$  for all  $\bar{a} \in \mathbb{Z}_8^*$ .

In the preceding example e.g. the subset  $\{\bar{1}, \bar{3}\}$  is a group. This motivates the following definition.

**Definition 2.5.** Let  $(G, *)$  be a group and let  $H$  be a subset of  $G$ . If  $(H, *)$  is group, then it is called a *subgroup* of  $(G, *)$ .

Every group  $G$  has at least two subgroups:  $\{e\}$  and  $G$ , the *trivial subgroups* of  $G$ .

**Lemma 2.2** (Subgroup criterion). *A non-empty set  $H$  of a group  $G$  is a subgroup of  $G$  if and only if  $ab^{-1} \in H$  for all  $a, b \in H$ .*

*Proof.* Exercise.  $\square$

**Example 2.5.**  $\mathbb{Z}_8^*$  has subgroups  $\{\bar{1}, \bar{3}\}$ ,  $\{\bar{1}, \bar{5}\}$ ,  $\{\bar{1}, \bar{7}\}$ . It is easy to see that these are the only non-trivial subgroups of  $\mathbb{Z}_8^*$ .

Let  $a$  be any element of a group  $G$ . The set  $\langle a \rangle := \{a^i \mid i \in \mathbb{Z}\}$  is a subgroup of  $G$  by the subgroup criterion. It is called a *cyclic subgroup* of  $G$ .

**Definition 2.6.** Let  $a$  be an element of a group  $G$ . If  $\langle a \rangle$  is finite, then its order is called the *order* of  $a$ . Otherwise,  $a$  is called an element of *infinite order*.

**Theorem 2.4.** *The order of an element  $a$  of a finite group is the least positive integer  $n$  satisfying  $a^n = e$ .*

*Proof.* Since  $G$  is finite,  $a^i = a^j$  for some  $0 < i < j$ . Hence,  $a^{j-i} = e$ . Let  $n$  be the least positive integer with  $a^n = e$ . Let  $k$  be any positive integer. Now  $k = nq + r$  for some  $0 \leq r < n$ , and  $a^k = a^{nq+r} = a^r$ . Hence  $\langle a \rangle = \{1, a, \dots, a^{n-1}\}$ , and all the powers  $a^i$  with  $i = 0, \dots, n-1$  are pairwise distinct by the choice of  $n$ . Hence  $|\langle a \rangle| = n$ .  $\square$

## 2.2. Equivalence relation, Lagrange's theorem, Cyclic group.

Next we generalize the concepts of congruence and residue class modulo  $n$ .

**Definition 2.7.** Let  $\sim$  be a relation on a set  $S$ . It is called an *equivalence relation* on  $S$  if it has the following three properties

- (1)  $a \sim a$  for all  $a \in S$  (*reflexivity*).
- (2) if  $a \sim b$  then  $b \sim a$  for all  $a, b \in S$  (*symmetry*).
- (3) if  $a \sim b$  and  $b \sim c$  then  $a \sim c$  for all  $a, b, c \in S$  (*transitivity*).

**Definition 2.8.** Let  $\sim$  be an equivalence relation on  $S$ , and let  $a \in S$ . The *equivalence class*  $\bar{a}$  of  $a$  with respect to  $\sim$  is the set

$$\bar{a} := \{b \in S \mid b \sim a\}.$$

Each element in  $\bar{a}$  is a *representative* of  $\bar{a}$ .

**Example 2.6.** Clearly the congruence  $\equiv$  modulo  $n$  is an equivalence relation on  $\mathbb{Z}$ , and the equivalence class of  $a \in \mathbb{Z}$  with respect to  $\equiv$  is the residue class of  $a$  modulo  $n$ .

We have analogues of Lemma 2.1 and Theorem 2.1:

**Lemma 2.3.** *Let  $\sim$  be an equivalence relation on  $S$ . Then*

$$a \sim b \Leftrightarrow \bar{a} \cap \bar{b} \neq \emptyset \Leftrightarrow \bar{a} = \bar{b}.$$

*Proof.* We may replace  $\equiv$  with  $\sim$  in the proof of Lemma 2.1, since there is used only the defining properties of an equivalence relation.  $\square$

**Theorem 2.5.** *Let  $\sim$  be an equivalence relation on  $S$ . There exists a subset  $T$  of  $S$  such that the set of equivalence classes  $\{\bar{t} \mid t \in T\}$  with respect to  $\sim$  forms a partition of  $S$ , i.e.*

$$S = \bigcup_{t \in T} \bar{t},$$

where the equivalence classes are pairwise distinct.

*Proof.* Let  $t \in S$ . Now  $t \in \bar{t}$  by the reflexivity. Hence,

$$S = \bigcup_{t \in S} \bar{t} = \bigcup_{t \in T' \subseteq S} \bar{t}$$

where  $\bar{a} \neq \bar{b}$  for all  $a, b \in T'$ ,  $a \neq b$ . By Lemma 2.3  $\bar{a} \cap \bar{b} = \emptyset$  for all  $a, b \in T'$ ,  $a \neq b$ . Hence we may choose  $T = T'$ .  $\square$

**Lemma 2.4.** *Let  $H$  be a subgroup of a group  $G$  and define relation  $\sim$  on  $G$  as follows:*

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

*Then  $\sim$  is an equivalence relation on  $G$ .*

*Proof.* (1) Since  $aa^{-1} = 1 \in H$ ,  $a \sim a$ . (2) Assume  $a \sim b$  i.e.  $ab^{-1} \in H$ . Since  $H$  is a group, the inverse element  $(ab^{-1})^{-1}$  is also in  $H$ . But  $(ab^{-1})^{-1} = ba^{-1}$ . Hence  $b \sim a$ . (3) Assume  $a \sim b$  and  $b \sim c$  i.e.  $ab^{-1} = h_1$  and  $bc^{-1} = h_2$  for some  $h_1, h_2 \in H$ . Now

$$ac^{-1} = a(b^{-1}h_2) = a((a^{-1}h_1)h_2) = (aa^{-1})(h_1h_2) \in H.$$

Hence  $a \sim c$ . □

Let  $a \in G$ . The equivalence class of  $a$  with respect the relation  $\sim$  defined above is

$$\bar{a} = \{b \in G \mid ba^{-1} \in H\} = \{ha \mid h \in H\} =: Ha.$$

and is called the *right coset of  $a$  modulo  $H$* .

If we had defined  $\sim$  as  $a \sim b$  if and only if  $a^{-1}b \in H$ , then the equivalence class of  $a$  would have been the *left coset of  $a$  modulo  $H$* :

$$aH := \{ah \mid h \in H\}.$$

We consider left cosets and call them just cosets.

**Example 2.7.** Let  $n \in \mathbb{N}$ ,  $G = (\mathbb{Z}, +)$  and  $H = \langle n \rangle$ . Now the coset of  $a$  modulo  $H$  is the set

$$a + H = \{a + h \mid h \in H\} = \{a + nk \mid k \in \mathbb{Z}\}$$

which is exactly the residue class of  $a$  modulo  $n$ .

The cardinalities of two cosets modulo  $H$  are equal:

**Lemma 2.5.** *Let  $H$  be a subgroup of a group  $G$  and  $a \in G$ . Then, the function*

$$f : H \rightarrow aH, f(x) = ax,$$

*is bijective.*

*Proof.* Let  $b \in aH$ . Now  $b = ah$  for some  $h \in H$ , and  $f(h) = b$ . Hence  $f$  is surjective. It is also injective:

$$f(h) = f(h') \Rightarrow ah = ah' \Rightarrow h = h'.$$

□

We can now prove an important result:

**Theorem 2.6** (Lagrange). *Let  $H$  be a subgroup of a finite group  $G$ . Then, the order of  $H$  is a factor of order of  $G$ .*

*Proof.* By Theorem 2.5 we have partition  $G = \bigcup_{t \in T \subseteq G} tH$ . By Lemma 2.5,  $|H| = |tH|$  for all  $t \in T$ , and therefore

$$|G| = \sum_{t \in T} |tH| = |T| \cdot |H|.$$

□

**Corollary 2.1.** *Let  $G$  be a finite group. Then,  $a^{|G|} = e$  for all  $a \in G$ .*

*Proof.* Let  $a \in G$ . By Lagrange's Theorem  $n := |\langle a \rangle|$  is a factor  $|G|$ , say  $|G| = nd$ . Now, by Theorem 2.4,  $a^{|G|} = a^{nd} = (a^n)^d = e$ . □

**Corollary 2.2** (Fermat's little theorem). *Let  $p$  be a prime number and let  $a \in \mathbb{Z}$ . Then*

$$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

*Proof.* Since  $\gcd(a, p) = 1$ ,  $\bar{a} \in \mathbb{Z}_p^*$ . Since  $|\mathbb{Z}_p^*| = p - 1$ , Corollary 2.1 implies that  $\bar{a}^{p-1} = \bar{1}$ , equivalently,  $a^{p-1} \equiv 1 \pmod{p}$ . □

**Theorem 2.7.** *Let  $G = \langle g \rangle$  be a cyclic group. Then*

(1) *each subgroup of  $H$  is cyclic.*

*If, moreover,  $|G| = n$ , then*

(2) *For each factor  $d$  of  $n$  there exists exactly one subgroup  $H$  of  $G$ , namely  $H = \langle g^{\frac{n}{d}} \rangle$ .*

*Proof.* (1) Obviously  $\{e\} = \langle e \rangle$ . Assume  $H \neq \{e\}$ . The elements of  $H$  are of the form  $g^i$ ,  $i \in \mathbb{Z}$ . Let  $m$  be the least positive integer such that  $g^m \in H$ . We show that  $H = \langle g^m \rangle$ .

Let  $g^t \in H$ . Now  $t = qm + r$ ,  $0 \leq r < m$ , for some  $q, r \in \mathbb{Z}$ , and therefore  $g^t = g^{qm}g^r$ . Hence,  $g^r = g^t g^{-qm} \in H$ . By the minimality of  $m$  we must have  $r = 0$ , and therefore  $g^t = g^{qm} \in \langle g^m \rangle$ .

(2) Let  $H$  be a subgroup of  $G$ . If  $H$  is trivial we are done. Assume  $H$  is non-trivial. By (1)  $H = \langle g^t \rangle$  for some  $t \in \mathbb{Z}$ ,  $t > 0$ . Write  $t = dt'$ , where  $d = \gcd(t, n)$ . We show that  $H = \langle g^d \rangle$ .

Obviously,  $H \subseteq \langle g^d \rangle$ . So, we only need to prove that  $g^d \in H$ . Since  $\gcd(t', n) = 1$ , we have  $t'x_0 \equiv 1 \pmod{n}$ , for some  $x_0 \in \mathbb{Z}$ . Now  $(g^{t'})^{x_0} = (g^{dt'})^{x_0} = (g^d)^{t'x_0} = (g^d)^{1+kn}$  for some integer  $k$ . Now, by Corollary 2.1, we get  $(g^{t'})^{x_0} = g^d(g^{dk})^n = g^d$ , and therefore  $g^d \in H$ .  $\square$

**Example 2.8.** The subgroups of the additive group  $\mathbb{Z}_{15}$  are  $\{\bar{0}\}$ ,  $\langle \bar{1} \rangle = \mathbb{Z}_{15}$ ,  $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}\}$ , and  $\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \bar{10}\}$ .

### 2.3. Homomorphism, Factor group, First isomorphism theorem.

When comparing the structures of two groups, functions between the groups which preserve the operations play an important role.

**Definition 2.9.** Let  $(G, *)$  and  $(G', \circ)$  be groups. A function  $f : G \rightarrow G'$  is called a *homomorphism* if it satisfies the following property:

$$f(a * b) = f(a) \circ f(b) \quad \forall a, b \in G.$$

A homomorphism which is also bijection is called an *isomorphism*. If there is an isomorphism between  $G$  and  $G'$ , then they are said to be isomorphic and this is denoted by  $G \simeq G'$ .

**Example 2.9.** The groups  $(\mathbb{R}, +)$  and  $(\mathbb{R}_{>0}, \cdot)$ , where  $\mathbb{R}_{>0}$  is the set of positive real numbers, are isomorphic since the exponential function  $f(x) = e^x$  is an isomorphism from  $(\mathbb{R}, +)$  onto  $(\mathbb{R}_{>0}, \cdot)$ .

**Lemma 2.6.** Let  $f : G \rightarrow G'$  be a homomorphism, and let  $e$  and  $e'$  be the identity elements of  $G$  and  $G'$ . Then

- (1)  $f(e) = e'$
- (2)  $f(a)^{-1} = f(a^{-1})$  for all  $a \in G$ .

*Proof.* (1)  $f(e) = f(e * e) = f(e) \circ f(e)$ . Hence,  $f(e) = e'$ .

(2)  $f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e) \stackrel{(1)}{=} e'$ . Hence, the inverse of  $f(a)$  equals  $f(a^{-1})$ .  $\square$

**Definition 2.10.** The *kernel*  $\ker f$  of a homomorphism  $f : G \rightarrow G'$  is the set of all inverse images of  $e'$  under  $f$  i.e.

$$\ker f = \{a \in G \mid f(a) = e'\}.$$

The *image*  $\text{im} f$  of  $f$  is the value set of  $f$  i.e.

$$\text{im} f = \{f(a) \mid a \in G\}.$$

**Lemma 2.7.** *The kernel of a homomorphism  $f : G \rightarrow G'$  is a subgroup of  $G$ , and the image of  $f$  is a subgroup of  $G'$ .*

*Proof.* By Lemma 2.6 (1),  $f(e) = e'$  and therefore  $\ker f \neq \emptyset$ . Let  $a, b \in \ker f$ . Now  $f(a * b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ f(b)^{-1} = e' \circ e'^{-1} = e' \circ e' = e'$ . Hence  $ab^{-1} \in \ker f$ . Now, by the subgroup criterion  $\ker f$  is subgroup of  $G$ .

Let  $c, d \in \text{im} f$ . Now  $c = f(a)$  and  $d = f(b)$  for some elements  $a, b \in G$ . Now  $cd^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ . Hence,  $cd^{-1} \in \text{im} f$ .  $\square$

**Theorem 2.8.** *Let  $f : G \rightarrow G'$  be a homomorphism, and let  $H = \ker f$ . The set  $G/H$  of cosets modulo  $H$  is a group with respect the operation  $\cdot$  defined by*

$$aH \cdot bH = abH.$$

*Proof.* First we show that the operation is well defined i.e. we show that if  $aH = a'H$  and  $bH = b'H$ , then  $a'H \cdot b'H = aH \cdot bH$ .

