

# Algebra Review

Instructor: Laszlo Babai  
Notes by Vincent Lucarelli and the instructor

June 15, 2001

## 1 Groups

**Definition 1.1** A **semigroup**  $(G, \cdot)$  is a set  $G$  with a binary operation  $\cdot$  such that:

Axiom 1  $(\forall a, b \in G)(\exists! a \cdot b \in G)$

Axiom 2  $(\forall a, b, c \in G)(a(bc) = a(bc))$

**Definition 1.2** A **group**  $(G, \cdot)$  is a semigroup such that:

Axiom 3 (Identity element)  $(\exists 1 \in G)(\forall a \in G)(1 \cdot a = a = a \cdot 1)$

Axiom 4 (Inverse)  $(\forall a \in G)(\exists b \in G)(a \cdot b = b \cdot a = 1)$

Multiplicative Notation:

- $ab = a \cdot b$
- In Axiom 4,  $b = a^{-1}$

Additive Notation:

- Binary operation ‘+’
- Identity becomes ‘0’
- Additive inverse ‘ $-a$ ’

The size of  $G$  as a set, which is denoted  $|G|$ , is called the **order** of  $G$ .

**Definition 1.3**  $G$  is an **abelian group** if  $G$  is a group such that  $(\forall a, b \in G)(ab = ba)$ .

**Definition 1.4**  $H \subseteq G$  is a **subgroup** of  $G$  (denoted  $H \leq G$ ) if

1.  $1 \in H$
2.  $H$  is closed under the binary operation
3.  $H$  is closed under inverses

**Definition 1.5** Let  $H \leq G$ . The sets of the form  $a \cdot H := \{ah : h \in H\}$  for  $a \in G$  are the **left cosets** of  $G$ . The left cosets partition  $G$ . **Right cosets** are defined analogously.

**Definition 1.6**  $|G : H| =$  number of left cosets of  $H$  in  $G$  is called the **index** of  $H$  in  $G$ .

**Exercise 1.7** Prove that the number of left cosets is the same as the number of right cosets, even if  $G$  is infinite. (*Hint*: construct a bijection between the left and the right cosets.)

**Exercise<sup>+</sup> 1.8** Prove: if  $G$  is finite then the left and the right cosets have a common system of representatives, i. e., there exists a set  $T$  of size  $|T| = |G : H|$  such that  $T$  contains exactly one element from every left coset as well as from every right coset.

**Exercise 1.9 (Lagrange)** If  $H \leq G$  then  $|G| = |H| \cdot |G : H|$ . Therefore, if  $|G| < \infty$  then  $|H| \mid |G|$ .

**Exercise 1.10** Prove: the intersection of subgroups is a subgroup.

**Definition 1.11** Let  $S \subset G$ . We define the subgroup of  $G$  **generated** by  $S$  by

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ H \supseteq S}} H.$$

A group is **cyclic** if it is generated by an element ( $|S| = 1$ ).

**Exercise 1.12**  $\langle S \rangle$  is the set of all products of elements of  $S$  and inverses of elements of  $S$ .

**Example 1.13** Let  $S = \{a, b\}$ . Then  $aba^{-4}bab^6 \in \langle S \rangle$ .

**Example 1.14** If  $|S| = 1$  and  $S = \{g\}$  then  $\langle S \rangle = \{g^n : n \in \mathbb{Z}\}$ .

**Exercise 1.15** If  $G$  is cyclic then

1. if  $|G| = \infty$  then  $G \cong (\mathbb{Z}, +)$
2. if  $|G| = n$  then  $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$

**Definition 1.16** The **order** of an element  $g \in G$  is the order of the cyclic group generated by  $g$ :  $|g| := |\langle g \rangle|$ .