If  $aH = a'H$  and  $bH = b'H$ , then  $a'H \cdot b'H = a'b'H = ah_1bh_2H$  for some  $h_1, h_2 \in H$ . We need to show that  $ah_1bh_2H = abH$ , or equivalently, that  $h_1b = bh_3$  for some  $h_3 \in H$  (by Lemmas 2.3 and 2.4). Since  $f(b^{-1}h_1b) = f(b)^{-1}f(h_1)f(b) = f(b)^{-1}f(b) = e'$ , we have  $b^{-1}h_1b = h_3$  for some  $h_3 \in H$ .

The associativity follows from the associativity of the operation of  $G$ , the identity element is  $H$  and the inverse element of  $aH$  is  $a^{-1}H$ .  $\square$

Note that if  $H$  is a subgroup of  $G$  satisfying  $bH = Hb$  for all  $b \in G$ , then the proof above shows that the set  $G/H$  of cosets modulo  $H$  is a group.

**Definition 2.11.** Let  $H$  be a subgroup of  $G$ . If  $aH = Ha$  for all  $a \in G$ , then  $H$  is said to be *normal* in  $G$ .

Now we can generalize the preceding theorem:

**Theorem 2.9.** *Let  $H$  be a normal subgroup of  $G$ . Then  $(G/H, \cdot)$  is a group.*

**Definition 2.12.** The group  $(G/H, \cdot)$  is called a factor group of  $G$  modulo  $H$ .

**Example 2.10.**  $\mathbb{Z}_7^*$  is an abelian group and therefore each of its subgroups is normal. Consider e.g. the factor group  $\mathbb{Z}_7^*/\langle\bar{6}\rangle$ . The cosets modulo  $\langle\bar{6}\rangle$  are

$$\bar{1} = \langle\bar{6}\rangle = \{\bar{1}, \bar{6}\}, \quad \bar{2} = \bar{2}\langle\bar{6}\rangle = \{\bar{2}, \bar{5}\}, \quad \bar{3} = \bar{3}\langle\bar{6}\rangle = \{\bar{3}, \bar{4}\},$$

and the group table of  $\mathbb{Z}_7^*/\langle\bar{6}\rangle$  is

|           |           |           |           |
|-----------|-----------|-----------|-----------|
| $\cdot$   | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ | $\bar{2}$ |

**Example 2.11.** Let  $n \in \mathbb{Z}$ ,  $n > 0$ . Obviously  $f : (\mathbb{Z}, +) \rightarrow \mathbb{Z}_n, f(a) = \bar{a}$ , is a homomorphism. Now  $\ker f = \langle n \rangle$ . The function  $F : \mathbb{Z}/\langle n \rangle \rightarrow \mathbb{Z}_n, F(a + \langle n \rangle) = \bar{a}$  is an isomorphism.

The example above can be generalized:

**Theorem 2.10** (First homomorphism theorem). *Let  $f : G \rightarrow G'$  be a homomorphism. Then the function*

$$F : G/\ker f \rightarrow \text{im}(f), F(aH) = f(a)$$

*is an isomorphism.*

*Proof.* Let  $H = \ker f$ . We first show that  $F$  is well defined. Let  $aH = a'H$ . Now  $a = a'h$  for some  $h \in H$ , and therefore  $f(a) = f(a'h) = f(a')f(h) = f(a')$ . Hence  $F(aH) = f(a) = f(a') = F(a'H)$ .

Let  $c \in \text{im} f$ . Now  $c = f(a)$  for some  $a \in G$ , and therefore  $F(aH) = f(a) = c$ . Hence,  $F$  is surjective. It is injective too:

$$\begin{aligned} F(aH) = F(bH) &\Rightarrow f(a) = f(b) \Rightarrow f(ab^{-1}) = f(a)f(b)^{-1} = e' \\ &\Rightarrow ab^{-1} \in H \Rightarrow aH = bH. \end{aligned}$$

□

**Example 2.12.** Let  $f : \mathbb{C}^* \rightarrow \mathbb{R}^*, f(z) = |z|$ . Now  $f(zw) = |zw| = |z||w| = f(z)f(w)$ , and so  $f$  is a homomorphism. Clearly  $\text{im} f = \mathbb{R}_{>0}$ . The kernel  $\ker f = \{z \in \mathbb{C}^* \mid |z| = 1\}$  is the unit circle  $S^1$  of the complex plane and so we have isomorphism  $\mathbb{C}^*/S^1 \simeq \mathbb{R}_{>0}$ .

## 3. RINGS AND FIELDS

## 3.1. Ring, Integral domain, Field, Characteristic.

Consider next a set where two binary operations are defined and which satisfy certain axioms.

**Definition 3.1.** Let  $R$  be a set with at least two elements, and let  $+$  and  $\cdot$  be two binary operations defined on  $R$ . The triple  $(R, +, \cdot)$  is called a *ring*, if the following axioms are satisfied:

- (1)  $(R, +)$  is an additive abelian group.
- (2)  $\cdot$  is associative.
- (3) There exists identity element 1 with respect to  $\cdot$ .
- (4) The *distributive laws* hold i.e. for all  $a, b, c \in R$  we have

$$a(b + c) = ab + ac \quad \text{and} \quad (b + c)a = ba + ca.$$

If  $ab = ba$  for all  $a, b \in R$ , then  $R$  is called a *commutative ring*.

**Remark 3.1.** In a ring  $R$  we denote by 0 the identity element with respect to  $+$ . Moreover, the additive inverse of  $a \in R$  is denoted by  $-a$ , and  $a + (-b)$  is abbreviated by  $a - b$ .

The following familiar looking rules hold in every ring.

**Lemma 3.1.** *Let  $R$  be a ring. Then*

- (1)  $0 \cdot a = 0 = a \cdot 0$  for all  $a \in R$ .
- (2)  $1 \neq 0$ .
- (3)  $(-a)b = -ab = a(-b)$  for all  $a, b \in R$ .
- (4)  $(-a)(-b) = ab$  for all  $a, b \in R$ .

*Proof.* Exercise. □

**Example 3.1.** Some familiar commutative rings are  $\mathbb{Z}$ ,  $\mathbb{R}$  and  $\mathbb{C}$ . The matrix ring  $(M_{n \times n}(\mathbb{R}), +, \cdot)$  is also a ring but not commutative.

**Example 3.2.** Let  $n \in \mathbb{N}$ . Then  $(\mathbb{Z}_n, +, \cdot)$  is a finite commutative ring. Assume  $n = mt$  with  $m, t > 1$ . Then  $\bar{m}\bar{t} = \bar{0}$  although both  $\bar{m} \neq \bar{0}$  and  $\bar{t} \neq \bar{0}$ . This motivates the following definition.

**Definition 3.2.** Let  $R$  be commutative ring.  $R$  is an *integral domain* if for all  $a, b \in R$  condition  $ab = 0$  implies  $a = 0$  or  $b = 0$ .

**Example 3.3.**  $\mathbb{Z}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are integral domains.

**Example 3.4.** Let  $n \in \mathbb{N}$ . We show that  $\mathbb{Z}_n$  is an integral domain if and only if  $n$  is a prime number. We have already seen, that  $\mathbb{Z}_n$  is not an integral domain if  $n$  is a composite number. Assume  $n$  is a prime. Then  $\mathbb{Z}_n^* = \{\bar{1}, \dots, \overline{n-1}\}$ . If now  $\bar{a}\bar{b} = \bar{0}$  and  $\bar{a} = 0$ , then by multiplying the equation by  $\bar{a}^{-1}$  we get  $\bar{b} = 0$ .

**Definition 3.3.** Let  $R$  be a ring. If an element  $a \in R$  has the multiplicative inverse  $a^{-1}$  it is called an *unit* in  $R$ . The set of units in  $R$  is denoted by symbol  $R^*$

**Example 3.5.**  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ,  $\mathbb{Z}^* = \{-1, 1\}$ .

**Lemma 3.2.**  $(\mathbb{R}^*, \cdot)$  is a group.

*Proof.* Exercise. □

In this course we are particularly interested in the commutative rings  $R$  with  $R^*$  maximal i.e.  $R^* = R \setminus \{0\}$ .

**Definition 3.4.** Let  $(F, +, \cdot)$  be a commutative ring. If  $F^* = F \setminus \{0\}$ , then  $F$  is called a *field*.

**Theorem 3.1.** *Each field is an integral domain. Each finite integral domain is a field.*

*Proof.* Let  $F$  be a field and let  $a, b \in F$  such that  $ab = 0$ . If  $a \neq 0$ , then by multiplying by  $a^{-1}$  we get  $b = 0$ .

Assume then that  $R$  is a finite integral domain. Let  $a \in R$ ,  $a \neq 0$ . To prove that  $R$  is field, it is enough to show that  $a^{-1}$  exists. To that end we consider the function  $f_a : R \rightarrow R$ ,  $f_a(x) = ax$ . If  $f_a$  is bijective, then it follows that  $f_a(b) = 1$  for some  $b \in R$ , and therefore  $b = a^{-1}$ .

We show that  $f_a$  indeed is a bijection. First,

$$f_a(b) = f_a(c) \Rightarrow ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c,$$

and so  $f_a$  is injective. Now  $|\text{im} f| = |R|$ , and it follows that  $f$  is surjective as well. □

**Corollary 3.1.**  $\mathbb{Z}_p$  is a field if and only if  $p$  is a prime number.

*Proof.* By Example 3.4,  $\mathbb{Z}_p$  is an integral domain if and only if  $p$  is a prime.  $\square$

A big difference in the rings  $\mathbb{Z}$  and  $\mathbb{Z}_n$  is that the order of any nonzero element in  $(\mathbb{Z}, +)$  is infinite while in  $(\mathbb{Z}_n, +)$   $nr = 0$  for all  $r \in R$ . We formalize this property.

**Definition 3.5.** Let  $R$  be a ring. The least positive integer  $n$  satisfying  $nr = 0$  for all  $r \in R$  is called the *characteristic* of  $R$ . If there does not exist a positive integer  $n$  such that  $nr = 0$  for all  $r \in R$ , then the characteristic of  $R$  is defined to be 0. The characteristic of  $R$  is denoted by  $\text{char}(R)$ .

**Example 3.6.** Obviously  $\text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$ . The characteristic of  $\mathbb{Z}_n$  is  $n$ , since  $nr = 0$  for all  $r \in \mathbb{Z}_n$ , and this is the least positive integer satisfying  $n\bar{1} = 0$ .

**Remark 3.2.** The characteristic of a ring  $R$  is the actually least positive integer  $n$  such that  $n1 = 0$ , since if  $n1 = 0$ , then  $nr = (n1)r = 0r = 0$  for all  $r \in R$ .

**Theorem 3.2.** *Let  $R$  be an integral domain with positive characteristic. Then  $\text{char}(R) = p$  for some prime number  $p$ .*

*Proof.* Let  $\text{char}(R) = n$ , and let  $n = mt$  for some integers  $m, t \geq 1$ . Now  $n1 = (m1)(t1) = 0$ , and since  $R$  is an integral domain,  $m1 = 0$  or  $t1 = 0$ . Since  $n$  is the least positive integer with  $n1 = 0$ , we must have  $m = n$  or  $t = n$ . Hence,  $n$  has only trivial factors and is therefore a prime.  $\square$

**Corollary 3.2.** *The characteristic of a finite field is a prime number.*

*Proof.* Let  $F$  be a finite field. Since  $n1 \in F$  for all positive integers  $n$ , and  $F$  is finite, we must have  $m1 = n1$  for some positive integers  $m, n$  with  $m \neq n$ . Hence  $(m - n)1 = 0$ , and therefore  $F$  is an integral domain with positive characteristic.  $\square$

### 3.2. Subring, Ideal, Residue class ring, Finite field $\mathbb{F}_p$ .

**Definition 3.6.** Let  $S$  be a subset of a ring  $(R, +, \cdot)$ . If also  $(S, +, \cdot)$  is a ring, it is called a *subring* of  $R$ .

**Definition 3.7.** An *ideal* of a ring  $(R, +, \cdot)$  is a subset  $I$  of  $R$  satisfying the following two properties:

- (1)  $(I, +)$  is a subgroup  $(R, +)$ .

(2)  $ri \in I$ , for all  $r \in R$  and for all  $i \in I$ .

**Example 3.7.** Let  $R$  be a commutative ring and let  $a \in R$ . Then the set  $(a) := \{ra \mid r \in R\}$  is easily seen to be an ideal of  $R$ . It is called a *principal ideal* of  $R$ . Here, element  $a$  is called a *generator* of  $(a)$ .

Since the additive group  $(R, +)$  of a ring  $R$  is assumed to be abelian, any ideal  $(I, +)$  of  $R$  is normal in  $(R, +)$ . Hence, we can form the factor group  $(R/I, +)$ , where  $(a + I) + (b + I) := a + b + I$ . We define the multiplication  $\cdot$  on  $R/I$  by setting  $(a + I) \cdot (b + I) := ab + I$ . The second condition in the definition of an ideal implies that this multiplication is well-defined, and now we get

**Theorem 3.3.** *Let  $I$  be an ideal of a commutative ring  $R$ . Then  $(R/I, +, \cdot)$  is a commutative ring.*

*Proof.* Exercise. □

We call  $(R/I, +, \cdot)$  as a *residue class ring* of  $R$  modulo  $I$ , and its element  $a + I$  is called the *residue class* of  $a$  modulo  $I$ .

**Example 3.8.** Let  $n \in \mathbb{N}$ . Now, the ring  $\mathbb{Z}/(n)$  consists of the residue classes  $a + (n) = \{a + nk \mid k \in \mathbb{Z}\} = \bar{a}$ . Hence,  $(\mathbb{Z}/(n), +, \cdot) = (\mathbb{Z}_n, +, \cdot)$ .

The concept of a homomorphism can also be defined in the context of ring theory.

**Definition 3.8.** Let  $R$  and  $R'$  be rings. A function  $f : R \rightarrow R'$  is called a *homomorphism* if it satisfies the following three conditions for all  $a, b \in R$ :

- (1)  $f(a + b) = f(a) + f(b)$
- (2)  $f(ab) = f(a)f(b)$
- (3)  $f(1_R) = 1_{R'}$

If  $f$  is also a bijection, it is called an *isomorphism*, and  $R$  and  $R'$  are called *isomorphic*. This is denoted by  $R \simeq R'$ .

**Definition 3.9.** The *kernel* of a ring homomorphism  $f : R \rightarrow R'$  is the set

$$\ker f = \{r \in R \mid f(r) = 0\}$$

**Lemma 3.3.** *The kernel of a ring homomorphism  $f : R \rightarrow R'$  is an ideal of  $R$ .*

*Proof.* Since  $f$  is a group homomorphism from  $(R, +)$  into  $(R', +)$ , we know that  $\ker f$  is subgroup of  $(R, +)$ . Moreover, if  $r \in R$  and  $i \in \ker f$ , then  $f(ri) = f(r)f(i) = f(r)0 = 0$  i.e.  $ri \in \ker R$ .  $\square$

Like in group theory, we have an isomorphism theorem.

**Theorem 3.4.** *Let  $f : R \rightarrow R'$  be a ring homomorphism, and let  $I = \ker f$ . Then*

$$F : R/I \rightarrow \text{im}f, \quad F(r + I) = f(r)$$

*is a ring isomorphism.*

*Proof.* Exercise.  $\square$

We can use mappings to transfer a structure from an algebraic system to a set without structure. For instance, let  $(R, +, \cdot)$  be ring and let  $S$  be a set. Assume we have a bijection  $f : R \rightarrow S$ . This bijection can be used to give the structure of  $R$  on  $S$  by defining  $+$  and  $\cdot$  on  $S$  as follows:

$$\begin{aligned} s + t &= f(f^{-1}(s) + f^{-1}(t)) \quad \forall s, t \in S, \\ s \cdot t &= f(f^{-1}(s)f^{-1}(t)) \quad \forall s, t \in S. \end{aligned}$$

Obviously  $(S, +, \cdot)$  is a ring and isomorphic to  $(R, +, \cdot)$ . We say that  $S$  has the *ring structure induced by  $f$* .

**Definition 3.10.** Let  $p$  be a prime number, and let  $\mathbb{F}_p$  denote the set  $\{0, 1, \dots, p-1\}$  with the ring structure induced by the function  $f : \mathbb{Z}_p \rightarrow \mathbb{F}_p, f(\bar{a}) = a$  for  $a = 0, \dots, p-1$ . Then  $(\mathbb{F}_p, +, \cdot)$  is called the *finite field (or Galois field) of order  $p$* .

**Remark 3.3.** The finite field  $\mathbb{F}_p$  can be seen as the set consisting of the integers  $0, 1, \dots, p-1$ , and where  $a + b = (a + b) \bmod p$ , and  $ab = ab \bmod p$ .

**Example 3.9.** The calculation tables of  $\mathbb{F}_2$  are

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

We have seen the existence of a finite field  $\mathbb{F}_p$  for each prime number  $p$ . We shall construct all the other existing finite fields as residue class rings of (formal) polynomial rings.

## 4. POLYNOMIALS

**Definition 4.1.** Let  $R$  be an integral domain. Let  $f : \mathbb{Z}_{\geq 0} \rightarrow R, f(i) = f_i$  be a function with finite image. Let  $n$  be the largest index such that  $f_n \neq 0$ . Then we denote

$$f(x) = f_0 + f_1x + \cdots + f_nx^n,$$

where  $f_n \neq 0$ , and say that  $f(x)$  is a (*formal*) *polynomial over  $R$* . Moreover,

- Elements  $f_i$  are the *coefficients* of  $f(x)$ .
- $f_0$  is the *constant term* of  $f(x)$ .
- $f_n$  is the *leading coefficient* of  $f(x)$
- $f(x)$  is *monic* if the leading coefficient equals 1.
- $n =: \deg(f(x))$  is the *degree* of  $f(x)$ .
- If  $f_i = 0$  for all  $i \in \mathbb{Z}_{\geq 0}$ , then  $f(x)$  is the *zero polynomial*, denoted by  $f(x) = 0$ , and then we set  $\deg(f(x)) = -\infty$ .
- The set of all polynomials over  $R$  is denoted by the symbol  $R[x]$ .

For a polynomial  $f(x)$  we use also the abbreviated notation  $f$ . By the definition of a polynomial, two polynomials  $f, g$  are equal if and only if their coefficients are equal for all indices i.e.  $f_i = g_i$  for all  $i \in \mathbb{Z}_{\geq 0}$ .

**Example 4.1.** Some familiar set of polynomials:  $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{C}[x]$ .

**Example 4.2.** We are especially interested in the sets

$$\mathbb{F}_p[x] = \{f_0 + f_1x + \cdots + f_nx^n \mid f_i \in \mathbb{F}_p, n \in \mathbb{N}\}.$$

In this set, for instance  $1 + x^2 + x^7$  and  $1 + 3x^2 + x^7$  are not equal if  $p \neq 2$ . However,  $3 = 3 \cdot 1 = 1$  in  $\mathbb{F}_2$ , and therefore the polynomials in question are equal in  $\mathbb{F}_2[x]$ .

Let  $f(x) = f_0 + f_1x + \cdots + f_mx^m \in R[x]$  and  $g(x) = g_0 + g_1x + \cdots + g_nx^n \in R[x]$ . Define their addition  $+$  and the multiplication  $\cdot$  “as usual”:

$$f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (f_i + g_i)x^i$$

$$f(x)g(x) = \sum_{i=0}^{n+m} \left( \sum_{t=0}^i f_t g_{i-t} \right) x^i,$$

**Remark 4.1.** We see that the product can be formed by multiplying all the monomials and then collecting together the monomials of equal degree, and by summing their coefficients.

**Example 4.3.** Let  $f(x) = 1 + x, g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]$ . Now

$$f(x) + g(x) = 1 + 1 + x + x^2 + x^3 = x + x^2 + x^3,$$

and

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

Moreover,  $\deg(f + g) = 3$  ja  $\deg(fg) = 4$ .

**Lemma 4.1.** Let  $f, g \in R[x]$ . Then

$$(1) \deg(f + g) \leq \max(\deg f, \deg g), \quad (2) \deg(fg) = \deg f + \deg g.$$

*Proof.* Exercise. □

**Theorem 4.1.**  $(R[x], +, \cdot)$  is an integral domain.

*Proof.* (Sketch.) It is easy to see that  $(R[x], +)$  is an Abelian group; the zero element is the zero polynomial 0, and the additive inverse  $-f$  of  $f(x) = f_0 + f_1x + \cdots + f_nx^n$  is  $-f(x) = -f_0 - f_1x - \cdots - f_nx^n$ .

The identity element of  $R[x]$  is the constant polynomial 1, and it follows from the definitions of  $+$  and  $\cdot$ , that  $\cdot$  is associative and commutative, and that the distributivity holds in  $R[x]$ . Moreover,  $R[x]$  is an integral domain:

$$\begin{aligned} fg = 0 &\Rightarrow \deg(f) + \deg(g) = \deg(fg) = -\infty \Rightarrow \deg f < 0 \text{ or } \deg g < 0 \\ &\Rightarrow f = 0 \text{ or } g = 0. \end{aligned}$$

□

**Remark 4.2.** It follows from Theorem 4.1 that

$$f(x)g(x) = \sum_{i=0}^n \sum_{j=0}^m f_i x^i g_j x^j = \sum_{i=0}^n \sum_{j=0}^m f_i g_j x^{i+j},$$

where  $n = \deg(f)$  ja  $m = \deg(g)$ .

**Theorem 4.2.** The set of units  $R[x]^*$  in  $R[x]$  is the set of units  $R^*$  in  $R$ .

*Proof.* If  $fg = 1$ , then  $\deg(f) + \deg(g) = 0$ . Since now  $\deg(f) \geq 0$  and  $\deg(g) \geq 0$ , we get  $\deg f = \deg g = 0$ . □

#### 4.1. Divisibility in $F[x]$ .

Let  $F$  be a field. Next we develop some divisibility theory in  $F[x]$ . Like in  $\mathbb{Z}$  we have

**Theorem 4.3** (Division algorithm). *Let  $f, g \in F[x]$ , with  $f \neq 0$ . Then there exist unique polynomials  $q, r \in F[x]$  such that*

$$g = fq + r, \quad \deg(r) < \deg(f).$$

*Proof.* Use “long division”. □

Here  $r$  is the *remainder of  $g$  divided by  $f$* . If  $r = 0$ , then we say that  $f$  *divides  $g$*  (or is a *factor of  $g$* ), and denote this by  $f \mid g$ .

**Example 4.4.** When dividing  $g(x) = x^5 + 2x^3 + 2x + 1$  by  $f(x) = 2x^2 + x + 2$  in  $\mathbb{F}_3[x]$ , the long division yields

$$x^5 + 2x^3 + 2x + 1 = (2x^2 + x + 2)(2x^3 + 2x^2 + x + 2) + x.$$

Hence, the remainder of  $g$  divided by  $f$  is  $x$ .

**Theorem 4.4.**  *$F[x]$  is a principal ideal domain, i.e. each ideal of  $F[x]$  is principal.*

*Proof.* Let  $I$  be an ideal of  $F[x]$ . If  $I = \{0\}$ , then  $I = (0)$ . Assume  $I \neq (0)$ , and let  $f$  be a nonzero polynomial of least degree contained in  $I$ . We claim that  $I = (f)$ . Let  $g \in I$ , and divide it by  $f$ :  $g = fq + r$ ,  $\deg(r) < \deg(f)$ . Now  $r = g - fq \in I$ , and by the minimality of  $\deg(f)$  we must have  $r = 0$ . Hence,  $I = (f)$ . □

**Remark 4.3.** If  $f$  is a generator of an ideal  $I \subseteq F[x]$ , then it is easy to see that  $f_n^{-1}f$  is a generator of  $I$  as well. Hence, each ideal  $I$  of  $F[x]$  is generated by a monic polynomial, and there is only one monic polynomial generating  $I$ .

**Theorem 4.5.** *Let  $h, g \in F[x]$ ,  $h \neq 0$ . There exists unique monic polynomial  $d \in F[x]$  satisfying the following two properties:*

- (1)  $d \mid h$  and  $d \mid g$ .
- (2) If  $c \in F[x]$  and  $c \mid h$  and  $c \mid g$ , then  $c \mid d$ .

*Proof.* The set  $(h, g) := \{ah + bg \mid a, b \in F[x]\}$  is easily seen to be a nonzero ideal of  $F[x]$ . Now, by Theorem 4.4,  $(h, g) = (f)$  for some  $f \in F[x]$ ,  $f \neq 0$ . If  $f_n$  is the

leading coefficient of  $f$ , then obviously  $(f) = (f_n^{-1}f)$ . We set  $d = f_n^{-1}f$  and show that  $d$  satisfies properties (1) and (2).

Since  $(d) = (h, g)$ ,  $h, g \in (d)$ , and therefore  $h = da$  and  $g = db$  for some  $a, b \in F[x]$  i.e.  $d \mid h$  and  $d \mid g$ .

Since  $(d) = (h, g)$ ,  $d \in (h, g)$  and therefore  $d = ah + bg$  for some  $a, b \in F[x]$ . Now, if  $c$  divides both  $h$  and  $g$ , then  $c \mid d$ .

If  $d'$  is another monic polynomial satisfying the properties (1) and (2), then  $(d') = (h, g) = (d)$ , and therefore  $d \mid d'$  and  $d' \mid d$ . It follows that  $d = d'$ .  $\square$

**Definition 4.2.** The polynomial  $d$  in Theorem 4.5 is called the *greatest common divisor* of  $h$  and  $g$  and denoted by  $\gcd(h, g)$ .

**Remark 4.4.** We saw in the proof of Theorems 4.5 we have the following equality of ideals:  $(\gcd(h, g)) = (h, g)$ .

The greatest common divisor of  $h \neq 0$  and  $g$  can be calculated by the *Euclidean algorithm* i.e. by using repeatedly the division algorithm:

$$\begin{aligned} g &= hq_1 + r_1, & \deg(r_1) &< \deg(h), \\ h &= r_1q_2 + r_2, & \deg(r_2) &< \deg(r_1), \\ r_1 &= r_2q_3 + r_3, & \deg(r_3) &< \deg(r_2), \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, & \deg(r_n) &< \deg(r_{n-1}), \\ r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

Let  $d = \gcd(h, g)$ . We observe that  $r_n \in (h, g) = (d)$ , and therefore  $d \mid r_n$ . On the other hand, we see that  $r_n \mid r_{n-1}$ , and  $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow \cdots \Rightarrow r_n \mid h \Rightarrow r_n \mid g$ . Hence, by Theorem 4.5,  $r_n \mid d$ . It now follows, that  $\gcd(h, g) = \ell^{-1}r_n$ .

**Example 4.5.** We calculate the greatest common divisor of the polynomials  $x^{12} + x^{10} + x^8 + x^3 + 1, x^8 + x^7 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_2[x]$  by using the Euclidean algorithm:

$$\begin{aligned} x^{12} + x^{10} + x^8 + x^3 + 1 &= (x^8 + x^7 + x^5 + x^4 + x^2 + x + 1)(x^4 + x^3 + x) \\ &\quad + x^7 + x^5 + x^3 + x^2 + x + 1 \end{aligned}$$

$$x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 = (x^7 + x^5 + x^3 + x^2 + x + 1)(x + 1) + x^6 + x^2 + x$$

$$x^7 + x^5 + x^3 + x^2 + x + 1 = (x^6 + x^2 + x)x + x^5 + x + 1$$

$$x^6 + x^2 + x = (x^5 + x + 1)x.$$

Hence,  $\gcd(x^{12} + x^{10} + x^8 + x^3 + 1, x^8 + x^7 + x^5 + x^4 + x^2 + 1) = x^5 + x + 1$ .

Next we define the analogue of a prime number.

**Definition 4.3.** A polynomial  $f \in F[x]$  is said to be *irreducible over  $F$*  if  $f$  has positive degree, and if  $f = bc$  for some  $b, c \in F[x]$ , then either  $b$  or  $c$  is a constant polynomial. If  $f$  is not irreducible, then it is called *reducible over  $F$* .

**Remark 4.5.** The irreducibility of a polynomial depends heavily on the field over which the polynomial is considered. For instance,  $x^2 + 1$  is irreducible over  $\mathbb{R}$ , but not over  $\mathbb{C}$  or  $\mathbb{F}_2$ .

**Example 4.6.** We show that  $x^2 + x + 1$  is irreducible over  $\mathbb{F}_2$ . If it was reducible, then its factors would be of degree one, say  $x^2 + x + 1 = (x + a)(x + b)$  with  $a, b \in \mathbb{F}_2$ . This implies  $x^2 + x + 1 = x^2 + (a + b)x + ab$ , which implies  $a + b = 1$  and  $ab = 1$ . But this is impossible.