**Exercise 1.17**  $g^k = 1 \Leftrightarrow k \mid |g|$

**Exercise 1.18**  $g^{|G|} = 1$

**Exercise 1.19 (Euler - Fermat)**  $(\forall a, n \in \mathbb{Z})(\text{g.c.d.}(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n})$

**Exercise 1.20** If  $G$  is an abelian group then

$$\frac{\text{l.c.m.} [|a|, |b|]}{\text{g.c.d.} [|a|, |b|]} \mid |ab| \mid \text{l.c.m.} [|a|, |b|].$$

This shows that if  $\text{g.c.d.} [|a|, |b|] = 1$  then  $|ab| = \text{l.c.m.} [|a|, |b|]$ .

**Definition 1.21**  $F_k$  is a **free group of rank  $k$  on free generators**  $\{a_1, \dots, a_k\}$  if the products of the  $a_i$  and the  $a_i^{-1}$  give 1 only by explicit cancellation.

**Example 1.22**  $ab^{-3}a^4a^{-2}a^{-2}b^5b^{-2}a^{-1} = 1$

**Exercise<sup>+</sup> 1.23**  $F_3 \leq F_2$ . In fact,  $F_\infty \leq F_2$ .

**Definition 1.24** For a commutative ring  $R$ , the **special linear group**  $SL(n, R)$  is the group of those  $n \times n$  matrices  $A \in M_n(R)$  with  $\det(A) = 1$ . (More about rings below; we assume all rings have an identity element.)

**Exercise\* 1.25 (Sanov)**  $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$  and  $A^T$  ( $A$  transpose) freely generate a free group  $F_2 \leq SL(2, \mathbb{Z})$ . (*Hint:* for  $T = (t_{ij}) \in SL(2, \mathbb{Z})$ , let  $m(T) = \max |t_{ij}|$ . Show that  $\forall T$  there is at most one  $X \in \{A, A^T, A^{-1}, A^{-T}\}$  such that  $m(T) \geq m(TX)$ .)

**Definition 1.26** Let  $G$  be a group and  $S \subseteq G \setminus 1$ . The **Cayley graph**  $\Gamma(G, S)$  has  $G$  for its vertex set; elements  $g, h \in G$  are adjacent if  $gh^{-1} \in S \cup S^{-1}$  (where  $S^{-1} = \{s^{-1} : s \in S\}$ ).

**Exercise 1.27** Prove:  $\Gamma(G, S)$  is connected if and only if  $S$  generates  $G$ .

**Exercise 1.28** Suppose  $G = \langle S \rangle$ . Then  $\Gamma(G, S)$  is bipartite if and only if  $G$  has a subgroup  $N$  of index 2 such that  $S \cap N = \emptyset$ .

**Exercise 1.29** Let  $S$  be a minimal set of generators of  $G$ , i. e., no proper subset of  $S$  generates  $G$ . Prove:  $K_{3,5} \not\subset \Gamma(G, S)$ .

A theorem of Erdős and Hajnal states that if an (infinite) graph  $X$  does not contain  $K_{m, \aleph_1}$  as a subgraph (for some  $m \in \mathbb{N}$ ) then  $\chi(X) \leq \aleph_0$ . As a consequence of the preceding exercise, if  $S$  is a minimal set of generators then  $\chi(\Gamma(G, S)) \leq \aleph_0$ .

**Exercise 1.30** Prove that every group  $G$  has a set  $S$  of generators such that  $\chi(G, S) \leq \aleph_0$ . *Hint.* Not every group has a minimal set of generators (e.g.,  $(\mathbb{Q}, +)$  does not). But every group has a *sequentially non-redundant* set of generators,  $\{s_\alpha : \alpha \in I\}$ , where  $I$  is a well-ordered set and  $(\forall \alpha \in I)(s_\alpha \notin \langle s_\beta : \beta < \alpha \rangle)$ . Prove that if  $S$  is sequentially non-redundant then  $K_{5,17} \not\subset \Gamma(G, S)$ .