**Lemma 4.2.** *Let  $f, b, c \in F[x]$ , with  $f$  irreducible. Then, if  $f \mid bc$ , then  $f \mid b$  or  $f \mid c$ .*

*Proof.* Assume that  $f$  does not divide  $b$ . Then, the greatest common divisor of  $f$  and  $b$  is 1. Now  $(1) = (f, b)$ , and therefore  $fu + bv = 1$ , for some  $u, v \in F[x]$ . We now get  $cfu + cbv = c$ , and since  $f$  divides the left hand side, it divides the right hand side as well.  $\square$

**Theorem 4.6** (Unique Factorization in  $F[x]$ ). *Let  $g \in F[x]$  be of positive degree. Then, there exist irreducible polynomials  $p_1, \dots, p_t \in F[x]$  and a constant  $u \in \mathbb{F}^*$  such that*

$$g(x) = up_1p_2 \cdots p_t.$$

*This factorization is unique apart from the order in which the factors occur.*

*Proof.* Assume that there exists polynomials of positive degree, which can not be written in the product of irreducible polynomials. Let  $g$  be one of them, and of the least degree. Now  $g$  can not be irreducible, and therefore  $g = ab$  for some  $a, b \in F[x]$  of positive degree. It follows that  $0 < \deg(a), \deg(b) < \deg(g)$ , and therefore  $a$  and  $b$  can be written as a product of irreducible polynomials. But then  $g$  can be written as a product of irreducible polynomials as well, and we have a contradiction.

The assertion concerning the uniqueness, follows easily from Lemma 4.2.  $\square$

#### 4.2. Residue class ring $F[x]/(f)$ .

Next we prove an important result, which shows that irreducible polynomials produce fields.

**Theorem 4.7.** *Let  $f \in F[x]$ . Then the residue class ring  $F[x]/(f)$  is a field if and only if  $f$  is irreducible over  $F$ .*

*Proof.* Assume that  $f$  is irreducible. We show that each nonzero element  $g + (f) \in F[x]/(f)$  has the multiplicative inverse. It then follows that  $F[x]/(f)$  is a field. Denote  $\bar{g} = g + (f)$ . If  $\bar{g} \neq \bar{0}$ , then  $g \notin (f)$ , which means that  $\gcd(g, f) = 1$ . Hence  $1 = gu + fv$  for some  $u, v \in F[x]$ , and therefore  $\bar{1} = \bar{g}\bar{u} = \bar{g}\bar{u}$ . Hence,  $u + (f)$  is the inverse of  $g + (f)$ .

Assume then that  $f$  is reducible, say  $f = ab$  for some  $a, b \in F[x]$  of positive degree. Now,  $0 < \deg(a), \deg(b) < \deg(f)$ , and therefore  $f$  divides neither  $a$  nor  $b$ . Hence,  $\bar{a}, \bar{b} \neq \bar{0}$ , but  $\bar{a}\bar{b} = \bar{f} = \bar{0}$ , which means that  $F[x]/(f)$  is not an integral domain and therefore not a field.  $\square$

**Remark 4.6.** By using the division algorithm, we see that a complete set of representatives for the residue classes modulo  $(f)$  is the set of polynomials of degree less than the degree  $n$  of  $f$ , and therefore

$$F[x]/(f) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (f) \mid a_0, \dots, a_{n-1} \in F\}.$$

In particular, if  $F = \mathbb{F}_p$ , then we observe that the number of elements in  $\mathbb{F}_p[x]/(f)$  is  $p^n$ . So:

*if  $f$  is irreducible over  $\mathbb{F}_p$  and of degree  $n$ , then  $\mathbb{F}_p[x]/(f)$  is a finite field of degree  $p^n$ .*

**Example 4.7.** We saw in Example 4.6 that  $f(x) = x^2 + x + 1$  is irreducible over  $\mathbb{F}_2$ . Hence,  $\mathbb{F}_2[x]/(f)$  is a finite field of order 4. Denote,  $\alpha = x + (p)$ ,  $0 = 0 + (p)$  and  $1 = 1 + (p)$ . Now  $\alpha^2 = \alpha + 1$ , and we have

$$\begin{aligned}\mathbb{F}_2[x]/(f) &= \{0 + (f), 1 + (f), x + (f), x + 1 + (f)\} \\ &= \{0, 1, \alpha, \alpha + 1 \mid \alpha^2 = \alpha + 1\} =: \mathbb{F}_4.\end{aligned}$$

The group tables of  $(\mathbb{F}_4, +)$  and  $(\mathbb{F}_4^*, \cdot)$  are

|              |              |              |              |              |
|--------------|--------------|--------------|--------------|--------------|
| +            | 0            | 1            | $\alpha$     | $1 + \alpha$ |
| 0            | 0            | 1            | $\alpha$     | $1 + \alpha$ |
| 1            | 1            | 1            | $1 + \alpha$ | $\alpha$     |
| $\alpha$     | $\alpha$     | $1 + \alpha$ | 0            | 1            |
| $1 + \alpha$ | $1 + \alpha$ | $\alpha$     | 1            | 0            |

|              |              |              |              |
|--------------|--------------|--------------|--------------|
| ·            | 1            | $\alpha$     | $1 + \alpha$ |
| 1            | 1            | $\alpha$     | $1 + \alpha$ |
| $\alpha$     | $\alpha$     | $1 + \alpha$ | 1            |
| $1 + \alpha$ | $1 + \alpha$ | 1            | $\alpha$     |

We end this section by considering polynomial functions.

**Definition 4.4.** Let  $f(x) = f_0 + f_1x + \cdots + f_nx^n$  be a polynomial over  $F$ . The *polynomial function induced by  $f(x)$* , is the function

$$f : F \rightarrow F, f(a) = f_0 + f_1a + \cdots + f_na^n.$$

**Example 4.8.** Different polynomials can induce the same polynomial function. Let e.g.  $f(x) = x, g(x) = x^2 \in \mathbb{F}_2[x]$ . Now  $f(x) \neq g(x)$ , but  $f(a) = g(a)$  for all  $a \in \mathbb{F}_2$  i.e. they induce the same polynomial function from  $\mathbb{F}_2$  onto  $\mathbb{F}_2$ .

**Definition 4.5.** An element  $b \in F$  is called a *root* (or a *zero*) of the polynomial  $f \in F[x]$ , if  $f(b) = 0$ .

**Theorem 4.8.** *An element  $b \in F$  is a root of a polynomial  $f \in F[x]$  if and only if  $x - b$  divides  $f(x)$ .*

*Proof.* By the division algorithm,  $f(x) = (x - b)g(x) + c$ , where  $c \in F$ . Now  $x - b$  divides  $f(x)$  if and only if  $c = 0$ . But  $c = f(b)$ , and the theorem follows.  $\square$

**Definition 4.6.** Let  $b \in F$  be a root of  $f \in F[x]$ . If  $k$  is a positive integer such that  $f(x)$  is divisible by  $(x - b)^k$ , but not  $(x - b)^{k+1}$ , then  $k$  is called the *multiplicity* of  $b$ . If  $k = 1$ , then  $b$  is called a *simple root* (or a *simple zero*) of  $f$ . If  $k \geq 2$ , then  $b$  is called a *multiple root* (or a *multiple zero*) of  $f$ .

**Lemma 4.3.** *Let  $f \in F[x]$ . If  $b_1, \dots, b_m$  are distinct roots of  $f$  with multiplicities  $k_1, \dots, k_m$ , then  $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$  divides  $f(x)$ .*

*Proof.* Each polynomial  $x - b_j$  is irreducible, and therefore each polynomial  $(x - b_j)^{k_j}$  occurs as a factor in the factorization of  $f$  as a product of irreducible polynomials. Hence,  $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$  appears in the factorization as well.  $\square$

**Theorem 4.9.** *Let  $f$  be polynomial over  $F$  of degree  $n$ . Then,  $f$  has at most  $n$  roots in  $F$ .*

*Proof.* Let  $b_1, \dots, b_m$  be the roots of  $f$  in  $F$ , and let  $k_1, \dots, k_m$  be their multiplicities. Now, by Lemma 4.3,  $f(x) = (x - b_1)^{k_1} \cdots (x - b_m)^{k_m} g(x)$  and therefore  $m \leq k_1 + \cdots + k_m \leq n$ .  $\square$

The irreducibility of a polynomial  $f$  over  $F$  is equivalent to the non-existence of a root of  $f$  in  $F$ , if the degree of  $f$  is small enough.

**Theorem 4.10.** *Any polynomial  $f \in F[x]$  of degree 2 or 3 is irreducible in  $F[x]$  if and only if  $f$  has no root in  $F$ .*

*Proof.* If  $f$  has a root in  $F$ , then  $f$  is reducible, by Theorem 4.8. Assume  $f$  has not a root in  $F$ . Then,  $f$  can not have a factor of degree one, again by Theorem 4.8. Hence, if  $\deg(f) = 2$ , it must be irreducible. If  $\deg(f) = 3$  and  $f$  does not have a factor of degree one, then it can not have a factor of degree two either, and so  $f$  is irreducible in this case too.  $\square$

**Example 4.9.** The assumption concerning the degree is necessary. For instance,  $x^4 + 2x^2 + 1$  has no zeros in  $\mathbb{R}$ , but it is reducible over  $\mathbb{R}$ :  $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ .

**Example 4.10.** We find the irreducible polynomials over  $\mathbb{F}_2$  of degree three. Let  $f(x) = x^3 + ax^2 + bx + c \in \mathbb{F}_2[x]$ . Now, by Theorem 4.10,  $f$  is irreducible if and only if  $f(0) = f(1) = 1$  i.e.  $c = 1$  and  $a + b = 1$ . Hence, the irreducible polynomials over  $\mathbb{F}_2$  of degree three are  $x^3 + x^2 + 1$  and  $x^3 + x + 1$ .

## 5. FIELD EXTENSIONS

**Definition 5.1.** Let  $F$  be a field. A subset  $K$  of  $F$  is called a *subfield* of  $F$ , if it is a field under the operations of  $F$ . If  $K$  is a subfield of  $F$ , then  $F$  is called an *extension (field)* of  $K$ . In this case the phrase *field extension*  $F/K$  is also used.

**Lemma 5.1** (Subfield Criterion). *Let  $K$  be a subset of a field  $F$ . Then,  $K$  is a subfield of  $F$  if and only if the following three properties hold:*

- (1)  $K$  contains at least two elements,
- (2)  $a - b \in K$  for all  $a, b \in K$ ,
- (3)  $ab^{-1} \in K$  for all  $a, b \in K, b \neq 0$ .

*Proof.* If  $K$  is a subfield of  $F$ , then the properties are satisfied by the definition of a field. Assume next that  $K$  satisfies the properties. By (1),  $K$  is non-empty. Now, (2) implies that  $(K, +)$  is a subgroup of  $(F, +)$ , and (3) implies that  $(K \setminus \{0\}, \cdot)$  is a subgroup of  $(F \setminus \{0\}, \cdot)$  (by the subgroup criterion). It remains to show that the distributive laws hold in  $K$ . But this is obvious, because they hold in  $F$ .  $\square$

**Lemma 5.2.** *The intersection of all subfields of a field  $F$  is a subfield of  $F$ .*

*Proof.* Since all subfields of  $F$  has at least 0 and 1, so do their intersection  $K$ . Let  $a, b \in K$ . Now,  $a, b$  are in each subfield of  $F$ , and therefore  $a - b$  belongs to each subfield of  $F$ , and if  $b \neq 0$  then also  $ab^{-1}$  belongs to each subfield of  $F$ .  $\square$

**Definition 5.2.** The intersection of all subfields of a field  $F$  is called the *prime field* of  $F$ .

**Theorem 5.1.** *Let  $F$  be a field. If  $\text{char}(F) = 0$ , then the prime field of  $F$  is isomorphic to  $\mathbb{Q}$ . Otherwise, it is isomorphic to  $\mathbb{F}_p$ , where  $p = \text{char}(F)$ .*

*Proof.* Let  $K$  be the prime field of  $F$ . Then, the set  $R$  of all integer multiples of the identity element 1 is a subring of  $K$ . But since  $K$  is a field, all the fractions  $a/b := ab^{-1}$  with  $a, b \in R, b \neq 0$ , are in  $K$  too.

Hence, if  $\text{char}(F) = 0$ , then  $K$  contains (and is contained to) a field isomorphic to  $\mathbb{Q}$ , and if  $\text{char}(F) = p$ , then it contains (and is contained to) a field isomorphic to  $\mathbb{F}_p$ .  $\square$

**Definition 5.3.** Let  $K$  be the subfield of a field  $F$ , and let  $M$  be a subset of  $F$ . The intersection  $K(M)$  of all the subfields of  $F$  containing both  $K$  and  $M$  is called the extension field of  $K$  obtained by *adjoining* the element of  $M$  to  $K$ . If  $M$  is finite, say  $M = \{a_1, \dots, a_n\}$ , then we write  $K(a_1, \dots, a_n) := K(M)$ . The extension  $K(a)/K$  is said to be *simple* and  $a$  is a *defining element* of the extension.

**Remark 5.1.** Note that  $K(M)$  is the “smallest” subfield of  $F$  containing both  $K$  and  $M$ . Moreover, since  $K(a)$  is a field it contains elements  $f(a)$  where  $f \in K[x]$ .

We are especially interested in the extensions  $K(a)/K$  where  $a$  is a root of a polynomial over  $K$ .

**Definition 5.4.** Let  $K$  be a subfield of  $F$ . An element  $a \in F$  is said to be *algebraic* over  $K$ , if  $f(a) = 0$  for some  $f \in K[x] \setminus \{0\}$ . Extension  $F/K$  is said to be *algebraic (extension)* if every element of  $F$  is algebraic over  $K$ .

**Theorem 5.2.** Let  $K$  be a subfield of  $F$ , and let  $a \in F$ . If  $a$  is algebraic over  $K$ , then there exists unique monic irreducible polynomial  $f$  over  $K$  such that  $f(a) = 0$ .

*Proof.* Obviously the set  $I := \{g(x) \in K[x] \mid g(a) = 0\}$  is an ideal of  $K[x]$ . By Remark 4.3, it is generated by a monic unique polynomial  $f(x)$  of the least positive degree contained in  $I$ . If  $f = gh$ , for some  $g, h \in K[x]$ , then  $0 = f(a) = g(a)h(a)$ , and therefore either  $f(a) = 0$  or  $g(a) = 0$ . By the minimality of the degree of  $f$ , we have  $g \in K^*$  or  $h \in K^*$  implying the irreducibility of  $f$ .  $\square$

**Definition 5.5.** Let  $a \in F$  be algebraic over  $K$ . The monic irreducible polynomial  $f$  over  $K$  satisfying  $f(a) = 0$  is called the *minimal polynomial of  $a$  over  $K$* . The degree of  $f$  is called the *degree of  $a$* .

**Example 5.1.** We find the minimal polynomial of  $a = \sqrt[3]{3} + 1$  over  $\mathbb{Q}$ . Now  $a - 1 = \sqrt[3]{3}$  and it follows that  $a^3 - 3a^2 + 3a - 1 = 3$ . Hence,  $a$  is a root of  $f(x) = x^3 - 3x^2 + 3x - 4$ . This monic polynomial of degree 3 has no roots in  $\mathbb{Q}$ , and is therefore irreducible. Hence  $f(x)$  is the minimal polynomial of  $\sqrt[3]{3} + 1$  over  $\mathbb{Q}$ .

Let  $K$  be a subfield of  $F$ . We can consider  $F$  as a vector space over  $K$ . The “vectors” are the elements of  $F$ , and the scalars are the elements of  $K$ .

**Lemma 5.3.** Let  $K$  be a subfield of  $F$ . Then,  $F$  is a vector space over  $K$  i.e. for all  $\alpha, \beta \in F$ , and all  $r, s \in K$  we have

- (1)  $(F, +)$  is an abelian group,
- (2)  $r(\alpha + \beta) = r\alpha + r\beta$ ,
- (3)  $(r + s)\alpha = r\alpha + s\alpha$ ,
- (4)  $(rs)\alpha = r(s\alpha)$ ,

$$(5) \quad 1\alpha = \alpha.$$

*Proof.* The lemma follows immediately by the definition of a field.  $\square$

**Definition 5.6.** Field extension  $F/K$  is called *finite*, if  $F$  is a finite dimensional vector space over  $K$ . The dimension of the vector space  $F$  over  $K$  is then called the *degree* of  $F$  over  $K$ , and denoted by the symbol  $[F : K]$ .

**Theorem 5.3.** *Every finite field extension is algebraic.*

*Proof.* Let  $F/K$  be a finite field extension with  $n = [F : K]$ , and let  $\alpha \in F$ . Now, the  $n+1$  elements  $1, \alpha, \dots, \alpha^n$  are linearly dependent over  $K$  i.e. there exist elements  $a_0, \dots, a_n \in K$  such that at least one of them is nonzero and  $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ . This means that  $\alpha$  is algebraic over  $K$ .  $\square$

**Lemma 5.4.** *Let  $F/M$  and  $M/K$  be finite extensions. Then  $F/K$  is finite, and*

$$[F : K] = [F : M][M : K].$$

*Proof.* Let  $n = [F : M]$  and  $m = [M : K]$ , and let  $\{\alpha_1, \dots, \alpha_n\}$  be a basis of  $F$  over  $M$  and  $\{\beta_1, \dots, \beta_m\}$  a basis of  $M$  over  $K$ . Now, it is easy to see that the set  $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$  is basis of  $F$  over  $K$ .  $\square$

Next theorem describes the key properties of simple field extensions.

**Theorem 5.4.** *Let  $\alpha \in F$  be algebraic of degree  $n$  over  $K$ , and let  $f$  be the minimal polynomial of  $\alpha$  over  $K$ . Then*

- (1)  $K(\alpha)$  is isomorphic to  $K[x]/(f)$ .
- (2)  $[K(\alpha) : K] = n$  and  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a basis of  $K(\alpha)/K$ .
- (3) Every  $\beta \in K(\alpha)$  is algebraic over  $K$ , and its degree over  $K$  is a factor of  $n$ .

*Proof.* (1) Obviously function  $\psi : K[x] \rightarrow K(\alpha)$ ,  $\psi(g(x)) = g(\alpha)$  is a ring homomorphism. By the proof of Theorem 5.2 its kernel is an ideal of  $K[x]$  generated by the minimal polynomial  $f$  of  $\alpha$ . Since  $f$  is irreducible,  $K[x]/(f)$  is a field, and now by the isomorphism theorem for rings, it is isomorphic to  $\text{im } \psi$ . But  $K \subseteq \text{im } \psi$  and  $\alpha \in \text{im } \psi$ , and therefore, by the definition of  $K(\alpha)$ , we have  $\text{im } \psi = K(\alpha)$ . This proves (1).

(2) As we saw above, each element  $\beta$  in  $K(\alpha)$  is of the form  $\beta = g(\alpha)$  for some  $g \in K[x]$ . By the division algorithm  $g = fq + r$  for some  $q, r \in K[x]$  with  $\deg(r) \leq n-1$ .

Hence,  $g(a) = f(a)q(a) + r(a) = r(a)$ , and therefore  $\{1, \alpha, \dots, \alpha^{n-1}\}$  spans  $K(\alpha)$  over  $K$ . Assume  $\sum_{i=0}^{n-1} a_i \alpha^i = 0$  for some  $a_0, \dots, a_n \in K$ . Now,  $\sum_{i=0}^{n-1} a_i x^i$  is in  $\ker \psi$ , and is therefore a multiple of  $f$ . But  $\deg(f) = n$ , and therefore  $a_0 = \dots = a_{n-1} = 0$  i.e.  $\{1, \alpha, \dots, \alpha^{n-1}\}$  is linearly independent over  $K$ . This proves (2).

(3) Let  $\beta \in K(\alpha)$ . Since  $K(\alpha)/K$  is finite,  $\beta$  is algebraic over  $K$  by Theorem 5.3. By Lemma 5.4,  $[K(\beta) : K] = [K(\alpha) : K]/[K(\alpha) : K(\beta)]$ , and by (2), the degree of  $\beta$  is equal to  $[K(\beta) : K]$ . This proves (3).  $\square$

Above we considered simple algebraic extensions  $K(\alpha)/K$  where  $\alpha$  is an element of a given field  $F$ . But how to construct simple algebraic extensions over  $K$  without reference to a previously given larger field?

**Theorem 5.5.** *Let  $f \in K[x]$  be irreducible and monic over the field  $K$ . Then there exists an algebraic extension  $K(\alpha)/K$  such that  $f$  is the minimal polynomial of  $\alpha$ .*

*Proof.* Let  $n = \deg(f)$ . We know that the residue class ring

$$K[x]/(f) = \{a_0x + a_1x + \dots + a_{n-1}x^{n-1} + (f) \mid a_0, \dots, a_{n-1} \in K\}$$

is a field. Set  $\alpha := x + (f)$  and  $a := a + (f)$  for all  $a \in K$ . Now, by the definition of addition and multiplication of residue classes modulo  $(f)$ , we get

$$K[x]/(f) \simeq \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in K\} = K(\alpha),$$

where the equality follows from Theorem 5.4 (2). Moreover,

$f(\alpha) = f_0 + f_1\alpha + \dots + \alpha^{n-1} = f_0 + f_1x + \dots + x^{n-1} + (f) = f(x) + (f) = 0 + (f) = 0$ , and since  $f$  is irreducible and monic, it is the minimal polynomial of  $\alpha$ .  $\square$

By Theorem 5.5, for each irreducible polynomial  $f \in K[x]$  there always exists an extension field  $F$  of  $K$  such that  $f$  has a root in  $F$ . Based on this we shall see, that there exist an extension field of  $K$  over which  $f$  factors to the irreducible factors of degree one, and this extension field is unique up to the isomorphism.

Let  $\psi$  be a field isomorphism from  $K$  onto  $K'$ , and let  $f(x) = f_0 + \dots + f_n x^n \in K[x]$ . By the notation  $\psi(f)$  we mean the polynomial  $\psi(f_0) + \dots + \psi(f_n)x^n \in K'[x]$ .

**Lemma 5.5.** *Let  $\psi$  be a field isomorphism from  $K$  onto  $K'$ , and let  $f \in K[x]$  be a monic irreducible polynomial over  $K$ . Let  $\alpha$  be a zero of  $f$  and let  $\beta$  be a zero of  $\psi(f)$ . Then, the fields  $K(\alpha)$  and  $K'(\beta)$  are isomorphic.*

*Proof.* We first show that  $\psi(f)$  is irreducible over  $K'$ . By Theorem 5.4 (1) it is then enough to show that the fields  $K[x]/(f)$  and  $K'[x]/(\psi(f))$  are isomorphic.

It is easy to see that  $\psi$  is actually a ring isomorphism from  $K[x]$  onto  $K'[x]$ . It follows that, if  $\psi(f) = gh$  for some  $g, h \in K'[x]$  then  $f = \psi^{-1}(g)\psi^{-1}(h)$ . Hence,  $\psi(f)$  is irreducible.

Obviously  $\psi' : K[x] \rightarrow K'[x]/(\psi(f))$ ,  $\psi'(g) = \psi(g) + (\psi(f))$  is a surjective ring homomorphism, and the kernel of  $\psi'$  consists of the polynomials  $g$  such that  $\psi(f) \mid \psi(g)$  equivalently  $f \mid g$ . Hence,  $K[x]/(f)$  and  $K'[x]/(\psi(f))$  are isomorphic by the isomorphism theorem for rings.  $\square$

**Definition 5.7.** Let  $f \in K[x]$  be of positive degree, and let  $F$  be an extension field of  $K$ . Then  $f$  is said to be *split in  $F$* , if there exist  $\alpha_1, \dots, \alpha_n \in F$  such that

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where  $a$  is the leading coefficient of  $f$ . If  $f$  splits in  $F$  and  $F = K(\alpha_1, \dots, \alpha_n)$ , then  $F$  is called a *splitting field* of  $f$  over  $K$ .

**Theorem 5.6.** For each  $f \in K[x]$  of positive degree there exists a splitting field of  $f$  over  $K$ . Any two splitting fields of  $f$  over  $K$  are isomorphic.

*Proof.* Let  $f = g_1^{k_1} h_1$  where  $g_1, h_1 \in K[x]$ ,  $g_1$  irreducible, and  $g_1 \nmid h_1$ . Now,  $g_1$  has a zero  $\alpha_1$  in  $K(\alpha_1)$  and therefore  $f(x) = (x - \alpha_1)^{k_1} t_1(x)$  for some  $t_1 \in K(\alpha_1)[x]$  with  $\deg(t_1) < \deg(f)$ . If  $\deg(t_1) = 0$ , then we are done. Otherwise, we write  $t_1 = g_2^{k_2} h_2$  where  $g_2, h_2 \in K(\alpha_1)[x]$ ,  $g_2$  irreducible, and  $g_2 \nmid h_2$ . Now,  $g_2$  has a zero  $\alpha_2$  in  $K(\alpha_1, \alpha_2)$  and therefore  $f(x) = (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} t_2(x)$  for some  $t_2 \in K(\alpha_1)[x]$  with  $\deg(t_2) < \deg(t_1)$ . Continuing in this way, we finally get  $f(x) = a(x - \alpha_1)^{k_1} \cdots (x - \alpha_m)^{k_m} \in K(\alpha_1, \dots, \alpha_m)$  i.e.  $K(\alpha_1, \dots, \alpha_m)$  is a splitting field of  $f$ .

Let  $K(\alpha'_1, \dots, \alpha'_n)$  be another splitting field of  $f$  over  $K$ , and assume  $m \leq n$ . Choose  $\psi$  in Lemma 5.5 be the trivial isomorphism  $\psi : K \rightarrow K$ ,  $\psi(c) = c$ . Now,  $K(\alpha_1) \simeq K(\alpha'_1)$ . Next choose  $K$  to be  $K(\alpha_1)$  and  $K'$  to be  $K(\alpha'_1)$  in Lemma 5.5, and we get isomorphism  $K(\alpha_1, \alpha_2) \simeq K(\alpha'_1, \alpha'_2)$ . Continuing in this way, we obtain an isomorphism from  $K(\alpha_1, \dots, \alpha_m)$  onto  $K(\alpha'_1, \dots, \alpha'_m)$  which maps each  $\alpha_i$  to  $\alpha'_i$ . If  $m < n$ , then  $f$  splits in a proper subfield  $K(\alpha'_1, \dots, \alpha'_n)$ , which is impossible by the definition of a splitting field. Hence,  $m = n$  and the proof is complete.  $\square$

We end this section by giving a criterion whether a polynomial  $f$  has a multiple root in its splitting field.

**Definition 5.8.** Let  $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_nx^n$  be a polynomial over  $K$ . The (formal) derivative of  $f$  is the polynomial  $f'(x) = f_1 + 2f_2x + \cdots + nf_nx^{n-1}$ .

**Lemma 5.6.** Let  $f, g \in K[x]$ . Then

- (1)  $(f + g)' = f' + g'$ .
- (2)  $(fg)' = f'g + fg'$ .

*Proof.* Exercise. □

**Theorem 5.7.** Let  $f \in K[x]$  and let  $\alpha$  be a root of  $f$  in its splitting field over  $K$ . Then,  $\alpha$  is a simple root of  $f(x)$  if and only if  $f'(\alpha) \neq 0$ .

*Proof.* Let  $F$  be the splitting of  $f$  over  $K$ . Write  $f(x) = (x - \alpha)^k g(x)$  where  $g(x) \in F[x]$ ,  $(x - \alpha) \nmid g(x)$ , and  $k$  is a positive integer.

Now  $f'(x) = k(x - \alpha)^{k-1}g(x) + (x - \alpha)^k g'(x)$ . If  $\alpha$  is simple, then  $k = 1$  and  $f'(\alpha) = g(\alpha) \neq 0$ . If  $\alpha$  is multiple, then  $k > 1$  and  $f'(\alpha) = 0$ . □

## 6. FINITE FIELDS

In this section we characterize the finite fields. First we show that the number of elements in a finite field is a prime power.

**Lemma 6.1.** Let  $F$  be a finite field containing a subfield  $K$  with  $q$  elements. Then  $F$  has  $q^m$  elements, where  $m = [F : K]$ .

*Proof.* Since  $F$  is a vector space over  $K$  of dimension  $m$ , each element  $\alpha \in F$  can be uniquely represented in the form  $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$ , where  $\{\alpha_1, \dots, \alpha_m\}$  is a fixed basis of  $F$  over  $K$ , and  $a_1, \dots, a_m \in K$ . Here each “scalar”  $a_i$  can be chosen in exactly  $q$  ways, and therefore  $|F| = q^m$ . □

**Theorem 6.1.** Let  $F$  be a finite field. Then  $F$  has  $p^n$  elements, where the prime  $p$  is the characteristic of  $F$  and  $n$  is the degree of  $F$  over its prime field.

*Proof.* Since  $F$  is finite, its characteristic is a prime  $p$  by Corollary 3.2. Now, by Theorem 5.1, the prime field of  $F$  is isomorphic to  $\mathbb{F}_p$ , and Lemma 6.1 now completes the proof. □

Next we show that there exists a finite field of order  $p^n$  for each prime  $p$  and for each positive integer  $n$ . We begin with a lemma, which is a generalization of Fermat's little theorem.