**Exercise 1.31** If a regular graph of degree  $r$  with  $n$  vertices has girth  $g$  then

$$n \geq 1 + r + r(r-1) + \dots + r(r-1)^{\lfloor (g-3)/2 \rfloor} > (r-1)^{g/2-1}.$$

Consequently,  $g < 1 + 2 \log n / \log(r-1)$ .

On the other hand, Erdős and Sachs proved for every  $r \geq 3$  there exist  $r$ -regular graphs of girth  $g \geq \log n / \log(r-1)$ . The following problem addresses the question of **explicit construction** of a 4-regular graph with large girth. The girth will be optimal within a constant factor.

**Exercise<sup>+</sup> 1.32 (Margulis)** Let  $G = SL(2, p) := SL(2, \mathbb{Z}/p\mathbb{Z})$ . Let  $S = \{A, B\}$  where  $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$  and  $B = A^T$  ( $A$  transpose). Note that  $|G| < p^3$  and  $\Gamma(G, S)$  has degree 4. Prove that the girth of  $\Gamma(G, S)$  is  $\Omega(\log p)$ . (*Hint.* Use Sanov's Theorem and the submultiplicativity of matrix norm.)

## 2 Rings

**Definition 2.1** A **ring**  $(R, +, \cdot)$  is an abelian group  $(R, +)$  and semigroup  $(R, \cdot)$  such that:

- (Distributivity)  $(\forall a, b, c \in R)(a(b+c) = ab+ac)$  and  $((b+c)a = ba+ca)$

**Exercise 2.2** In a ring  $R$ ,  $(\forall a \in R)(a \cdot 0 = 0 = 0 \cdot a)$

**Definition 2.3**  $(R, +, \cdot)$  is a **commutative** if  $(R, \cdot)$  is abelian.

**Definition 2.4**  $R$  is a **ring with identity** if  $(R, \cdot)$  satisfies Axiom 3 (semigroup with identity) and  $1 \neq 0$ .

**CONVENTION.** By “rings” we shall always mean **rings with identity**.

**Definition 2.5**  $a \in R$  is a **unit** if  $\exists a^{-1} \in R$ .

**Exercise 2.6** The units of  $R$  form a multiplicative group denoted  $R^\times$ .

**Example 2.7** Let  $R$  be a ring.

- $M_n(R) :=$  set of  $n \times n$  matrices over  $R$  is a ring

**Exercise 2.8** Let  $R$  be a commutative ring.  $GL(n, R)$  denotes the group of units of  $M_n(R)$ . Prove:  $A \in M_n(R)$  belongs to  $GL(R)$  if and only if  $\det(A) \in R^\times$ .

**Example 2.9** mod  $m$  residue classes form a ring, denoted  $\mathbb{Z}/m\mathbb{Z}$ .

**Exercise 2.10** What is the order of the group of units of  $\mathbb{Z}/m\mathbb{Z}$ ?

**Definition 2.11**  $a \in R$  is a **left zero divisor** if  $a \neq 0$  and  $(\exists b \in R, b \neq 0)(ab = 0)$ . **Right zero divisors** are defined analogously.

**Definition 2.12**  $a \in R$  is a **zero-divisor** if  $a$  is a left OR a right zero-divisor.

**Exercise 2.13** 1. If  $\exists a^{-1}$  then  $a$  is not a zero-divisor.

2. The converse is false.

3. The converse is true if  $R$  is finite.

4. The converse is true if  $R = M_n(F)$  where  $F$  is a field. In this case,  $A \in R$  is a zero-divisor if and only if  $\det(A) = 0$ .

**Definition 2.14** An **integral domain** is a commutative ring with no zero-divisors.

**Definition 2.15** A **division ring** is a ring where all nonzero elements are units, i. e.,  $R^\times = R \setminus \{0\}$ .