**Lemma 6.2.** *If  $F$  is a finite field with  $q$  elements, then  $a^q = a$  for all  $a \in F$ .*

*Proof.* Obviously  $a^q = a$  if  $a = 0$ . If  $a \neq 0$  then  $a^{q-1} = 1$ , since  $F^*$  is a group of order  $q - 1$ . This implies that  $a^q = a$ .  $\square$

**Theorem 6.2.** *For every prime  $p$  and every positive integer  $n$  there exists a finite field with  $p^n$  elements.*

*Proof.* Let  $q = p^n$  and let  $f(x) = x^q - x$ . Since  $f'(x) = -1$ , each root of  $f$  is simple in the splitting field  $F$  of  $f$  over  $\mathbb{F}_p$ . It now follows from Theorem 4.9 that  $f$  has exactly  $q$  roots in  $F$ . We show that the roots of  $f$  form a subfield of  $F$ . First,  $0, 1$  are roots of  $f$ . Second, if  $\alpha, \beta$  are roots of  $f$ , then, since  $\text{char}(F) = p$ , we have  $f(\alpha - \beta) = (\alpha - \beta)^q - (\alpha - \beta) = \alpha^q - \alpha - (\beta^q - \beta) = 0 - 0 = 0$  by Lemma 6.2. Third, if  $\beta \neq 0$ , then  $f(\alpha\beta^{-1}) = (\alpha\beta^{-1})^q - (\alpha\beta^{-1}) = 0$  by Lemma 6.2. Now, by the subfield criterion, the roots of  $f$  form a field with  $q$  elements.  $\square$

Since the splitting field of a polynomial over  $\mathbb{F}_p$  is unique up to the isomorphisms, next theorem shows that for a given prime  $p$  and for a given positive integer  $n$  there exists (essentially) only one finite field with  $q = p^n$  elements.

**Theorem 6.3.** *Let  $F$  be a finite field with  $q$  elements, and let  $K$  be a subfield of  $F$ . Then, the polynomial  $x^q - x$  factors in  $F[x]$  as*

$$x^q - x = \prod_{a \in F} (x - a).$$

*Moreover,  $F$  is the splitting field of  $x^q - x$  over  $K$ .*

*Proof.* The polynomial  $x^q - x$  has at most  $q$  roots in  $F$ , and now by Lemma 6.2, its roots are exactly the  $q$  elements of  $F$ . Hence,  $x^q - x$  splits over  $F$  in the given manner, and it cannot split in any smaller field.  $\square$

**Definition 6.1.** From now on we denote by  $\mathbb{F}_q$  the finite field with  $q$  elements.

Next we characterize the subfields of  $\mathbb{F}_q$ .

**Theorem 6.4.** *Every subfield of  $\mathbb{F}_{p^n}$  has  $p^m$  elements, where  $m$  is a positive factor of  $n$ . Conversely, if  $m$  is a positive factor of  $n$ , then there is exactly one subfield of  $\mathbb{F}_{p^n}$  with  $p^m$  elements.*

*Proof.* Let  $K$  be a subfield of  $\mathbb{F}_{p^n}$ . By Theorem 6.1,  $K$  has  $p^m$  elements for some positive integer  $m$ . By Lemma 6.1,  $p^n = p^{mt}$  where  $t = [\mathbb{F}_{p^n} : K]$ . Hence,  $m$  is a factor of  $n$ .

Conversely, let  $m$  be a positive factor of  $n$ . Now,  $p^m - 1$  divides  $p^n - 1$ , and therefore  $x^{p^m} - 1$  divides  $x^{p^n} - 1$ . Since  $\mathbb{F}_{p^n}$  is the splitting field of  $x^{p^n} - x$  by Theorem 6.3, polynomial  $x^{p^m} - x$  splits in  $\mathbb{F}_{p^n}$ . Now, by the proof of Theorem 6.2, the roots of  $x^{p^m} - x$  in  $\mathbb{F}_{p^n}$  form a subfield with  $p^m$  elements. On the other hand, if  $K$  is any subfield of  $\mathbb{F}_{p^n}$  with  $p^m$  elements, then its elements are the roots of  $x^{p^m} - x$ . But this polynomial has exactly  $p^m$  roots, and so there is only one subfield with  $p^m$  elements.  $\square$

**Example 6.1.** The subfields of  $\mathbb{F}_{2^{20}}$  are  $\mathbb{F}_2$ ,  $\mathbb{F}_{2^2}$ ,  $\mathbb{F}_{2^4}$ ,  $\mathbb{F}_{2^5}$ ,  $\mathbb{F}_{2^{10}}$  and  $\mathbb{F}_{2^{20}}$ .

Next we prove an important fact.

**Theorem 6.5.** *The multiplicative group  $\mathbb{F}_q^*$  of a finite field  $\mathbb{F}_q$  is cyclic.*

*Proof.* We may assume that  $q > 3$ . Let  $q - 1 = p_1^{k_1} \cdots p_m^{k_m}$  be the canonical prime decomposition of  $q - 1$ . For each  $i = 1, \dots, m$ , let  $h_i = (q - 1)/p_i$ . The polynomial  $x^{h_i} - 1$  has at most  $h_i$  roots, and therefore there exists  $a_i \in \mathbb{F}_q^*$  which is not a root of  $x^{h_i} - 1$ . Let  $b_i = a_i^{(q-1)/p_i^{k_i}}$ . The order of  $b_i$  is a factor of  $p_i^{k_i}$ . On the other hand,  $b_i^{p_i^{k_i-1}} = a_i^{(q-1)/p_i} \neq 1$ , and therefore the order of  $b_i$  is  $p_i^{k_i}$ . We show that  $b := b_1 \cdots b_m$  generates  $\mathbb{F}_q^*$ .

Assume on the contrary that the order of  $b$  is a non-trivial factor of  $q - 1$ , which means that it is a factor of  $(q - 1)/p_i$  for at least one  $i = 1, \dots, m$ , say for  $i = 1$ . Now,

$$1 = b^{(q-1)/p_1} = b_1^{(q-1)/p_1} b_2^{(q-1)/p_1} \cdots b_m^{(q-1)/p_1} = b_1^{(q-1)/p_1} \cdot 1 \cdots 1 = b_1^{(q-1)/p_1},$$

which implies that the order  $p_1^{k_1}$  of  $b_1$  is a factor of  $(q - 1)/p_1$ , which is impossible.  $\square$

**Definition 6.2.** A generator of the cyclic group  $\mathbb{F}_q^*$  is called a primitive element of  $\mathbb{F}_q$ .

**Example 6.2.** Let  $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$  where  $\alpha$  is a root of the irreducible polynomial  $f(x) = x^4 + x^3 + x^2 + x + 1$ . Now the order of  $\alpha$  is either 3, 5 or 15. Obviously,  $\alpha^3 \neq 1$  but  $\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1$ . On the other hand, the order of an element  $\beta$  in  $\mathbb{F}_4 \setminus \mathbb{F}_2$  is three, and therefore, by the proof of Theorem 6.5,  $\alpha\beta$  is a primitive element of  $\mathbb{F}_{16}$ .

We next find such a  $\beta$ . We observe that the degree of  $\beta$  over  $\mathbb{F}_2$  is 2, and therefore it is a root of  $x^2 + x + 1$  in  $\mathbb{F}_{16}$ . So, it is enough to find  $a_0, a_1, a_2, a_3 \in \mathbb{F}_2$  such that

$$(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3)^2 + a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + 1 = 0,$$

equivalently,

$$a_0 + a_1\alpha^2 + a_2\alpha^4 + a_3\alpha^6 + a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + 1 = 0.$$

Here,  $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$  and  $\alpha^6 = \alpha\alpha^5 = \alpha$ , and therefore we have

$$a_2 + 1 + (a_1 + a_2 + a_3)\alpha + a_1\alpha^2 + (a_2 + a_3)\alpha^3 = 0,$$

equivalently,  $a_2 = 1$ ,  $a_1 = 0$ ,  $a_3 = 1$ . Hence, we may choose  $\beta = \alpha^2 + \alpha^3$  or  $\beta = 1 + \alpha^2 + \alpha^3$ .

**Theorem 6.6.** Let  $\mathbb{F}_q$  be a subfield of the finite field  $\mathbb{F}_{q^n}$ . Then,  $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$  where  $\gamma$  is a primitive element of  $\mathbb{F}_{q^n}$ .

*Proof.* Since  $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$  and  $\gamma \in \mathbb{F}_{q^n}$ , we have  $\mathbb{F}_q(\gamma) \subseteq \mathbb{F}_{q^n}$ . On the other hand,  $\mathbb{F}_q(\gamma)$  is a field and therefore it contains 0 and all the powers of  $\gamma$ . Hence,  $\mathbb{F}_{q^n} \subseteq \mathbb{F}_q(\gamma)$ .  $\square$

**Corollary 6.1.** Let  $\mathbb{F}_q$  be a finite field and let  $n$  be a positive integer. Then, there exists an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$ .

*Proof.* Let  $\gamma$  be the primitive element of  $\mathbb{F}_{q^n}$ . Then  $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$  by Theorem 6.6, and the minimal polynomial of  $\gamma$  over  $\mathbb{F}_q$  is of degree  $n$  by Theorem 5.4 and irreducible by the definition.  $\square$

**Definition 6.3.** The minimal polynomial of a primitive element of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  is called a *primitive polynomial* over  $\mathbb{F}_q$ .

We end this section by describing the roots of an irreducible polynomial over a finite field.

**Lemma 6.3.** Let  $f$  be an irreducible polynomial over  $\mathbb{F}_q$  of degree  $m$ . Then  $f(x)$  divides  $x^{q^n} - x$  if and only if  $m$  divides  $n$ .

*Proof.* Let  $\alpha$  be a root of  $f$  in its splitting field over  $\mathbb{F}_q$ . Assume first that  $f(x) \mid (x^{q^n} - x)$ . Now  $\alpha^{q^n} = \alpha$  which means that  $\alpha \in \mathbb{F}_{q^n}$  by Theorem 6.3. It follows that  $\mathbb{F}_q(\alpha)$  is a subfield of  $\mathbb{F}_{q^n}$ , and therefore the degree  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$  is a factor of  $n$  by Lemma 5.4. But  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$  by Theorem 5.4.

Assume then that  $m$  is a factor of  $n$ . Now  $\mathbb{F}_{q^n}$  has the subfield  $\mathbb{F}_{q^m}$  by Theorem 6.4. On the other hand  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$  and therefore  $\alpha \in \mathbb{F}_{q^m}$ . Now  $\alpha$  is a zero of  $x^{q^m} - x$  and therefore  $f(x) \mid (x^{q^m} - x)$  by the proof of Theorem 5.2.  $\square$

**Theorem 6.7.** *If  $f$  is an irreducible polynomial over  $\mathbb{F}_q$  of degree  $m$ , then  $f$  has a root  $\alpha$  in  $\mathbb{F}_{q^m}$ . Moreover, all the roots of  $f$  are simple and they are  $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ .*

*Proof.* Let  $\alpha$  be a root of  $f$  in its splitting field over  $\mathbb{F}_q$ . The degree  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$  and therefore  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ . It follows from Lemma 6.2 that  $\alpha^{q^i}$  is a root of  $f$  for all non-negative integers  $i$ :

$$f(\alpha^{q^i}) = \sum_{j=0}^m f_j \alpha^{jq^i} = \left( \sum_{j=0}^m f_j \alpha^j \right)^{q^i} = f(\alpha)^{q^i} = 0.$$

Since the degree of  $f$  is  $m$ , it remains to prove that  $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$  are distinct. If  $\alpha^{q^i} = \alpha^{q^j}$  for some  $0 \leq i < j \leq m-1$ , then by rising this identity to the power of  $q^{m-i}$  we get

$$\alpha = \alpha^{q^m} = \alpha^{q^{m+j-i}}.$$

It follows that  $f(x)$  is a divisor of  $x^{q^{m+j-i}} - x$  and now, by Lemma 6.3,  $m$  divides  $m+j-i$ . But is possible only if  $m$  divides  $j-i$  which is impossible, since  $1 \leq j-i \leq m-1$ .  $\square$

**Definition 6.4.** Let  $\alpha \in \mathbb{F}_{q^m}$ . Then, the elements  $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$  are the *conjugates* of  $\alpha$  over  $\mathbb{F}_q$ .

**Remark 6.1.** If  $\alpha \in \mathbb{F}_{q^m}$  and its degree over  $\mathbb{F}_q$  is  $d \mid m$ . Then, the conjugates of  $\alpha$  over  $\mathbb{F}_q$  are the elements  $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$ , each repeated with  $m/d$  times.

**Theorem 6.8.** *Let  $\alpha \in \mathbb{F}_{q^m}$ . Then, the conjugates of  $\alpha$  over  $\mathbb{F}_q$  has the same order in  $\mathbb{F}_q^*$ .*

*Proof.* By theory of cyclic groups.  $\square$

**Example 6.3.** Let  $\gamma \in \mathbb{F}_{16}$  be a root of  $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ . Then, the conjugates of  $\gamma$  over  $\mathbb{F}_2$  are  $\gamma, \gamma^2, \gamma^4 = \gamma + 1$  and  $\gamma^8 = \gamma^2 + 1$ . Since  $f$  is a primitive

polynomial over  $\mathbb{F}_2$ , the conjugates of  $\gamma$  over  $\mathbb{F}_2$  are primitive elements of  $\mathbb{F}_{16}$ , by Theorem 6.8.

The conjugates of  $\gamma$  over  $\mathbb{F}_4$  are  $\gamma$  and  $\gamma^4$ . Hence, the minimal polynomial of  $\gamma$  over  $\mathbb{F}_2$  is  $(x + \gamma)(x + \gamma^4) = x^2 + (\gamma + \gamma^4)x + \gamma^5 = x^2 + x + \gamma^2 + \gamma$ .

## 7. A BRIEF INTRODUCTION TO THE ERROR CORRECTING BLOCK CODES

Assume we would like to send information, expressed as a finite sequence of symbols, over a noisy channel. Then errors may (or will) occur and of course we would like to correct, or at least detect, the errors in the receiving end of the channel. The main idea is to transmit *redundant* information; that is, one extends the sequence of message symbols to a longer sequence in a systematic manner. We call such a systematic extension of a message as *encoding*.

Let  $\mathbb{F}_q$  be a finite field. We assume that the *message word* is a vector  $(a_1, \dots, a_k) \in \mathbb{F}_q^k$  and it is encoded into a code word  $(c_1, \dots, c_n) \in \mathbb{F}_q^n$  where  $n > k$ . In this context a function from  $\mathbb{F}_q^k$  into  $\mathbb{F}_q^n$  is called a *coding scheme*, and a function from  $\mathbb{F}_q^n$  into  $\mathbb{F}_q^k$  a *decoding scheme*.

A simple coding scheme arises when  $(a_1, \dots, a_k)$  is encoded into a code word  $\mathbf{c} := (a_1, \dots, a_k, c_{k+1}, \dots, c_n)$ , where the *control symbols*  $c_{k+1}, \dots, c_n$  are chosen in a systematic manner. For instance, let  $H$  be an  $(n - k) \times n$  matrix with entries in  $\mathbb{F}_q$  that is of the special form

$$H = (A \mid I_{n-k})$$

where  $A$  is an  $(n - k) \times k$  matrix and  $I_{n-k}$  is the  $(n - k) \times (n - k)$  identity matrix. The control symbols  $c_{k+1}, \dots, c_n$  are calculated from the system of equations

$$H\mathbf{c}^T = \mathbf{0}.$$

The equations of this system are called *parity-check equations*.