### 3 Gaussian integers and quaternions; sums of two squares and four squares

**Definition 3.1** The **Gaussian Integers** are complex numbers of the form  $\{a + bi : a, b \in \mathbb{Z}\}$  where  $i = \sqrt{-1}$ . They form the ring  $\mathbb{Z}[i]$ . The *norm* of  $z \in \mathbb{Z}[i]$  is  $N(z) = a^2 + b^2 = z\bar{z}$ .

**Exercise 3.2** Define divisibility among Gaussian integers. Observe that  $z | w \Rightarrow N(z) | N(w)$ . Show that the units among the Gaussian integers are  $\pm 1, \pm i$ .

**Exercise 3.3** Use Gaussian integers to show that  $(a^2 + b^2)(c^2 + d^2) =$  sum of two squares. *Hint.* Observe that  $N(zw) = N(z)N(w)$ .

**Exercise<sup>+</sup> 3.4** Define division with remainder among Gaussian integers. Show the existence of g.c.d.'s. Use this to establish unique prime factorization in  $\mathbb{Z}[i]$ .

**Exercise 3.5** Show: if  $z$  is a prime in  $\mathbb{Z}[i]$  then  $N(z)$  is either  $p$  or  $p^2$  for some prime  $p \in \mathbb{Z}$ . In the former case  $p = N(z) = a^2 + b^2$ ; in the latter case,  $p = z$ .

**Exercise<sup>+</sup> 3.6** Let  $p \in \mathbb{Z}$  be a prime. Prove:  $p$  is a prime in  $\mathbb{Z}[i]$  if and only if  $p \equiv -1 \pmod{4}$ . *Hint.* “If:” if  $p \equiv -1 \pmod{4}$  then  $p \neq a^2 + b^2$ . “Only if:” if  $p \equiv 1 \pmod{4}$  then  $(\exists a \in \mathbb{Z})(p \mid a^2 + 1)$ . Let  $w = a + bi \in \mathbb{Z}[i]$ . Let  $z = \text{g.c.d.}(p, w)$ .

**Exercise 3.7** Infer from the preceding exercise: if  $p$  is a prime (in  $\mathbb{Z}$ ) and  $p \equiv 1 \pmod{4}$  then  $p$  can be written as  $a^2 + b^2$ .

**Exercise<sup>+</sup> 3.8** The positive integer  $n = \prod p_i^{\alpha_i}$  can be written as a sum of two squares if and only if  $(\forall i)(p_i \equiv -1 \pmod{4} \Rightarrow 2 \mid \alpha_i)$ .

**Exercise<sup>+</sup> 3.9** Show that the number of ways to write  $n$  as  $a^2 + b^2$  in  $\mathbb{Z}$  is

$$\epsilon + \prod_{i:p_i \equiv 1 \pmod{4}} (\alpha_i + 1)$$

where  $\epsilon = 1$  if  $n$  is a square and 0 otherwise.

**Exercise 3.10** Let  $n$  be a product of primes  $\equiv 1 \pmod{4}$  and suppose  $n$  is not a square. Prove: the number of ways to write  $n$  as  $a^2 + b^2$  is  $d(n)$  (the number of positive divisors of  $n$ ).

**Definition 3.11** The **quaternions** form a 4-dimensional division algebra  $\mathbb{H}$  over  $\mathbb{R}$ , i.e., a division ring which is a 4-dimensional vector space over  $\mathbb{R}$ . The standard basis is denoted by  $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ , so a quaternion is a formal expression of the form  $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ . Multiplication is performed using distributivity and the following rules:

- $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ;
- $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ ;
- $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$ ;
- $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$ .

It is clear that  $\mathbb{H}$  is a ring. We need to find inverses.

**Exercise 3.12** For  $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ , we define the **norm** of  $z$  by  $N(z) = a^2 + b^2 + c^2 + d^2$ . Prove:  $N(z) = z\bar{z} = \bar{z}z$ , where  $\bar{z} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$  is the **conjugate** quaternion.

**Exercise 3.13** Let  $z, w \in \mathbb{H}$ . Prove:  $N(zw) = N(z)N(w)$ .

### Exercise 3.14

$$(a^2 + b^2 + c^2 + d^2)(k^2 + l^2 + m^2 + n^2) = t^2 + u^2 + v^2 + w^2$$

where  $t, u, v, w$  are bilinear forms of  $(a, b, c, d)$  and  $(k, l, m, n)$  with integer coefficients. Calculate the coefficients.

**Exercise\* 3.15 (Lagrange)** Every integer is a sum of 4 squares. *Hint.* By the preceding exercise, it suffices to prove for primes. First prove that for every prime  $p$  there exist  $x_1, \dots, x_4 \in \mathbb{Z}$  such that  $p \mid \sum x_i^2$  and  $\text{g.c.d.}(x_1, \dots, x_4) = 1$ . Let now  $m > 0$  be minimal such that  $mp = x_1^2 + \dots + x_4^2$ ; note that  $m < p$ . If  $m \geq 2$ , we shall reduce  $m$  and thereby obtain a contradiction (Fermat's method of infinite descent; Fermat used it to prove that if  $p \equiv 1 \pmod{4}$  then  $p$  is the sum of 2 squares). If  $m$  is even, halve  $m$  by using  $(x_1 \pm x_2)/2$  and  $(x_3 \pm x_4)/2$  (after suitable renumbering). If  $m$  is odd, take  $y_i = x_i - mt_i$  such that  $|y_i| < m/2$ . Observe that  $0 < \sum y_i^2 < m^2$  and  $m \mid \sum y_i^2$ , so  $\sum y_i^2 = md$  where  $0 < d < m$ . Now represent  $m^2 dp = (\sum x_i^2)(\sum y_i^2)$  as a sum of four squares,  $\sum z_i^2$ , using the preceding exercise. Analyzing the coefficients, verify that  $(\forall i)(m \mid z_i)$ . Now  $dp = \sum (z_i/m)^2$ , the desired contradiction.

## 4 Fields

**Definition 4.1** A **field** is a commutative division ring.

**Example 4.2** Let  $F$  be a field.

- $M_n(F) :=$  set of  $n \times n$  matrices over  $F$  is a ring
- $GL_n(F) :=$  group of units of  $M_n(F)$  is called the "General Linear Group"

**Exercise 4.3** A finite ring with no zero divisors is a division ring. (*Hint:* use Exercise 2.13.)

**Theorem 4.4 (Wedderburn)** A finite division ring is a field.

**Exercise 4.5** If  $F$  is a field and  $G \leq F^\times$  is a finite multiplicative subgroup then  $G$  is cyclic.

**Definition 4.6** Let  $R$  be a ring and for  $x \in R$  let  $n_x$  be the g.c.d. of all  $n$  such that  $nx = 0$  where

$$\begin{aligned} nx &:= x + \dots + x \text{ when } n > 0 \\ nx &:= -x - \dots - x \text{ (} n \text{ times) when } n < 0 \\ nx &:= 0 \text{ (} n \text{ times) when } n = 0. \end{aligned}$$

**Exercise 4.7**  $n_x \cdot x = 0$

**Exercise 4.8** If  $R$  has no zero divisors then  $(\forall x, y \neq 0)(n_x = n_y)$ .

**Definition 4.9** The common value  $n_x$  is called the **characteristic** of  $R$ .

**Exercise 4.10** If  $R$  has no zero divisors then  $\text{char}(R) = 0$  or it is prime. In particular, every field has 0 or prime characteristic.

**Exercise 4.11** If  $R$  is a ring without zero-divisors, of characteristic  $p$ , then  $(a + b)^p = a^p + b^p$ .

**Exercise 4.12**

1. If  $R$  has characteristic 0 then  $R \supseteq \mathbb{Z}$
2. If  $R$  has characteristic  $p$  then  $R \supseteq \mathbb{Z}/p\mathbb{Z}$ .