**Example 7.1.** Let  $q = 2$ ,  $k = 4$ ,  $n = 7$ , and let

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The control symbols  $c_5, c_6, c_7$  of the code word  $\mathbf{c} = (a_1, a_2, a_3, a_4, c_5, c_6, c_7)$  are calculated by solving  $H\mathbf{c}^T = \mathbf{0}$  for given symbols  $a_1, a_2, a_3, a_4$ :

$$a_1 + a_3 + a_4 + c_5 = 0$$

$$a_1 + a_2 + a_4 + c_6 = 0$$

$$a_1 + a_2 + a_3 + c_7 = 0$$

and it follows that the coding scheme in this case is the linear map from  $\mathbb{F}_2^4$  into  $\mathbb{F}_2^7$  given by

$$(a_1, a_2, a_3, a_4) \mapsto (a_1, a_2, a_3, a_4, a_1 + a_3 + a_4, a_1 + a_2 + a_4, a_1 + a_2 + a_3)$$

In general we use the following terminology.

**Definition 7.1.** Let  $H$  be an  $(n - k) \times n$  matrix of rank  $n - k$  with entries in  $\mathbb{F}_q$ . The subset  $C$  of  $\mathbb{F}_q^n$  whose elements  $\mathbf{c}$  satisfy  $H\mathbf{c}^T = \mathbf{0}$  is called a *linear  $[n, k]$  code* over  $\mathbb{F}_q$ . Here,

- $n$  is the *length* of  $C$ ,
- $k$  is the *dimension* of  $C$ ,
- the elements of  $C$  are the code are *code words* of  $C$ ,
- $H$  is the (*parity-*)*check matrix* of  $C$ .

Moreover, if  $H$  is of the form  $(A \mid I_{n-k})$  then  $C$  is called a *systematic code*.

**Remark 7.1.** A linear  $[n, k]$  code over  $\mathbb{F}_q$  is an subspace of dimension  $k$  of  $\mathbb{F}_q^n$ , since it is the kernel (or the null space) of  $H$ .

By the following lemma, linear  $[n, k]$  codes over  $\mathbb{F}_q$  are exactly the subspaces of  $\mathbb{F}_q^n$ .

**Lemma 7.1.** *Let  $C$  be a subspace of  $\mathbb{F}_q^n$  of dimension  $k$ . Then there exists  $(n - k) \times n$  matrix  $H$  of rank  $n - k$  with entries in  $\mathbb{F}_q$  such that  $H\mathbf{c}^T = \mathbf{0}$  for all  $\mathbf{c} \in C$ .*

*Proof.* Let  $\{\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(k)}\}$  be a basis of  $C$  over  $\mathbb{F}_q$ . The solution space  $S$  of the system of equations

$$c_1^{(1)}x_1 + \dots + c_n^{(1)}x_n = 0$$

$$c_1^{(2)}x_1 + \dots + c_n^{(2)}x_n = 0$$

$$\vdots$$

$$c_1^{(k)}x_1 + \dots + c_n^{(k)}x_n = 0$$

has dimension  $n - k$ . Let  $H$  be the matrix whose rows form a base of  $S$ . Now  $H\mathbf{c}^T = \mathbf{0}$  for all  $\mathbf{c} \in C$ .  $\square$

The parity-check equations  $H\mathbf{c}^T = \mathbf{0}$  with  $H = (A \mid I_{n-k})$  and  $\mathbf{c} = (a_1, \dots, a_k, c_{k+1}, \dots, c_n)$  can be written in the form

$$\mathbf{0} = H\mathbf{c}^T = A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} + \begin{pmatrix} c_{k+1} \\ \vdots \\ c_n \end{pmatrix} \Leftrightarrow \begin{pmatrix} c_{k+1} \\ \vdots \\ c_n \end{pmatrix} = -A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

Equivalently,

$$\mathbf{c}^T = \begin{pmatrix} I_k \\ -A \end{pmatrix} \mathbf{a}^T = \left( \mathbf{a}(I_k \mid -A^T) \right)^T,$$

where  $\mathbf{a} = (\mathbf{a}_1, \dots, \mathbf{a}_k)$ .

Hence, in this case, the coding scheme from  $\mathbb{F}_q^k$  into  $\mathbb{F}_q^n$  is given by

$$\mathbf{a} \mapsto \mathbf{a}(I_k \mid -A^T),$$

and moreover,  $C$  is the row space of the matrix  $(I_k \mid -A^T)$ .

**Definition 7.2.** The  $k \times n$  matrix  $G = (I_k \mid -A^T)$  is called the *generator matrix* of a linear  $[n, k]$  code with check matrix  $H = (A \mid I_{n-k})$ .

**Example 7.2.** The generator matrix  $G$  of the linear  $[7, 4]$  code in Example 7.1 is

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

and the code words are the 16 linear combinations over  $\mathbb{F}_2$  of the rows of  $G$ .

We generalize this definition in an obvious manner:

**Definition 7.3.** Let  $C$  be a linear  $[n, k]$  code over  $\mathbb{F}_q$ . If  $C$  is the row space of an  $n \times k$  matrix  $G$  of rank  $k$  with entries in  $\mathbb{F}_q$ , then it is called a *generator matrix* of  $C$ .

Consider next decoding.

**Definition 7.4.** If  $\mathbf{c}$  is a code word and  $\mathbf{y}$  is the received word after the transmission of  $\mathbf{c}$  over a channel, then  $\mathbf{e} = \mathbf{y} - \mathbf{c}$  is called the *error vector* of  $\mathbf{c}$ .

**Definition 7.5.** Let  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ . Then,

- (1) The *Hamming distance*  $d(\mathbf{x}, \mathbf{y})$  between  $\mathbf{x}$  and  $\mathbf{y}$  is the number of coordinates in which  $\mathbf{x}$  and  $\mathbf{y}$  differ.
- (2) The *Hamming weight*  $w(\mathbf{x})$  of  $\mathbf{x}$  is the number of nonzero coordinates of  $\mathbf{x}$ .

We observe that  $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ . Moreover, we have the following lemma.

**Lemma 7.2.** *The Hamming distance is a metric on  $\mathbb{F}_q^n$ . That is, for all  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$  we have*

- (1)  $d(\mathbf{x}, \mathbf{y}) = 0$  if and only if  $\mathbf{x} = \mathbf{y}$ ,
- (2)  $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ ,
- (3)  $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ .

*Proof.* Exercise. □

If  $\mathbf{y}$  is the received word, then, one usually tries to find the code word  $\mathbf{c}$  such that  $w(\mathbf{y} - \mathbf{c})$  is as small as possible; that is we assume that it is more likely that few errors have occurred rather than many errors.

Thus, in decoding we are looking for a code word that is closest to the received word according to the Hamming distance. This rule is called the *nearest neighbor decoding*.

**Example 7.3.** Let the message words be the elements of  $\mathbb{F}_4$  and encode each of them by using the generator matrix  $G$  in Example 7.2. Assume that the word  $\mathbf{y} = (1, 1, 0, 0, 1, 0, 1)$  was received. Now  $H\mathbf{y}^T \neq \mathbf{0}$ , where  $H$  is the check matrix of the code given in Example 7.1, and therefore  $\mathbf{y}$  is not in the code. Let  $\mathbf{c}$  be the sum of the first two rows of  $G$  i.e.  $\mathbf{c} = (1, 1, 0, 0, 1, 0, 0)$ . Now  $\mathbf{y}$  and  $\mathbf{c}$  differ only in one coordinate place and we *assume* that  $\mathbf{c}$  was sent.

**Definition 7.6.** Let  $t \in \mathbb{N}$ . Code  $C \subset \mathbb{F}_q^n$  is called *t-error-correcting* if for any  $\mathbf{y} \in \mathbb{F}_q^n$  there is at most one code word  $\mathbf{c} \in C$  such that  $d(\mathbf{y}, \mathbf{c}) \leq t$ .

**Definition 7.7.** For a code  $C \subset \mathbb{F}_q^n$ , the number

$$d_C = \min_{\substack{\mathbf{u}, \mathbf{v} \in C \\ \mathbf{u} \neq \mathbf{v}}} d(\mathbf{u}, \mathbf{v})$$

is called the *minimum distance* of  $C$ .

Obviously,

$$d_C = \min_{\mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}} w(\mathbf{c}),$$

i.e. the minimum distance of a linear code  $C$  is the Hamming weight of a code word of the least weight in  $C$ .

**Theorem 7.1.** *Let  $C$  be a code with minimum distance  $d_C$ . Then, by using the nearest neighbor decoding, it is possible to correct up to  $t$  errors if  $d_C \geq 2t + 1$ .*

*Proof.* It follows from Lemma 7.2 (3) that the closed balls  $B_t(\mathbf{c}) = \{\mathbf{x} \in \mathbb{F}_q^n \mid d(\mathbf{x}, \mathbf{c}) \leq t\}$  with  $\mathbf{c} \in C$  do not overlap if  $d_C \geq 2t + 1$ . Hence, if at most  $t$  errors occurs in a code word  $\mathbf{c}$ , the resulting word belongs only to the ball  $B_t(\mathbf{c})$ .  $\square$

**Lemma 7.3.** *A linear  $[n, k]$  code  $C$  over  $\mathbb{F}_q$  with a check matrix  $H$  has minimum distance  $d_C \geq s + 1$  if and only if any  $s$  columns of  $H$  are linearly independent over  $\mathbb{F}_q$ .*

*Proof.* We observe that  $\mathbf{c} \in C$  iff  $H\mathbf{c}^T = \mathbf{0}$  iff  $\sum_{i=1}^n c_i H^{(i)} = \mathbf{0}$ , where  $H^{(i)}$  is the  $i$ th column of the check matrix  $H$  of  $C$ . Let  $\mathbf{c} \in C$  with  $w(\mathbf{c}) = d_C$ . Now a set of  $d_C$  columns is linearly dependent, and moreover, any  $s$  columns of  $H$  are linearly independent if  $s < d_C$ , by the definition of the minimum distance.  $\square$

**Example 7.4.** By Lemma 7.3, the minimum distance of the code in Example 7.1 is 3. Hence, the decoding in Example 7.3 is correct if only one error occurred during the transmission.

In general it is quite difficult to determine the minimum distances in an infinite family of linear codes. The following family is an exception.

**Definition 7.8.** Let  $m \geq 2$ . A linear code  $C_m$  over  $\mathbb{F}_2$  of length  $2^m - 1$  is called a *binary Hamming code* if the columns of the check matrix of  $C_m$  are the binary representations of the integers  $1, 2, \dots, 2^m - 1$ .

**Example 7.5.** The check matrix  $H$  of  $C_3$  is

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Hence  $C_3$  is a binary  $[7, 4]$  code with minimum distance 3.

In general we have

**Theorem 7.2.** *The binary Hamming code  $C_m$  is a linear  $[2^m - 1, 2^m - m - 1]$  code over  $\mathbb{F}_2$  with minimum distance 3.*

*Proof.* The rank of  $H$  is obviously  $m$ , hence the dimension of  $C_m$  is  $2^m - 1 - m$ . Moreover, since  $H$  does not contain the all zeros column, and any two distinct columns are non-equal, the minimum distance is at least three. Since the sum of any two columns is a column of  $H$ , it follows that the the minimum distance is three.  $\square$

### 7.1. Cyclic codes.

Next we consider a class of linear codes whose mathematical structure is fairly well known and which admit efficient decoding algorithm based on the arithmetics in a finite field.

**Definition 7.9.** A linear  $[n, k]$  code  $C$  over  $\mathbb{F}_q$  is called *cyclic* if  $(a_0, a_1, \dots, a_{n-1}) \in C$  implies  $(a_{n-1}, a_0, \dots, a_{n-2}) \in C$ .

From now on we assume that  $\gcd(n, q) = 1$ . The residue class ring  $\mathbb{F}_q[x]/(x^n - 1)$  is a vector space over  $\mathbb{F}_q$  and it is easy to see that that the function from  $\mathbb{F}_q^n$  into  $\mathbb{F}_q[x]/(x^n - 1)$  given by

$$(a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1x + \dots + a_{n-1}x^{n-1} + (x^n - 1)$$

is an vector space isomorphism over  $\mathbb{F}_q$ .

We identify the elements of  $\mathbb{F}_q[x]/(x^n - 1)$  with the elements in the set  $R_n$  of polynomials of degree less than  $n$ . Moreover, the multiplication of the elements is modulo  $x^n - 1$  and the addition is the usual addition of polynomials, and it follows that  $R_n$  is ring isomorphic to  $\mathbb{F}_q[x]/(x^n - 1)$ .

Because of the isomorphism above, we shall also denote an element  $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  in  $R_n$  as the vector  $(a_0, a_1, \dots, a_{n-1})$ .

**Lemma 7.4.** A linear  $[n, k]$  code  $C$  over  $\mathbb{F}_q$  is cyclic if and only if the corresponding polynomial set is an ideal of  $R_n$ .

*Proof.* Assume  $C$  is cyclic. Let  $g(x) \in R_n$ . Now  $xg(x) \bmod x^n - 1 = (g_{n-1}, g_0, \dots, g_{n-2}) \in C$  and it follows that  $x^k g(x) \in C$  for all non-negative integers  $k$ . Moreover, since  $R_n$  is an vector space over  $\mathbb{F}_q$ , it now follows that  $a(x)g(x) \in C$  for all  $a \in R_n$ . Hence,  $C$  is an ideal of  $R_n$ . The converse assertion is seen similarly.  $\square$

From now we call the ideals of  $R_n$  as cyclic codes. Moreover, a principal ideal of  $R_n$  generated by  $g(x)$  is denoted by  $\langle g(x) \rangle$ .

**Theorem 7.3.** *Let  $C$  be a nonzero cyclic code in  $R_n$ . There exists a monic polynomial  $g(x) \in C$  with the following properties;*

- (1)  $C = \langle g(x) \rangle$ ,
- (2)  $g(x) \mid (x^n - 1)$ .

Let  $k = n - \deg(g)$ , and let  $g(x) = \sum_{i=0}^{n-k} g_i x^i$  where  $g_{n-k} = 1$ . Then

- (3) *The dimension of  $C$  is  $k$  and  $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$  is a basis of  $C$ ,*
- (4) *A generator matrix for  $C$  is*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & \ddots & \ddots & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} \end{pmatrix}.$$

*Proof.* (1) Let  $g$  be the monic polynomial of least positive degree in  $C$ . Let  $c \in C$ . By the division algorithm  $c = tg + r$  for some polynomials  $t, r \in \mathbb{F}_q[x]$  with  $\deg(r) < \deg(g)$ . But  $r = c - tg \in C$ , and therefore  $r = 0$ .

(2)  $x^n - 1 = 0 \in C$  and the claim follows from (1).

(3) and (4) Let  $c \in C$ . Now  $c = tg$  for some  $t \in C$ . Obviously we may assume that  $\deg(t) < k$ , and it follows that

$$c = t_0g(x) + t_1xg(x) + \cdots + t_{k-1}x^{k-1}g(x).$$

Hence,  $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$  spans  $C$  over  $\mathbb{F}_q$ , and obviously it is linearly independent. Items (3) and (4) follow from this.  $\square$

**Definition 7.10.** Let  $C = \langle g(x) \rangle$  be a cyclic code in  $R_n$ . Then  $g(x)$  is called the *generator polynomial* of  $C$ . Moreover, the polynomial  $h(x) = (x^n - 1)/g(x)$  is called the *check polynomial* of  $C$ .

**Lemma 7.5.** *Let  $h(x) = \sum_{i=0}^k h_i x^i \in \mathbb{F}_q[x]$  be the check polynomial of  $C$ . Then, a check matrix of  $C$  is*

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & & & & \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix}.$$

*Proof.* We observe that the  $(i, j)$ th entry of  $HG^T$  is  $\sum_{s=0}^{n-1} h_{k-s-j+1}g_{s-i+1}$  which is the coefficient of  $x^{k+i+j-2}$  of  $h(x)g(x)x^{i+j-2} = (x^n - 1)x^{i+j-2} = 0$  in  $R_n$ . Hence,

$HG^T = \mathbf{0}$ , and it follows that  $C$  is contained in the kernel of  $H$ . But the dimension of  $C$  is  $k$  which is the dimension of the kernel of  $H$ , and therefore  $H$  is a check matrix of  $C$ .  $\square$

Cyclic codes can also be described by means of the roots of the generator polynomial in the the splitting field of  $x^n - 1$  over  $\mathbb{F}_q$ .

Let  $g(x)$  be a factor of degree  $n - k$  of  $x^n - 1$ . Since the derivative of  $x^n - 1$  is  $nx^{n-1} \neq 0$  by the assumption  $\gcd(q, n) = 1$ , it follows that its roots are simple. Hence,  $g(x)$  has exactly  $n - k$  roots in the splitting field of  $x^n - 1$  over  $\mathbb{F}_q$ .

**Lemma 7.6.** *Let  $C = \langle g(x) \rangle$  be a cyclic code of dimension  $k$  in  $R_n$ , and let  $\alpha_1, \dots, \alpha_{n-k}$  be the roots of  $g(x)$ . Then  $c(x) \in C$  if and only if  $c(\alpha_i) = 0$  for all  $i = 1, \dots, n - k$ .*

*Proof.* Let  $c(x) \in R_n$ . If  $c(x) \in C$ , then  $c(x) = t(x)g(x)$  for some  $t(x) \in \mathbb{F}_q[x]$ . Hence, each root of  $g(x)$  is a root of  $c(x)$ .

If  $c(x) \notin C$ , then  $c(x) = t(x)g(x) + r(x)$  with  $0 \leq \deg(r) < \deg(g)$ . If each root of  $g(x)$  were a root of  $c(x)$ , then  $r(x)$  would have more roots than  $\deg(r)$  roots, which is impossible.  $\square$

Since  $g(\alpha^s) = 0$  implies  $g(\alpha^{qs}) = g(\alpha^s)^q = 0$  if  $g(x) \in \mathbb{F}_q[x]$ , we consider the  $q$ -cyclotomic cosets modulo  $n$ :

$$C_s(q, n) := \{s \bmod n, sq \bmod n, sq^2 \bmod n, \dots\},$$

where  $s$  is an integer.

**Lemma 7.7.** *The  $q$ -cyclotomic cosets modulo  $n$  form a partition of  $\{0, 1, \dots, n\}$ .*

*Proof.* It is easy to see that relation  $\sim$  defined by

$$a \sim b \Leftrightarrow a \in C_b(q, n)$$

is an equivalence relation on  $\{0, 1, \dots, n\}$ .  $\square$

**Theorem 7.4.** *Let  $\alpha$  be an element of order  $n$  in the splitting field  $x^n - 1$  over  $\mathbb{F}_q$ . Then*

$$x^n - 1 = \prod_{s \in S} m_{\alpha^s}(x),$$

where  $S$  is a complete set of representatives of  $q$ -cyclotomic coset of  $s$  modulo  $n$  and  $m_{\alpha^s}(x)$  is the minimal polynomial over  $\mathbb{F}_q$  of  $\alpha^s$ .

*Proof.* The irreducible factors over  $\mathbb{F}_q$  of  $x^n - 1$  are the minimal polynomials over  $\mathbb{F}_q$  of the roots of  $x^n - 1$ . The roots of  $x^n - 1$  are the elements of  $\langle \alpha \rangle$  and the roots of  $m_{\alpha^s}(x)$  are exactly the elements  $\alpha^j$  where  $j$  runs over  $C_s(q, n)$  (see Remark 6.1).  $\square$

**Corollary 7.1.** *Let  $C = \langle g(x) \rangle$  be a cyclic code of in  $R_n$ . Then  $g(x) = \prod_{t \in T} m_t(x)$  for some subset  $T$  of  $S$ .*

*Proof.* By the definition of a generator polynomial  $g(x)$  is a factor of  $x^n - 1$ . The corollary now follows from 7.4.  $\square$

**Definition 7.11.** Let  $C = \langle g(x) \rangle$  be a cyclic code of in  $R_n$  with  $g(x) = \prod_{t \in T} m_{\alpha^t}(x)$ . Then, the set  $\{\alpha^t \mid t \in T\}$  is called a *defining set* of  $C$ .

**Theorem 7.5.** *Let  $C = \langle g(x) \rangle$  be a cyclic code of dimension  $k$  in  $R_n$ , and let  $\{\alpha^{t_1}, \dots, \alpha^{t_r}\}$  be a defining set of  $C$ . Let  $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in R_n$ . Then,  $a(x) \in C$  if and only if*

$$\underbrace{\begin{pmatrix} 1 & \alpha^{t_1} & \alpha^{2t_1} & \dots & \alpha^{(n-1)t_1} \\ 1 & \alpha^{t_2} & \alpha^{2t_2} & \dots & \alpha^{(n-1)t_2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{t_r} & \alpha^{2t_r} & \dots & \alpha^{(n-1)t_r} \end{pmatrix}}_{=:H} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

*Proof.* By Lemma 7.6,  $a(x) \in C$  if and only if  $a(\alpha^{t_j}) = 0$  for all  $j = 1, \dots, r$  if and only if  $a_0 + a_1\alpha^{t_j} + \dots + a_{n-1}\alpha^{(n-1)t_j} = 0$  for all  $j = 1, \dots, r$  if and only if

$$\begin{pmatrix} 1 & \alpha^{t_j} & \alpha^{2t_j} & \dots & \alpha^{(n-1)t_j} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0$$

for all  $j = 1, \dots, r$ .  $\square$

**Definition 7.12.** Let  $C = \langle g(x) \rangle$  be a cyclic code of dimension  $k$  in  $R_n$ , and let  $\{\alpha^{t_1}, \dots, \alpha^{t_r}\}$  be a defining set of  $C$ . If the roots  $\alpha^{t_1}, \dots, \alpha^{t_r}$  are in  $\mathbb{F}_{q^m}$ , then the matrix  $H$  in Theorem 7.5 is called a *check matrix* of  $C$  over  $\mathbb{F}_{q^m}$ .

**Example 7.6.** Let  $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$  with  $\alpha^4 = \alpha + 1$ . The minimal polynomials of  $\alpha$  and  $\alpha^3$  over  $\mathbb{F}_2$  are  $m_\alpha(x) = x^4 + x + 1$  and  $m_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$ . These

polynomials are factors of  $x^{15} + 1$ , and since their greatest common divisor is 1, their product is a factor of  $x^n + 1$  as well.

Consider cyclic  $[15, 7]$  code  $C = \langle g(x) \rangle$  in  $R_{15}$  with  $g(x) = m_\alpha(x)m_{\alpha^3}(x)$ . By Theorem 7.5 the check matrix of  $C$  over  $\mathbb{F}_{16}$  is

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{42} \end{pmatrix}$$

We shall see that the minimum distance of  $C$  is at least 5 and therefore  $C$  can correct up to 2 errors.

The encoding is simple: each message word  $a_0 + a_1x + \dots + a_7x^7$  is encoded to the word  $c(x) = a(x)g(x)$ . Consider the decoding. Assume that the received word is  $\mathbf{y} = (y_0, y_1, \dots, y_{14})$ , and write it in the form  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  where  $\mathbf{c}$  is a code word and  $\mathbf{e}$  is an *error vector* with  $w(\mathbf{e}) \leq 2$ . We calculate the *syndrome of  $\mathbf{y}$* :  $H\mathbf{y}^T = H\mathbf{e}^T \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$ .

If two errors occurred, say say  $e(x) = x^i + x^j$  for some unknown  $0 \leq i < j \leq 14$ , then

$$H\mathbf{e}^T = \begin{pmatrix} \alpha^i + \alpha^j \\ \alpha^{3i} + \alpha^{3j} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}.$$

Hence, to locate the error positions  $i$  and  $j$  we need to solve the system of equations  $x + y = S_1$ ,  $x^3 + y^3 = S_3$ , where  $x = \alpha^i$  and  $y = \alpha^j$ , equivalently

$$(4) \quad x^2 + S_1x + \frac{S_1^3 + S_3}{S_1} = 0.$$

If one error occurred, then  $\alpha^i = S_1$  and  $\alpha^{3i} = S_3$ , and therefore  $S_1^3 = S_3$ . We observe that in this case equation (4) has only one nonzero solution. If no errors occurred during the transmission, then  $S_1 = S_3 = 0$ .

To summarize, by the following decision process we can find the transmitted word  $\mathbf{c}$  if at most two errors occurred during the transmission:

- (1) Evaluate the syndrome  $H\mathbf{y}^T = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$  of the received word  $\mathbf{y}$ .
- (2) If  $S_1 = S_3 = 0$ , then decide that no errors occurred.
- (3) If  $S_1^3 = S_3 \neq 0$ , then decide that a single error occurred at the coordinate place  $i$ , where  $\alpha^i = S_1$ .
- (4) If  $S_1^3 \neq S_3$ , then solve equation (4). If it is not solvable, then more than two errors occurred and they can not be located. Otherwise, it has two distinct solutions  $x, y$  and then decide that two errors occurred at the coordinate places  $i$  and  $j$ , where  $x = \alpha^i$  and  $y = \alpha^j$ .

More specifically, assume that the received word  $\mathbf{y} = 1001110000000000$ . Then  $H\mathbf{y}^T = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$ , where

$$S_1 = 1 + \alpha^3 + \alpha^4 + \alpha^5 = \alpha^2 + \alpha^3 = \alpha^6, \quad S_3 = 1 + \alpha^9 + \alpha^{12} + \alpha^{15} = 1 + \alpha^2.$$

Now  $S_1^3 = \alpha^{18} = \alpha^3 \neq S_3$ . Hence, we need to solve the equation

$$x^2 + \alpha^6 x + \frac{1 + \alpha^6}{\alpha^6} = 0,$$

equivalently

$$x^2 + \alpha^6 x + \alpha^9 + 1 = 0.$$

By trial and error we find that the two roots are  $x = \alpha^8$  and  $y = \alpha^{14}$ . Hence, we decide that the transmitted word was  $\mathbf{c} = 1001110010000001$ .

This code word corresponds to the polynomial  $c(x) = 1 + x^3 + x^4 + x^5 + x^8 + x^{14}$  and by dividing it with the generator polynomial  $g(x)$  we get  $a(x) = 1 + x^3 + x^5 + x^6$ . Hence the original message word was 1001011.

**Definition 7.13.** Let  $n$  be a positive integer and let  $m$  be the least positive integer such that  $q^m \equiv 1 \pmod{n}$ . Let  $b$  be a nonnegative integer and let  $\alpha \in \mathbb{F}_{q^m}$  be of order  $n$ . A *BCH code* over  $\mathbb{F}_q$  of length  $n$  and *designed distance*  $d$  with  $2 \leq d \leq n$  is the cyclic code with zeros  $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+d-2}$ .

If  $b = 1$ , the corresponding BCH code is called a *narrow sense* BCH code. If  $n = q^m - 1$ , the BCH code is called *primitive*. If  $n = q - 1$ , the BCH code of length  $q - 1$  is called a *Reed-Solomon (or RS) code*.

**Theorem 7.6** (BCH bound). *The minimum distance of a BCH code of designed distance  $d$  is at least  $d$ .*

*Proof.* The BCH code is the kernel (or the null space) of the matrix

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \dots & \alpha^{(n-1)(b+d-2)} \end{pmatrix}.$$

To prove the theorem, it is enough to show that any  $d - 1$  distinct columns of  $H$  are linearly independent (by Lemma 7.3). The determinant of any  $d - 1$  distinct

columns of  $H$  is

$$\begin{aligned}
& \begin{vmatrix} \alpha^{bi_1} & \alpha^{bi_2} & \dots & \alpha^{bi_{d-1}} \\ \alpha^{(b+1)i_1} & \alpha^{(b+1)i_2} & \dots & \alpha^{(b+1)i_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(b+d-2)i_1} & \alpha^{(b+d-2)i_2} & \dots & \alpha^{(b+d-2)i_{d-1}} \end{vmatrix} \\
&= \alpha^{b(i_1+i_2+\dots+i_{d-1})} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{d-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(d-2)i_1} & \alpha^{(d-2)i_2} & \dots & \alpha^{(d-2)i_{d-1}} \end{vmatrix} \\
&= \alpha^{b(i_1+i_2+\dots+i_{d-1})} \prod_{1 \leq k < j \leq d-1} (\alpha^{i_j} - \alpha^{i_k}) \neq 0.
\end{aligned}$$

Hence, any  $d - 1$  distinct columns of  $H$  are linearly independent.  $\square$

**Example 7.7.** In Example 7.6 we considered cyclic  $[15, 7]$  code  $C$  over  $\mathbb{F}_2$  with a defining set  $\{\alpha, \alpha^3\}$ , and claimed that the minimum distance of  $C$  is at least 5. Since  $\alpha, \alpha^2, \alpha^3$ , and  $\alpha^4$  are zeros of  $C$ , the BCH bound implies that the minimum distance of  $C$  is indeed at least 5.