**Exercise 4.13** If  $F$  is a field of characteristic 0 then  $F \supseteq \mathbb{Q}$ .

**Definition 4.14** A **subfield** of a ring is a subset which is a field under the same operations. If  $K$  is a subfield of  $L$  then we say that  $L$  is an extension of  $K$ ; the pair  $(K, L)$  is referred to as a **field extension** and for reasons of tradition is denoted  $L/K$ .

**Definition 4.15** A **prime field** is a field without a proper subfield.

**Exercise 4.16** The prime fields are  $\mathbb{Q}$  and  $\mathbb{Z}/p\mathbb{Z}$  ( $p$  prime).

**Definition 4.17** Observe: if  $L/K$  is a field extension then  $L$  is a vector space over  $K$ . The **degree** of the extension is  $[L : K] := \dim_K L$ . A **finite extension** is an extension of finite degree.

**Exercise 4.18** The order of a finite field is a prime power. *Hint.* Let  $L$  be a finite field and  $K$  its prime field, so  $|K| = p$ ; let  $[L : K] = k$ . Prove:  $|L| = p^k$ .

**Exercise 4.19** The degree of the extension  $\mathbb{C}/\mathbb{R}$  is 2. The degree of the extension  $\mathbb{R}/\mathbb{Q}$  is uncountably infinite (continuum).

**Exercise<sup>+</sup> 4.20** Prove that  $\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots, \sqrt{p}$  are linearly independent over  $\mathbb{Q}$ .

**Exercise 4.21** If  $K \subset L \subset M$  are fields then  $[M : L][L : K] = [M : K]$ .

## 5 Polynomials over Rings and Fields

**Definition 5.1** Let  $R$  be a commutative ring. (As always we assume  $R$  has an identity.)  $R[x]$  denotes the ring of polynomials in the variable  $x$  with coefficients in  $R$ .

**Exercise 5.2** If  $R$  is an integral domain then  $R[x]$  is an integral domain.

**Definition 5.3** A **unique factorization domain** (UFD) is an integral domain in which every element can be written uniquely as a product of irreducible elements. The factorization is unique up to the order of the factors and multiplying each factor by units.

**Example 5.4** Every field is a UFD. The rings  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  are UFDs.

**Exercise 5.5** Prove: if  $R$  is a UFD then  $R[x]$  is a UFD.

**Exercise 5.6** For an integral domain  $R$ , define the field of quotients (or field of fractions)  $\left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}$  by copying how  $\mathbb{Q}$  arises from  $\mathbb{Z}$ . (*Hint*: “rational numbers” are equivalence classes of fractions).

**Definition 5.7** Let  $F$  be a field and  $F(x)$  be the field of quotients of  $F[x]$ .  $F(x)$  is called the **function field** over  $F$ .

**Exercise 5.8**  $\dim_{\mathbb{R}} \mathbb{R}[x]$  is countably infinite and  $\dim_{\mathbb{R}} \mathbb{R}(x)$  is uncountably infinite. (*Hint*: Show  $\left\{ \frac{1}{x - \alpha} : \alpha \in \mathbb{R} \right\}$  is linearly independent over  $\mathbb{R}$ .)

**Definition 5.9** Let  $F$  be a field.  $f \in F[x]$  is **irreducible** if  $f$  is not constant (i. e.,  $\deg f \geq 1$ ) and  $(\forall g, h \in F[x])(f = gh \Rightarrow \deg g = 0 \text{ or } \deg h = 0)$ .

**Definition 5.10** Let  $L/K$  be a field extension; let  $\alpha \in L$ . We say that  $\alpha$  is **algebraic** over  $K$  if  $(\exists f \in K[x])(f \neq 0 \text{ and } f(\alpha) = 0)$ . We define  $m_{\alpha}(x)$  as the g.c.d. of all such polynomials.  $m_{\alpha}(x)$  and we call it the **minimal polynomial** of  $\alpha$  (over  $K$ ). If all elements of  $L$  are algebraic over  $K$  then we call  $L/K$  an algebraic extension.

**Exercise 5.11**  $m_{\alpha}(\alpha) = 0$ .

**Exercise 5.12**  $m_{\alpha}$  is irreducible over  $K$ .

**Exercise 5.13** Every finite extension is algebraic.

**Definition 5.14** Let  $R$  be a ring.  $I \subseteq R$  is a **left ideal** of  $R$  if  $I$  is an additive subgroup of  $R$  and  $(\forall r \in R)(rI \subseteq I)$ . Right ideals are defined analogously.  $I$  is an **ideal** if it is both a left- and a right-ideal.

**Definition 5.15** Let  $R$  be a ring and  $I$  an ideal of  $R$ . The additive quotient group  $R/I$  with elements  $a + I$  is a ring under the multiplication rule  $(a + I)(b + I) = ab + I$ . It is called the **quotient ring**.

**Exercise 5.16** Let  $F$  be a field and  $f \in K[x]$ . The ring  $K[x]/(f)$  is a field if and only if  $f$  is irreducible.

**Definition 5.17** A **simple extension**  $K(\alpha)$  is the smallest field containing  $K$  and  $\alpha$ .

**Exercise 5.18** If  $\alpha$  is algebraic over  $K$  then  $K(\alpha) = K[\alpha] = \{f(\alpha) : f \in K[x]\} \simeq K[x]/(m_\alpha)$ .

**Exercise 5.19** Let  $\mathbb{F}_q$  be a finite field of order  $q$ . Then

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

$$x^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^\times} (x - \alpha)$$

**Exercise<sup>+</sup> 5.20** Let  $q = p^n$  be a prime power. Let  $F_d(x)$  be the product of all monic irreducible polynomials of degree  $d$  over  $\mathbb{F}_p$ . Prove that  $x^q - 1 = \prod_{d|n} F_d(x)$ . (For this exercise, do not assume the existence of  $\mathbb{F}_q$ . The field  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  of course exists.)

**Exercise<sup>+</sup> 5.21** Let  $N_d$  be the number of monic irreducible polynomials of degree  $d$  over  $\mathbb{F}_p$ . Observe from the preceding exercise that  $p^k = \sum_{d|k} dN_d$ . Infer:

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

Conclude that  $N_n \neq 0$ .

**Exercise 5.22** Prove that there exists a field of order  $p^n$ . *Hint.* The preceding exercise shows that there exists an irreducible polynomial  $f$  of degree  $n$  over  $\mathbb{F}_p$ . Take the field  $\mathbb{F}_p[x]/(f)$ .

**Exercise 5.23** Prove: the field of order  $p^k$  is unique (up to isomorphism).

## 6 Irreducibility over $\mathbb{Z}$ , Gauss lemma, cyclotomic polynomials

**Exercise 6.1 (Gauss Lemma)** A polynomial  $f \in \mathbb{Z}[x]$  is **primitive** if the g.c.d. of its coefficients is 1. Prove: the product of primitive polynomials is primitive. (*Hint.* Assume  $fg = ph$  where  $f, g, h \in \mathbb{Z}[x]$  and  $p$  is a prime. Look at this equation modulo  $p$  and use the fact that  $\mathbb{F}_p[x]$  is an integral domain.)

**Exercise 6.2** If  $f \in \mathbb{Z}[x]$  splits into factors of lower degree over  $\mathbb{Q}[x]$  then such a split occurs over  $\mathbb{Z}[x]$ . In fact, if  $f = gh$  where  $g, h \in \mathbb{Q}[x]$  then  $(\exists r \in \mathbb{Q})(rg \in \mathbb{Z}[x] \text{ and } h/r \in \mathbb{Z}[x])$ .

**Exercise 6.3** Let  $f(x) = \prod_{i=1}^n (x - a_i) - 1$  where the  $a_i$  are distinct integers. Then  $f(x)$  is irreducible over  $\mathbb{Q}$ . *Hint.* Let  $f = gh$  where  $g, h \in \mathbb{Z}[x]$ . Observe that  $(\forall i)(g(a_i) + h(a_i) = 0)$ .

**Exercise 6.4** Let  $f(x) = \left( \prod_{i=1}^n (x - a_i) \right)^2 + 1$  where the  $a_i$  are distinct integers. Then  $f(x)$  is irreducible over  $\mathbb{Q}$ . *Hint.* Let  $f = gh$  where  $g, h \in \mathbb{Z}[x]$ . Observe that  $(\forall i)(g(a_i) = h(a_i) = \pm 1)$ . Observe further that  $g$  never changes sign; nor does  $h$ .

**Exercise 6.5** Let  $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ . If  $p$  is a prime and  $p \nmid a_n, p \mid a_0, \dots, p \mid a_{n-1}, p^2 \nmid a_0$ , then  $f$  is irreducible over  $\mathbb{Q}$ . (*Hint:* Unique factorization in  $\mathbb{F}_p[x]$ ).

**Exercise 6.6** If  $p$  is a prime then  $\Phi_p(x) := x^{p-1} + x^{p-2} + \dots + x + 1$  is irreducible over  $\mathbb{Q}$ . (*Hint:* Introduce the variable  $z = x - 1$ .)

**Exercise 6.7**  $\text{g.c.d.}(x^k - 1, x^\ell - 1) = x^d - 1$  where  $d = \text{g.c.d.}(k, \ell)$ .

**Definition 6.8** The  **$n$ -th cyclotomic polynomial** is defined as

$$\Phi_n(x) = \prod_{\omega} (x - \omega) \in \mathbb{C}[x]$$

where the product extends over all complex primitive  $n$ -th roots of unity.

**Exercise 6.9**

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

**Exercise 6.10** Let  $f, g \in \mathbb{Z}[x]$  with the leading coefficient of  $g$  equal to 1. If  $\frac{f}{g} \in \mathbb{Q}[x]$  then  $\frac{f}{g} \in \mathbb{Z}[x]$ .

**Exercise 6.11**

$$\Phi_n(x) \in \mathbb{Z}[x]$$

**Exercise 6.12**

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

**Exercise 6.13** Let  $f, g$  be polynomials over the field  $F$ . Prove: if  $g^2 | f$  then  $g | f'$ , where  $f'$  is the (formal) derivative of  $f$ .

**Exercise 6.14** Prove: if  $p \nmid n$  then  $x^n - 1$  has no multiple factors over  $\mathbb{F}_p$ .

**Exercise<sup>+</sup> 6.15** Let  $a \neq b$  and  $n$  be positive integers. Let  $p$  be a prime. Assume  $p | \text{g.c.d.}(\Phi_a(n), \Phi_b(n))$ . Prove:  $p | \text{g.c.d.}(a, b)$ .

**Exercise 6.16** Prove: if  $f$  is a polynomial over any field of characteristic  $p$ , then  $f(x^p) = (f(x))^p$ .

**Exercise<sup>+</sup> 6.17** Let  $\omega$  be a complex primitive  $n$ -th root of unity. Prove: if  $p$  is a prime and  $p \nmid n$  then the minimal polynomials of  $\omega$  and  $\omega^p$  (over  $\mathbb{Q}$ ) coincide. (*Hint.* Let  $f$  and  $g$  be the minimal polynomials of  $\omega$  and  $\omega^p$ , respectively. Assume  $f \neq g$ ; then  $fg | x^n - 1$ . Observe that  $f(x) | g(x^p)$ . Look at this equation over  $\mathbb{F}_p$  and conclude that  $x^n - 1$  has a multiple factor over  $\mathbb{F}_p$ , a contradiction.)

**Exercise 6.18** A major result is now immediate:  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .