

## CONTENTS

1. Recollections	1
2. Integers	1
3. Modular Arithmetic	3
4. Groups	5
5. Permutations and the Symmetric Groups	11
6. Cosets and normal subgroups	12
7. Automorphisms of groups	18
8. Abelian Groups	19
9. Group Actions	23
10. Sylow theorems	28
11. Solvable and simple groups	29
12. Composition series and Jordan-Hölder Theorem	31
13. Rings and Fields	31
14. Ring homomorphisms and ideals	35
15. Polynomial rings over fields.	38
16. Field extensions.	38
17. Algebraic extensions.	38
18. Algebraic closure and normal extensions.	38
19. Separable extensions	40
20. Galois theory	43

### 1. RECOLLECTIONS

Recall: Sets, maps of sets, equivalence relations on sets.

### 2. INTEGERS

Write  $\mathbb{Z}$  for the set of integers. Remember we have the following operations on  $\mathbb{Z}$ : Addition ("+" ) and multiplication ("·"), satisfying various properties. Also recall that the natural numbers  $\mathbb{N} = \{0, 1, \dots\}$  are *well-ordered*, that is, any non-empty subset has a smallest element.

**Proposition 2.1.** *Let  $m, n$  be two non-zero integers. Then there exist unique integers  $q$  and  $r$  such that  $n = mq + r$  and  $0 \leq r < m$ .*

*Proof.* There is a maximal integer  $q$  such that  $mq \leq n$  (proof: The set of  $q'$  such that  $mq' \leq n$  is bounded above, by the Archimedean axiom). Set  $r = n - mq$ . Apparently,  $0 \leq r < m$ , or  $m(q + 1) \leq n$ , contradicting the maximality of  $q$ . Uniqueness of  $q$  is clear from this, and that implies uniqueness of  $r$ . □

This result is known as "division algorithm" (even though it isn't really an algorithm). Its existence is an important property of the integers.

**Definition 2.2.** Let  $m, d$  be two integers. If there is an integer  $q$  such that  $n = qd$  then we say that  $d$  *divides*  $n$  or that  $d$  *is a divisor of*  $n$ . We write  $d|n$ .

*Example 2.3.* The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24. The positive divisors of 42409 are 1, 42409.

**Lemma 2.4.** *Suppose  $d|n$  and  $d|m$ , and that  $a, b$  are any integers. Then  $d|am + bn$ .*

*Proof.* Suppose  $n = dq_1$  and  $m = dq_2$ . Then  $am + bn = (aq_1 + bq_2)d$ .  $\square$

**Definition 2.5.** If  $m, n$  are not both 0, then a number  $d$  dividing both  $n$  and  $m$  is called a common divisor of  $m$  and  $n$ . A (positive) common divisor  $d$  with the property that any other common divisor  $d'$  divides  $d$  is called a *greatest common divisor* and written  $\gcd(m, n)$ .

**Theorem 2.6.** For every pair  $m, n$  of integers, not both 0, there is a unique greatest common divisor  $g$ . Moreover, there are integers  $a, b$  such that  $am + bn = g$ .

*Proof.* Uniqueness is clear: If  $d$  and  $d'$  are greatest common divisors, then  $d|d'$  and  $d'|d$ . That is, there are positive integers  $q, q'$  such that  $d = qd'$  and  $d' = q'd$ . So,  $d = qq'd$  and therefore  $qq' = 1$  and hence  $q = q' = 1$ .

Now let  $S = \{k > 0 | \exists a, b \in \mathbb{Z} : k = am + bn\}$ . By the well-orderedness of the natural numbers,  $S$  has a minimal element  $g$ . Obviously, every common divisor of  $m, n$  divides  $g$ . On the other hand, by the division algorithm 2.1, we can write  $n = qg + r$  for some  $q$  and  $0 \leq r < g$ . In this case either  $r = (1 - qa)n - qbm \in S$ , contradicting the minimality of  $g$ , or  $r = 0$ . We conclude  $r = 0$  and therefore  $g|n$ . Similarly, we conclude  $g|m$ .  $\square$

There is an effective algorithm for computing the greatest common divisor of a pair  $m, n$  of integers, the *Euclidian algorithm*. It works as follows:

First off, we can as well assume  $m, n > 0$ . If  $n = m$  then  $\gcd(m, n) = n$ , we are done. Otherwise, suppose  $n > m$ , say. Use the division algorithm to write  $n = mq_0 + r_1$ . Repeat the same procedure with  $m, r_1$  in place of  $n, m$ , getting  $m = r_1q_1 + r_2$ ; repeat again, getting  $r_1 = r_2q_2 + r_3$ , etc. pp.. Eventually,  $r_i = 0$  (why? Explain!). Let  $k$  be the minimal number such that  $r_{k+1} = 0$ . I claim  $r_k = \gcd(m, n)$ . Indeed, for any  $i \leq k$ ,  $r_{i-1} = r_iq_i + r_{i+1}$ . Since  $r_k|r_k$ , descending induction on  $i$  shows that  $r_k|r_{i-1}$ , so that  $r_k|m$  and  $r_k|n$ . On the other hand, we can clearly write  $r_k = am + bn$  for some  $a, b \in \mathbb{Z}$ . That is,  $r_k$  is a common divisor and at least as large as the  $\gcd(m, n)$ ; therefore,  $r_k = \gcd(m, n)$ , as claimed.

Theorem 2.6 has a number of consequences. We need a couple more definitions:

**Definition 2.7.** A pair  $m, n$  of integers is called relatively prime if  $\gcd(m, n) = 1$ .

**Definition 2.8.** A natural number  $p$  is called a prime (number) if it has exactly two divisors (namely, 1 and  $p$ ).

*Example 2.9.* 59 and 42409 are prime numbers, while 256 and 1 are not.

**Proposition 2.10.** Suppose  $a, b$  are relatively prime and  $c$  is any integer. If  $d$  is a common divisor of  $a$  and  $bc$ , then  $d$  is a common divisor of  $a$  and  $c$ .

*Proof.* Write  $1 = sa + tb$ . Then  $c = csa + tbc$ . Since  $d|a$  and  $d|bc$  by assumption, we conclude that  $d|c$ .  $\square$

**Corollary 2.11.** For any two integers  $a, b$  and a prime number  $p$ , if  $p|ab$  then  $p|a$  or  $p|b$ .

*Proof.* If  $p|a$ , then we are done. If not, then  $\gcd(a, p) = 1$ . Since  $p$  is a common divisor of  $p$  and  $ab$ , it is a common divisor of  $p$  and  $b$ , by the preceding Proposition 2.10.  $\square$

Now we can prove the fundamental theorem of arithmetic:

**Theorem 2.12.** *Let  $n$  be a positive integer. Then there exist a unique set of prime numbers  $p_1, \dots, p_s$  and natural numbers  $a_1, \dots, a_s > 0$ , such that*

$$n = p_1^{a_1} \cdots p_s^{a_s}$$

*Proof.* we prove existence of the decomposition by induction. The statement is obviously true for  $n = 1$  (in this case, there are no prime factors -  $s = 0$ ). Assume we have proved the assertion for all  $k < n$ , for some  $n > 1$ . Either  $n$  is prime, in which case we are done. Or there is a factorization  $n = km$  with  $k$  and  $m$  both less than  $n$ . Using strong induction, we get a prime decomposition.

The uniqueness of the decomposition is clear for  $n = 1$  (there are no factors). Now assume

$$n = p_1^{a_1} \cdots p_s^{a_s} = q_1^{b_1} \cdots q_t^{b_t}.$$

By Lemma 2.12,  $p_1 | q_i$  for some  $i$ ; reordering if necessary, we can assume  $p_1 | q_1$ . By strong induction,

$$k = p_1^{a_1-1} \cdots p_s^{a_s} = q_1^{b_1-1} \cdots q_t^{b_t}$$

has a unique prime decomposition. That is,  $s = t$  and after reordering  $p_i = q_i$  and  $a_i = b_i$  for all  $i$ , as claimed.  $\square$

*Remark 2.13.* Note that the proof does not at all give a good method to actually compute the prime factorization of a given integer. In fact, finding a good algorithm to do this (or proving such an algorithm does not exist) is one of the more important problems in mathematics today.

### 3. MODULAR ARITHMETIC

Let  $n > 0$  be an integer. We can define an equivalence relation on  $\mathbb{Z}$  by  $a \equiv b \pmod n$  (i.e.,  $a$  and  $b$  are related - we read " $a$  is congruent to  $b$  modulo  $n$ ") if and only if  $n | a - b$ . We write  $[k]$  (or  $[k]_n$  if the *modulus*  $n$  is not clear) for the equivalence class (also called *congruence class*) of  $k \in \mathbb{Z}$  with respect to this relation.

**Definition 3.1.** The set of equivalence classes with respect to this relation is written  $\mathbb{Z}/n$ .

**Lemma 3.2.** *The set  $\mathbb{Z}/n$  is in one-to-one correspondence with the set of natural numbers less than  $n$ , given by the map*

$$\{0, 1, \dots, n-1\} \longrightarrow \mathbb{Z}/n$$

*mapping  $k \mapsto [k]$ .*

*Proof.* The division algorithm shows that the indicated map is surjective and injective.  $\square$

The important property of the congruence relation is that it is additive and multiplicative.

**Lemma 3.3.** *Assume  $a \equiv b \pmod n$  and  $c \equiv d \pmod n$ . Then*

- (1)  $a + c \equiv b + d \pmod n$ .
- (2)  $ac \equiv bd \pmod n$ .

*Proof.* (1) By assumption,  $n | b - a$  and  $n | d - c$ . Hence,  $n | b - a + d - c = b + d - (a + c)$ .  
 (2)  $bd - ac = b(d - c) + c(b - a)$ .  $\square$

That is, we can define the operations of addition and multiplication on  $\mathbb{Z}/n$ , as

$$[a] + [b] = [a + b]$$

and

$$[a][b] = [ab]$$

(the previous Lemma ensures the results do not depend on the choice of representative in a congruence class).

Clearly, we have a zero element:  $[a] + [0] = [0] + [a] = [a]$ , and a unit element:  $[a][1] = [1][a] = [a]$ , we can subtract elements:  $[a] - [b] = [a - b]$ .

Also clearly, addition and multiplication are commutative and there is a distributive law.

In general, though, we can not divide (no surprise there - we started with the integers, after all). But there is the following result, showing that certain congruence classes are *invertible* or a *unit*, meaning that they divide  $[1]$ :

**Proposition 3.4.** *Let  $a$  be an integer. Then there is another integer  $b$  such that  $ab \equiv 1 \pmod{n}$  if and only if  $\gcd(a, n) = 1$ . That is, there is  $[b] \in \mathbb{Z}/n$  such that  $[a][b] = [1]$  (so  $[a]$  is a unit) if and only if  $\gcd(a, n) = 1$ .*

*Proof.* Recall that  $\gcd(a, n)$  can be described as the least positive integer that can be expressed as a linear combination of  $a$  and  $n$ . If  $ab \equiv 1 \pmod{n}$ , then there is an integer  $d$  such that  $ab - 1 = dn$  or  $1 = ab - dn$ . So  $\gcd(a, n) = 1$ .

Conversely, suppose  $\gcd(a, n) = 1$ , so there are integers  $b, d$  such that  $1 = ab + dn$ . But then  $ab = 1 - dn \equiv 1 \pmod{n}$ .  $\square$

Note that the congruence class of the inverse  $b$  is unique, if it exists. Indeed, if  $ac \equiv 1 \pmod{n}$ , then  $b \equiv bac \equiv c \pmod{n}$ .

*Notation 3.5.* The set of units in  $\mathbb{Z}/n$  (i.e., the set of congruence classes relatively prime to  $n$ ) is written  $\mathbb{Z}/n^*$  or  $U(n)$ .

**Corollary 3.6.** *The set of units  $\mathbb{Z}/n^*$  is closed under multiplication. In other words, if  $a$  and  $b$  are both relatively prime to  $n$  then so is  $ab$ .*

*Proof.* Suppose  $[a]$  and  $[b]$  are units. Then there exist  $[c]$  and  $[d]$  such that  $[a][c] = [1]$  and  $[b][d] = [1]$ . Consequently,  $[ab][cd] = [a][b][c][d] = [1][1] = [1]$ , so  $[ab]$  is a unit. By the proposition, this means that  $ab$  is relatively prime to  $n$ .  $\square$

**Corollary 3.7.** *If  $n = p$  is a prime, then every congruence class  $[a] \neq [0]$  is a unit in  $\mathbb{Z}/p$ . That is, in  $\mathbb{Z}/p$ , it is possible to divide by any non-zero element!*

*Proof.* If  $a$  is not divisible by  $p$ , then  $\gcd(a, p) = 1$  since  $p$  is a prime number.  $\square$

*Example 3.8.* Consider the set  $\mathbb{Z}/8$  of congruence classes modulo 8. Its set of units  $\mathbb{Z}/8^*$  consists of the classes  $[1], [3], [5], [7]$ .

**Definition 3.9.** The Euler  $\phi$ -function is the function on positive integers assigning to a number  $n > 0$  the cardinality  $\phi(n)$  of the set of units  $\mathbb{Z}/n^*$  in  $\mathbb{Z}/n$ .

*Example 3.10.* For any prime  $p$ , we have that  $\phi(p) = p - 1$ . On the other hand,  $\phi(8) = 4$  and  $\phi(24) = 8$ . Roughly, if a number has many prime factors, then  $\phi(n)/n$  is small.

We will come back to the sets  $\mathbb{Z}/n$  when we talk about abelian groups, see Section 8.

## 4. GROUPS

In this section, we define the notion of group and homomorphism of groups, list some examples and study their basic properties.

*Example 4.1.* Consider a square. We can describe its symmetries by the geometric operations that leave the square invariant: The rotations by multiples of  $\pi/2$  and the reflections along the diagonals and the bisectors of sides. Thus, there are 8 symmetries (call the set of those symmetries  $D_8$ ). Note the following features of this set of symmetries:

- (1) There is an identity symmetry.
- (2) We can compose any two of the symmetry operations and the result will be a symmetry operation. For example, if we first perform reflection along the horizontal bisector and then along the vertical bisector, the result is a rotation by  $\pi$ .
- (3) Every symmetry operation is invertible: It can be reversed by performing a symmetry operation. For example, the reflections are reversed by just performing the same reflection again; the rotation by  $\pi/2$  is reversed by the rotation by  $3\pi/2$ .
- (4) Composition of symmetries is associative.

Note that composition of symmetries is *not* commutative in the above example: A rotation by  $\pi/2$  followed by reflection along the horizontal bisector is the same as reflection along the diagonal connecting the upper left and lower right vertices, while performing the reflection along the horizontal bisector first and then rotating by  $\pi/2$  results in the same operation as reflection along the other diagonal.

*Example 4.2.* The set  $\mathbb{Z}/n$  has an addition operation with the following properties (see section 3):

- (1) Addition is associative.
- (2) There is a zero element.
- (3) Every element has an inverse, namely, its negative.
- (4) Addition is commutative.

*Example 4.3.* The set  $\mathbb{Z}/n^*$  of units modulo  $n$  has the multiplication operation, with these properties:

- (1) The multiplication is associative.
- (2) There is an identity element.
- (3) Every element has an inverse.
- (4) The multiplication is commutative.

*Example 4.4.* The set of all invertible  $2 \times 2$ -matrices over the real numbers (written  $Gl(2, \mathbb{R})$ ) has the operation of matrix multiplication, with these properties:

- (1) The multiplication is associative.
- (2) There is an identity element, namely the identity matrix.
- (3) Every element has an inverse, namely, the inverse matrix.

These examples suggest the following definition.

**Definition 4.5.** A *group*  $G$  is a (non-empty) set together with a map (called *group operation*)  $G \times G \rightarrow G$ , sending  $(g, h) \in G \times G$  to an element (often, but not always, called their *product*)  $g * h$  (also written  $gh$  or  $g \cdot h$ ), and a distinguished element  $e \in G$  (called the *neutral element*, or *identity element*, or *unit element*) such that:

- (1) (associativity) For all  $g, h, k \in G$ , we have  $(g * h) * k = g * (h * k)$ .
- (2) (neutral element) For all  $g \in G$ , we have  $g * e = e * g = g$ .
- (3) (inverse) For all  $g \in G$  there exists an element  $g^{-1} \in G$  (called *inverse* of  $g$ ) such that  $g * g^{-1} = g^{-1} * g = e$ .

The following facts are immediate consequences of the definition.

- Lemma 4.6.** (1) *The neutral element is unique.*  
 (2) *The inverse of any element  $g$  is unique.*

*Proof.* (1) Suppose  $e'$  is also a neutral element. Then  $e = e * e' = e'$ .

(2) Suppose  $h$  and  $h'$  are both inverses of  $g$ . Then  $h = h * e = h * g * h' = e * h' = h'$ .  $\square$

In fact, the first observation can be strengthened.

**Lemma 4.7.** *Suppose  $G$  is a group with neutral element  $e$ , and  $g, h \in G$ . If  $gh = h$ , then  $g = e$ .*

*Proof.*  $gh = h$  implies that  $g = ge = g(hh^{-1}) = (gh)h^{-1} = hh^{-1} = e$ .  $\square$

**Lemma 4.8.** *Let  $G$  be a group,  $g, h \in G$ . Then*

$$(gh)^{-1} = h^{-1}g^{-1}$$

*Proof.* We have  $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = e$ .  $\square$

**Definition 4.9.** If  $G$  is a group such that the operation is commutative, then  $G$  is called an *abelian* or *commutative* group. The group operation in an abelian group is often (but not always) written as "+", because  $\mathbb{Z}$  with addition as operation is the most important example of an abelian group. In this case the neutral element is written 0.

*Notation 4.10.* We write  $g^n$  for  $g * \dots * g$  ( $n$  factors), if  $n > 0$ . If  $n < 0$ , we write  $g^n$  for  $(g^{-1})^{-n}$ . Finally,  $g^0 = e$ .

If the operation is denoted +, then we write  $nx$  for  $x + \dots + x$  ( $n$  summands), etc..

- Example 4.11.* (1)  $D_8$  is a group with operation given by composition and neutral element the identity.  
 (2) The set  $\mathbb{Z}/n$  is an abelian group with operation given by addition and neutral element [0].  
 (3) The set  $\mathbb{Z}/n^*$  is an abelian group with operation given by multiplication and neutral element [1].  
 (4) The set of invertible  $2 \times 2$  matrices is a group with operation given by matrix multiplication and neutral element the identity matrix.  
 (5) The set  $\mathbb{R}^*$  of non-zero real numbers is an abelian group with operation given by multiplication and neutral element 1.

A finite group and its operation can be described by a *group table*... . **(do some examples here !!!)**

Next we define maps between groups compatible with the structure.

**Definition 4.12.** Let  $G$  and  $H$  be two groups. A map  $f : G \rightarrow H$  is called a *group homomorphism* if for all  $g, g' \in G$ ,

$$f(g * g') = f(g) * f(g').$$

A group homomorphism is sometimes called a monomorphism if it is an injective map, an epimorphism if it is a surjective map, and an isomorphism if it is a bijective map. If  $G = H$ , we say that  $f$  is an *endomorphism*. Finally, an endomorphism that is also an isomorphism is called *automorphism*.

*Remark 4.13.* (1) If  $f : G \rightarrow H$  is a group homomorphism, then  $f(e_G) = e_H$ . This is implied by Lemma 4.7 in light of the fact that  $f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$ .

(2) If  $f : G \rightarrow H$  is a group homomorphism, then for all  $g \in G$ , we have  $f(g^{-1}) = f(g)^{-1}$ . Indeed,  $f(g) * f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ .

The composition of homomorphisms is a homomorphism.

**Lemma 4.14.** *Let  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow K$  be group homomorphisms. Then the composition  $\psi\phi : G \rightarrow K$  is a homomorphism.*

*Proof.* Calculate  $\psi(\phi(gg')) = \psi(\phi(g)\phi(g')) = \psi(\phi(g))\psi(\phi(g'))$ . □

An isomorphism of groups has an inverse map that is also a group homomorphism.

**Lemma 4.15.** *Let  $f : G \rightarrow H$  be an isomorphism of groups. The inverse map of sets  $f^{-1} : H \rightarrow G$  is a group homomorphism (actually, an isomorphism).*

*Proof.* Exercise. □

*Example 4.16.* (1) Take the map  $f : \mathbb{Z}/4 \rightarrow D_8$  defined by  $f([k]) = r_k$  where  $r_k$  is rotation by  $k\pi/2$ . This is a group monomorphism.

(2) Take the map  $s : D_8 \rightarrow \mathbb{Z}/2$  sending a symmetry to 0 if it leaves the vertices of the square in cyclic order and to 1 if it doesn't. This is an epimorphism (it maps the rotations to 0 and the reflections to 1).

(3) Suppose  $m|n$  are positive integers. Then the map  $p : \mathbb{Z}/n \rightarrow \mathbb{Z}/m$ , defined as  $p([k]_n) = [k]_m$  is well-defined and an epimorphism of groups.

(4) The map  $\det : Gl(2, \mathbb{R}) \rightarrow \mathbb{R}^*$  is an epimorphism of groups.

If  $G$  is an abelian group, then taking powers is a homomorphism:

**Proposition 4.17.** *Let  $A$  be an abelian group. Write the operation as addition. The map  $n : A \rightarrow A$  defined by  $n(x) = nx$  is a homomorphism, for any  $n \in \mathbb{Z}$ .*

*Proof.* First, suppose  $n = 0$ . Then 0 is just the trivial homomorphism. If  $n > 0$ , then we have  $n(a + a') = na + na'$  since the group is abelian. If  $n = -1$ , then  $(-1)(a + a') = -(a + a') = -a' + (-a) = -a + (-a') = (-1)a + (-1)a'$ , again because  $A$  is abelian. Finally, if  $n < 0$ , then  $n(a) = (-1)(-n)(a)$  is a composition of two homomorphisms and hence a homomorphism. □

To understand groups, it is often helpful to look at their *subgroups* first (since those are smaller). We define the term next.

**Definition 4.18.** Let  $G$  be a group. A subset  $H \subset G$  is a *subgroup* if it is a group with the operation inherited from  $G$ . In this case we write  $H < G$ .

*Example 4.19.* (1)  $G$  itself is a subgroup of  $G$ , sometimes called *improper subgroup*.

- (2) If  $e$  is the neutral element of  $G$ , then the subset  $\{e\}$  is a subgroup, called *trivial subgroup*. Somewhat illogically, any subgroup of  $G$  that is neither trivial nor improper is called a *nontrivial* subgroup.
- (3) The subset  $\{-1, +1\} \subset \mathbb{R}^*$  is a subgroup.
- (4) The subset  $\mathbb{N} \subset \mathbb{Z}$  is *not* a subgroup.

There are a number of results allowing us to recognize if a given subset of a group is, in fact, a subgroup.

**Lemma 4.20.** *A nonempty subset  $H \subset G$  in a group is a subgroup if and only if for all pairs  $a, b \in H$ , the element  $ab^{-1}$  of  $G$  is in  $H$ .*

*Proof.* If  $H$  is a subgroup, then it contains a neutral element, that is an element  $e_H$  such that  $e_H h = h e_H = h$  for all  $h \in H$ . By Lemma 4.7 we conclude  $e_H = e$ , where  $e$  is the neutral element of  $G$ . Now suppose  $a, b \in H$ . Since  $H$  is a subgroup, there is  $c \in H$  such that  $bc = cb = e$ ; this implies  $c = b^{-1}$  (remember, inverses are unique), so  $b^{-1} \in H$ . But  $H$  is closed under the group operation (being a group...), hence  $ab^{-1} \in H$ .

Suppose conversely that for all  $a, b \in H \subset G$ , we have  $ab^{-1} \in H$ . First, choosing an element  $a \in H$ , we conclude that  $e = aa^{-1} \in H$ , so  $H$  has a neutral element. Next, choosing  $a = e$ , we see that  $b \in H \Rightarrow b^{-1} \in H$ , so  $H$  has inverses. Finally, for  $a, c \in H$ , writing  $b = c^{-1} \in H$ , we conclude that  $ac = ab^{-1} \in H$ , so  $H$  is closed under the operation. That is, the group operation induces an operation  $H \times H \rightarrow H$ , which is associative and has inverses and a neutral element - so  $H$  is a subgroup.  $\square$

*Example 4.21.* (1) The subset  $2\mathbb{Z} \subset \mathbb{Z}$  of even integers is a subgroup: If  $a, b$  are even, so is  $a - b$ .  
 (2)  $\mathbb{N} \subset \mathbb{Z}$  is not a subgroup -  $1, 2 \in \mathbb{N}$  but  $1 - 2$  is not.

An easy consequence of the above subgroup criterion is the fact that the intersection of an arbitrary family of subgroups is a subgroup.

**Corollary 4.22.** *Let  $G$  be group and  $\{H_\alpha | \alpha \in A\}$  a family of subgroups of  $G$ . Then  $\bigcap_{\alpha \in A} H_\alpha$  is a subgroup.*

*Proof.* Let  $a, b \in \bigcap_{\alpha \in A} H_\alpha$  be two elements of the intersection. For each  $\alpha \in A$ , we have  $ab^{-1} \in H_\alpha$  since  $H_\alpha$  is a subgroup. That is,  $ab^{-1} \in \bigcap_{\alpha \in A} H_\alpha$ , which proves the assertion by Lemma 4.20.  $\square$

Another, very similar criterion is the following.

**Lemma 4.23.** *A nonempty subset  $H \subset G$  in a group is a subgroup if and only if  $a \in H \Rightarrow a^{-1} \in H$  and  $a, b \in H \Rightarrow ab \in H$ .*

*Proof.* Suppose the two conditions of the lemma are satisfied. Then  $H$  is nonempty and  $a, b \in H \Rightarrow ab^{-1} \in H$ . Hence  $H < G$ , by Lemma 4.20.

Conversely, if  $H$  is a subgroup, then  $e \in H$  (see proof of 4.20). Now Lemma 4.20 easily implies the two conditions.  $\square$

*Example 4.24.* (1) The subset of upper triangular invertible matrices with 1's on the diagonal in  $Gl(2, \mathbb{R})$  is a subgroup.  
 (2) The subset of invertible diagonal matrices in  $Gl(2, \mathbb{R})$  is a subgroup.

*Remark 4.25.* If  $H < G$  is a subgroup, then we have a canonical group monomorphism  $i_H : H \rightarrow G$ , defined by  $i_H(g) = g$ . It is called the *embedding* of the subgroup  $H$ .

To each element  $g \in G$  in a group corresponds a subgroup *generated* by  $g$ .

**Lemma/Definition 4.26.** Let  $G$  be a group,  $g \in G$ . Write  $\langle g \rangle$  for the set  $\{g^n | n \in \mathbb{Z}\}$  of powers of  $g$  (if the group operation is written as addition, this is the set  $\{ng | n \in \mathbb{Z}\}$  of multiples of  $g$ ). Then  $\langle g \rangle$  is a subgroup of  $G$  called the subgroup generated by  $g$ . The number of elements in  $\langle g \rangle$  is denoted  $|g|$  and called the order of  $g$ .

*Proof.* We have to prove that  $\langle g \rangle$  is a subgroup. For this we use Lemma 4.20. Take two elements  $g^n$  and  $g^m$  of  $\langle g \rangle$ . Then  $g^n(g^m)^{-1} = g^{n-m} \in \langle g \rangle$ .  $\square$

*Remark 4.27.* If  $|g|$  is finite, then it is equal to the smallest positive integer  $n$  such that  $g^n = 1$ .

**Definition 4.28.** A group  $G$  such that there exists  $g \in G$  with  $\langle g \rangle = G$  is called *cyclic*, and such an element  $g$  is called a *generator* of  $G$ . Note that a cyclic group is abelian.

*Example 4.29.* (1) The group  $\mathbb{Z}$  is cyclic; the only two generators are 1 and  $-1$ .  
 (2) For  $n \geq 1$  the group  $\mathbb{Z}/n$  is cyclic. A congruence class  $[k] \in \mathbb{Z}/n$  is a generator if and only if  $\gcd(k, n) = 1$  (exercise: why is that so?).  
 (3) The group  $\mu_n = \{z \in \mathbb{C} | z^n = 1\}$  of  $n$ -th roots of unity is cyclic.

Subgroups of cyclic groups are themselves cyclic:

**Lemma 4.30.** Suppose  $G$  is a cyclic group and  $H < G$  is a subgroup. Then  $H$  is cyclic.

*Proof.* Choose a generator  $g$  of  $G$ . If  $H$  is the trivial subgroup, then it is cyclic. If  $H$  is non-trivial, then there is a smallest positive integer  $n$  such that  $g^n \in H$ . Suppose  $g^m \in H$ . Let  $k = \gcd(m, n)$ ; write  $k = am + bn$  with suitable  $a, b \in \mathbb{Z}$ . Then  $g^k = (g^m)^a(g^n)^b \in H$  and therefore  $k \geq n$ , so that  $n|m$ . That is,  $g^m = (g^n)^q$  for some  $q \in \mathbb{Z}$ . But this means that  $H = \langle g \rangle$ , so  $H$  is cyclic.  $\square$

Instead of subgroups generated by just one elements, we can also look at those generated by any set of elements.

**Lemma/Definition 4.31.** Let  $G$  be a group and  $S \subset G$  a subset (not necessarily a subgroup - just some collection of elements of  $G$ .) Then there is a smallest subgroup  $\langle S \rangle$  of  $G$  containing  $S$  ("smallest" means that any subgroup containing  $S$  also contains  $\langle S \rangle$ ), called the subgroup generated by  $S$ .

*Proof.* Just define  $\langle S \rangle$  as the intersection of all subgroups containing  $S$ . By Corollary 4.22, this is a subgroup; clearly it is the smallest subgroup containing  $S$ .  $\square$

**Definition 4.32.** Let  $G$  be a group. A subset  $S \subset G$  such that  $\langle S \rangle = G$  is called a *set of generators* for  $G$ .

*Example 4.33.* (1) For an element  $g \in G$ , we have  $\langle g \rangle = \langle \{g\} \rangle$ , so the notation is consistent.  
 (2) A set of generators for  $D_8$  is the set of reflections, or the set consisting of one of the reflections and the rotation by  $\pi/2$ .

Another important kind of subgroup associated to elements in a group in  $G$  is the *centralizer*.

**Lemma/Definition 4.34.** *Let  $S \subset G$  be a set of elements in a group. The set  $C_G(S) = \{g \in G \mid \forall s \in S : gs = sg\}$  is a subgroup of  $G$ , called the centralizer of  $S$  in  $G$ . If  $S = \{s\}$  has only one element, we write  $C_G(s)$  for  $C_G(\{s\})$ . The centralizer of  $C_G(G)$  of  $G$  itself is called center of  $G$  and usually denoted  $Z(G)$ .*

*Proof.* We have to prove that the centralizer of a subset is a subgroup. Clearly, we have  $C_G(S) = \bigcap_{s \in S} C_G(s)$ . Since the intersection of subgroups is a subgroup, it suffices to prove the assertion in case  $S$  has only one element  $s$ . We use Lemma 4.23. Suppose  $gs = sg$ . Then  $g^{-1}s = g^{-1}sgg^{-1} = g^{-1}gsg^{-1} = sg^{-1}$ . If, in addition,  $hs = sh$ , then  $(gh)s = gsh = s(gh)$ . So our criterion applies to show that  $C_G(s)$  is a subgroup.  $\square$

*Example 4.35.* (1) For any group  $G$ , the centralizer  $C_G(e)$  of the neutral element is  $G$ .  
 (2)  $G$  is abelian if and only if  $Z(G) = G$ .  
 (3) The center of  $Gl(2, \mathbb{R})$  is the group of nonzero multiples of the identity matrix.

Yet another supply of subgroups is produced by using group homomorphisms.

**Proposition/Definition 4.36.** *Let  $f : G \rightarrow H$  be a homomorphism of groups. Write  $e_H$  for the neutral element of  $H$ . The subset  $\{g \in G \mid f(g) = e_H\}$  is a subgroup, denoted by  $\ker(f)$ , the kernel of  $f$ .*

*Proof.* Suppose  $f(g) = e_H$ . Then  $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$ , so  $g \in \ker(f) \Rightarrow g^{-1} \in \ker(f)$ . Moreover, if  $g, h \in \ker(f)$ , then  $f(gh) = f(g)f(h) = e_H e_H = e_H$ , so  $gh \in \ker(f)$ . Thus Lemma 4.23 implies that  $\ker(f)$  is a subgroup, as asserted.  $\square$

*Example 4.37.* (1) If  $f : G \rightarrow H$  is a monomorphism, then  $\ker(f) = e_G$  is the trivial subgroup.  
 (2) The kernel of the determinant homomorphism  $\det : Gl(2, \mathbb{R}) \rightarrow \mathbb{R}^*$  is written  $Sl(2, \mathbb{R})$  and called *special linear group* (of dimension 2, over the real numbers). It is the set of all  $2 \times 2$  matrices with determinant 1.  
 (3) The kernel of the homomorphism  $s : D_8 \rightarrow \mathbb{Z}/2$  of Example 4.16 (2) consists exactly of the four rotations in  $D_8$ .  
 (4) The kernel of the homomorphism  $\mathbb{Z}/n \rightarrow \mathbb{Z}/m$  for  $m|n$  of Example 4.16 (3) is the set of all congruence classes  $[k]_n$  such that  $m|k$ .

The image of a group homomorphism is also a subgroup.

**Proposition/Definition 4.38.** *Let  $f : G \rightarrow H$ . Then the subset  $\{h \in H \mid \exists g \in G : f(g) = h\}$  (the image of  $f$ ) is a subgroup, written  $\text{im}(f)$  or  $f(G)$ .*

*Proof.* Exercise.  $\square$

*Example 4.39.* (1) If  $f : G \rightarrow H$  is an epimorphism, then  $\text{im}(f) = H$ .  
 (2) If  $G$  is any group and  $g \in G$ , then the image of the unique group homomorphism  $f_g : \mathbb{Z} \rightarrow G$  with  $f_g(1) = g$  is the subgroup  $\langle g \rangle$  generated by  $g$ .

## 5. PERMUTATIONS AND THE SYMMETRIC GROUPS

**Definition 5.1.** Let  $X$  be a set. A bijective map  $\sigma : X \rightarrow X$  is called a *permutation* of  $X$ .

*Example 5.2.* (1) The multiplication by  $n$  map  $n : \mathbb{Z} \rightarrow \mathbb{Z}$  is a permutation of  $\mathbb{Z}$  if and only if  $n = 1$  or  $n = -1$ .  
 (2) There are many other permutations of  $\mathbb{Z}$ !  
 (3) A set with two elements has exactly two permutations: The trivial one and the one that switches the two elements.

Let  $X$  be a set and write  $S_X$  for the set of permutations of  $X$ . Then there is an operation on  $S_X$  given by composition of maps (note that the composition of two bijective maps is again bijective). For two permutations  $\sigma$  and  $\tau$  of  $X$ , we write  $\sigma\tau$  for the composition  $\sigma \circ \tau$  and call this the *permutation product* (or simply *product*) of the two permutations.

**Lemma 5.3.** Let  $X$  be a set. Then the permutation product makes  $S_X$  into a group.

*Proof.* The identity permutation is a neutral element, and the inverse map of a permutation is an inverse.  $\square$

**Definition 5.4.** The permutation group of the set  $\{1, 2, \dots, n\}$  is written  $S_n$  (or  $\Sigma_n$ ) and called the *symmetric group of degree  $n$* .

**Lemma 5.5.** Let  $\phi \in S_n$ . Then  $\phi$  defines an equivalence relation on  $\{1, \dots, n\}$  in the following way:  $i \sim j$  if and only if there is an  $n \in \mathbb{Z}$  such that  $\phi^n(i) = j$ . The equivalence classes of this relation are called the *orbits* of  $\phi$ .

*Proof.* We have to show the relation defined in the statement of the lemma is symmetric, reflexive and transitive. This is an easy exercise.  $\square$

**Definition 5.6.** A permutation  $\sigma \in S_n$  is called a *cycle* if it has at most one orbit with more than one element. The number of elements in that largest orbit is called the *length* of the cycle. A cycle of length  $k$  may be written  $(a_1 a_2 \dots a_k)$  where  $a_1$  is an element of the largest orbit and  $a_i = \sigma^{i-1}(a_1)$  for  $1 \leq i \leq k$ . Two cycles are called *disjoint* if their largest orbits are disjoint. Finally, a cycle of length 2 is also called a *transposition*.

It turns out that any permutation can be written as a product of disjoint cycles in an essentially unique way. First, a preparatory lemma.

**Lemma 5.7.** Let  $\sigma$  and  $\tau$  be disjoint cycles in  $S_n$ . Then  $\sigma\tau = \tau\sigma$ , that is, they commute.

*Proof.* Write  $A = \{1, \dots, n\}$  and  $O_\sigma$  (resp.  $O_\tau$ ) for the largest orbit of  $\sigma$  (resp.  $\tau$ ). Let  $a \in A$ . If  $a$  is not in either  $O_\sigma$  or  $O_\tau$ , then  $\sigma\tau(a) = \tau\sigma(a) = a$ . If  $a \in O_\sigma$ , then so is  $\sigma(a)$  and hence  $\sigma\tau(a) = \sigma(a) = \tau\sigma(a)$  because  $O_\sigma$  and  $O_\tau$  are disjoint. Similarly if  $a \in O_\tau$ . That is, the maps  $\sigma$  and  $\tau$  commute, as asserted.  $\square$

Now for the cycle decomposition.

**Proposition 5.8.** Let  $\sigma \in S_n$  be a permutation. Then there is a product decomposition

$$\sigma = \sigma_1 \cdots \sigma_r$$

where the  $\sigma_i$  are pairwise disjoint cycles.

*Proof.* Let  $O_1, \dots, O_r$  be the orbits of  $\sigma$ . Write  $l_i$  for the number of elements in  $O_i$ . For each  $i$ , choose an element  $a_{i1} \in O_i$  and define  $a_{ij} = \sigma^{j-1}(a_{i1})$  for  $1 \leq j \leq l_i$ . Now define the cycles  $\sigma_i = (a_{i1}a_{i2} \dots a_{il_i})$ . By definition, the cycles  $\sigma_1, \dots, \sigma_r$  are disjoint and their product (in any order, see Lemma 5.7) is  $\sigma$ .  $\square$

Note that the cycles of length at least 2 in the cycle decomposition of  $\sigma$  are uniquely determined (namely, by the corresponding orbit of  $\sigma$ ).

The cycle decomposition is useful since cycles are easier to understand than general elements.

**Lemma 5.9.** *Any cycle can be written as a product of transpositions.*

*Proof.* Suppose we have a cycle  $\sigma = (a_1 \dots a_k)$ . Then  $\sigma = (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$ .  $\square$

**Corollary 5.10.** *Every element in  $S_n$  can be written as a product of transpositions. That is (in the language of Definition 4.32), the set of transpositions generates  $S_n$ .*

Note that there are many ways to write a given permutation as a product of transpositions! It turns out, however, that for a given permutation one always needs either an even or an odd number of transpositions - no permutation can be written as a product of an even number of transpositions *and* also as a product of an odd number of transpositions.

Let  $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$  be a function and  $\sigma \in S_n$  a permutation. Define a new function  $\pi(\sigma)(f)$  by  $\pi(\sigma)(f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ . It follows from this definition that  $\pi(\sigma)\pi(\tau) = \pi(\sigma\tau)$  for permutations  $\sigma, \tau \in S_n$ .

**Theorem 5.11.** *There is a unique homomorphism  $\epsilon : S_n \rightarrow \{+1, -1\}$  such that for every transposition  $\tau$  we have  $\epsilon(\tau) = -1$ .*

*Proof.* Let  $\Delta : \mathbb{Z}^n \rightarrow \mathbb{Z}$  be the function defined as

$$\Delta(x_1, \dots, x_n) = \prod_{i < j} (x_j - x_i)$$

with the product over all pairs of integers  $1 \leq i < j \leq n$ .

Now let  $\tau$  be a transposition, say  $\tau = (r s)$ . Say  $r < s$ . If we compute

$$\pi(\tau)(\Delta)(x_1, \dots, x_n) = \prod_{i < j} (x_{\tau(j)} - x_{\tau(i)})$$

we see that  $\pi(\tau)(\Delta) = -\Delta$ . For a permutation  $\sigma$ , set  $\epsilon(\sigma)$  to be the sign  $+1$  or  $-1$  such that  $\pi(\sigma)(\Delta) = \epsilon(\sigma)\Delta$ . Since  $\pi$  is multiplicative, we have that  $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$ , so  $\epsilon$  is a homomorphism, taking the value  $-1$  on each transposition. Uniqueness follows from the fact that  $S_n$  is generated by transpositions.  $\square$

*Notation 5.12.* A permutation  $\sigma$  is called *odd* if  $\epsilon(\sigma) = -1$ ; otherwise, it is called *even*. The kernel of  $\epsilon$  is written  $A_n$  and called the *alternating group* of degree  $n$ .

## 6. COSETS AND NORMAL SUBGROUPS

Recall that the group  $\mathbb{Z}/n$  is the set of congruence classes mod  $n$ . A congruence class mod  $n$  is in fact subset of  $\mathbb{Z}$  of the form  $a + n\mathbb{Z}$ . That is, it is a translate of the subgroup  $n\mathbb{Z}$  of  $\mathbb{Z}$ . Taken together, these translates give a partition of  $\mathbb{Z}$ . This can be generalized to any subgroup of an arbitrary group.

**Lemma/Definition 6.1.** *Let  $G$  be a group and  $H < G$  a subgroup. Then we obtain two equivalence relations on  $G$  as follows:*

- (1) *We say two elements  $g, g' \in G$  are right equivalent (under the action of  $H$ ), written  $g \sim_r g'$  if there exists a  $h \in H$  such that  $gh = g'$ .*
- (2) *We say  $g, g' \in G$  are left equivalent (under the action of  $H$ ), written  $g \sim_l g'$  if there exists a  $h \in H$  such that  $hg = g'$ .*

*Proof.* We have to prove the relations defined above are equivalence relations. The proof is similar in both cases, so we just deal with the right equivalence. The relation is clearly reflexive. If  $gh = g'$  then  $g = g'h^{-1}$  and  $h^{-1} \in H$  since  $H$  is a subgroup. That is, the relation is symmetric. Finally, if  $gh = g'$  and  $g'h' = g''$ , then  $g(hh') = g''$  and  $hh' \in H$  since  $H$  is a subgroup, so the relation is also transitive.  $\square$

*Notation 6.2.* We write  $G/H$  for the set of equivalence classes of the right relation; this set is called the set of *left cosets* of  $H$  in  $G$ .

Similarly, we write  $H \backslash G$  for the set of *right cosets* of  $H$  in  $G$ .

Note that the left coset of  $g \in G$  is the set  $gH$  of elements of the form  $gh$  for some  $h \in H$ . Since equivalence classes are either disjoint or equal, we conclude:

**Lemma 6.3.** *Suppose  $gH$  and  $g'H$  are cosets of  $H$  in  $G$ . If  $gH \cap g'H \neq \emptyset$ , then  $gH = g'H$ .*

In fact, all the cosets are of the same size.

**Lemma 6.4.** *Let  $gH$  and  $g'H$  be cosets of  $H$  in  $G$ . Then there is a bijective map of sets  $gH \rightarrow g'H$ .*

*Proof.* The map can be defined as multiplication with  $g'g^{-1}$  from the left: If  $gh \in gH$ , then  $g'g^{-1}gh = g'h \in g'H$ . It has multiplication with  $gg'^{-1}$  as inverse map, therefore it is bijective.  $\square$

Now we can immediately conclude the following important result.

**Theorem 6.5.** *Let  $G$  be a finite group and  $H < G$  a subgroup. Then*

$$|G| = |H||G/H|$$

*and similarly for right cosets.*

*Proof.* Choose a set of representatives  $x_1, \dots, x_r \in G$  of  $G/H$ . That is,  $x_iH \cap x_jH = \emptyset$  if  $i \neq j$  and  $G = \bigcup_{i=1}^r x_iH$ . Then  $|G| = \sum_{i=1}^r |x_iH|$ . By Lemma 6.4, we have that  $|x_iH| = |H|$  for all  $i$ ; also  $r = |G/H|$ . This proves the assertion.  $\square$

**Corollary 6.6.** *Let  $G$  be a finite group and  $H < G$  a subgroup. Then  $|H|$  divides  $|G|$ .*

**Corollary 6.7.** *Let  $G$  be a finite group and  $g \in G$  an element. Then the order of  $g$  divides the order of  $G$ .*

**Corollary 6.8.** *Let  $G$  be a finite group with  $|G| = n$  and  $g \in G$ . Then  $g^n = e$ .*

*Proof.* By the previous corollary,  $|g|$  divides  $n$ . Write  $n = |g|q$ . Then  $g^n = (g^{|g|})^q = e^q = e$ .  $\square$

We write  $(G : H)$  (or sometimes  $[G : H]$ ) for the cardinality of  $G/H$  (or  $H \backslash G$ ; it is easy to see they are always the same). The number  $(G : H)$  is called the *index* of  $H$  in  $G$ .

**Corollary 6.9.** *Let  $G$  be a finite group and  $H < G$  a subgroup. Then  $(G : H)$  divides the order of  $G$ .*

**Corollary 6.10.** *Let  $G$  be a finite group of prime order (that is,  $|G| = p$  is a prime number). Then  $G$  is cyclic.*

*Proof.* Let  $g \in G$  be an element such that  $g \neq e$ . Then the order of  $g$  is  $p$  (it divides  $p$  and is bigger than 1, and  $p$  is prime), so  $\langle g \rangle = G$  and  $G$  is cyclic.  $\square$

**Corollary 6.11.** *Let  $n > 1$  be an integer and  $a \in \mathbb{Z}$  such that  $\gcd(a, n) = 1$ . Then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .*

*Proof.* The order of  $\mathbb{Z}/n^*$  is  $\phi(n)$ . Now the assertion follows from Corollary 6.8.  $\square$

**Corollary 6.12.** *Let  $p$  be a prime and  $a$  an integer not divisible by  $p$ . Then  $a^p \equiv a \pmod{p}$ .*

*Proof.* Just observe that  $\phi(p) = p - 1$  and use the previous corollary.  $\square$

Next, we investigate those subgroups whose left and right cosets coincide; these are called normal subgroups.

**Definition 6.13.** Let  $G$  be a group. A subgroup  $H < G$  is called a *normal* subgroup, written  $H \triangleleft G$  if  $gH = Hg$  for all  $g \in G$ .

It is often easier to check the following criterion.

**Proposition 6.14.** *A subgroup  $H < G$  is normal if and only if for all  $g \in G$  and  $h \in H$  we have  $ghg^{-1} \in H$ .*

*Proof.* Suppose first that  $H$  is normal. Let  $g \in G$  and  $h \in H$ . Since  $gH = Hg$ , we know that there exists  $h' \in H$  such that  $gh = h'g$ . Thus,  $ghg^{-1} = h' \in H$ , as asserted.

Conversely, assume that for all  $g \in G$  and  $h \in H$ ,  $ghg^{-1} \in H$ . Let  $g \in G$  and  $h \in H$ . Then  $gh = (ghg^{-1})g \in Hg$  and  $hg = g(g^{-1}hg) \in gH$ , so  $gH = Hg$ , and  $H$  is normal.  $\square$

**Corollary 6.15.** *Let  $G$  be an abelian group and  $H < G$  a subgroup. Then  $H$  is a normal subgroup.*

*Proof.* Suppose  $g \in G$  and  $h \in H$ . Then  $ghg^{-1} = h \in H$  since  $G$  is abelian.  $\square$

**Corollary 6.16.** *Let  $G$  be a group and  $H < G$  a subgroup contained in the center  $Z(G)$ . Then  $H$  is normal.*

*Proof.* As for the previous corollary.  $\square$

**Corollary 6.17.** *Let  $f : G \rightarrow G'$  be a homomorphism of groups. Then the kernel  $\ker(f)$  is a normal subgroup of  $G$ .*

*Proof.* We saw in Proposition 4.36 that  $\ker(f)$  is a subgroup. Now suppose  $h \in \ker(f)$  and  $g \in G$ . Then  $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g^{-1}) = f(g)f(g)^{-1} = e$ . That is,  $ghg^{-1} \in \ker(f)$ . Now Proposition 6.14 proves the assertion.  $\square$

*Example 6.18.* (1) Every subgroup of  $\mathbb{Z}$  is normal.

(2) The alternating group  $A_n$  is a normal subgroup of the symmetric group  $S_n$ .

(3) The special linear group  $Sl(n, \mathbb{R})$  of  $n \times n$  matrices with determinant 1 is a normal subgroup of  $Gl(n, \mathbb{R})$ .

(4) The subgroup of rotations in  $D_4$  is a normal subgroup.

If  $H$  is not a normal subgroup, it is still true that  $gHg^{-1}$  is a subgroup (though not necessarily  $H$  again).

**Proposition 6.19.** *Let  $H < G$  be a subgroup and  $g \in G$ . Then the subset  $gHg^{-1}$  is again a subgroup of  $G$  (called a conjugate subgroup). Moreover, the groups  $H$  and  $gHg^{-1}$  are isomorphic.*

*Proof.* Let  $ghg^{-1} \in H$ . Then  $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$ . Moreover, if in addition  $gh'g^{-1} \in gHg^{-1}$ , then  $(ghg^{-1})(gh'g^{-1}) = g(hh')g^{-1} \in gHg^{-1}$ . We conclude that  $gHg^{-1}$  is a subgroup.

We have a map  $c_g : H \rightarrow gHg^{-1}$  given by  $c_g(h) = ghg^{-1}$ . We saw above that  $c_g(hh') = c_g(h)c_g(h')$  for all  $h, h' \in H$ , so  $c_g$  is a homomorphism. Moreover, the map  $c_{g^{-1}} : gHg^{-1} \rightarrow g^{-1}(gHg^{-1})g = H$  is inverse to  $c_g$ , so it is an isomorphism.  $\square$

**Corollary 6.20.** *Let  $G$  be a finite group and suppose  $H < G$  is the only subgroup of order  $|H|$ . Then  $H$  is normal.*

*Proof.* By the proposition,  $|gHg^{-1}| = |H|$  for all  $g \in G$ , and  $gHg^{-1}$  is a subgroup for all  $g \in G$ . Since  $H$  was assumed to be the only subgroup of order  $|H|$ , we conclude that  $H = gHg^{-1}$  for all  $g \in G$ . That is,  $H$  is normal.  $\square$

For an arbitrary subgroup  $H < G$ , there is a "largest" subgroup in which it is normal.

**Lemma/Definition 6.21.** *Let  $H < G$  be a subgroup. Then*

$$N_G(H) = \{g \in G \mid \forall h \in H : ghg^{-1} \in H\}$$

*is a subgroup of  $G$  called the normalizer of  $H$  in  $G$ .*

*Proof.* Let  $g, g' \in N_G(H)$  and  $h \in H$ . Then  $(gg')h(gg')^{-1} = g(g'hg'^{-1})g^{-1} \in H$  and  $g^{-1}hg = (gh^{-1}g^{-1})^{-1} \in H$ . Hence  $N_G(H)$  is a subgroup, as claimed.  $\square$

*Remark 6.22.* A subgroup is normal in its normalizer.

**Lemma 6.23.** *Let  $H < G$  be a subgroup and  $K < G$  a subgroup such that  $H \triangleleft K$ . Then  $K < N_G(H)$ .*

We have seen that a kernel of a group homomorphism is a normal subgroup. The converse is also true: If a subgroup is normal, then there is a group homomorphism of which it is the kernel.

**Theorem 6.24.** *Let  $G$  be a group and  $N \triangleleft G$  a normal subgroup. Then there is a unique group structure on the set of left cosets  $G/N$  such that the canonical map  $G \rightarrow G/N$  sending  $g \in G$  to its left coset  $gN \in G/N$  is a group homomorphism.*

*Proof.* We first prove uniqueness. Write the group operation of  $G/N$  as  $*$ . Since the canonical map (assuming it exists) is a homomorphism, we have necessarily  $(gN) * (hN) = ghN$ ,  $e_{G/N} = e_G N$  and  $(gN)^{-1} = g^{-1}N$ . But this determines the group structure (it tells us what the group operation, neutral element and inverses are), so it is unique.

We just saw how the group structure on  $G/N$  must look if it exists. To show existence, it suffices to prove that  $(gN) * (hN) = ghN$  is well-defined (from that

it will follow that  $N = e_G N$  is a neutral element and  $g^{-1}N$  is an inverse of  $gN$ . So suppose that  $gN = g'N$  and  $hN = h'N$ . That means  $g = g'n_1$  and  $h = h'n_2$  for some  $n_1, n_2 \in N$ . We have to show that  $(gh)N = (g'h')N$ . Let  $(gh)n \in (gh)N$ . Now

$$(gh)n = (g'n_1h'n_2)n = (g'h'h'^{-1}n_1h'n_2)n = (g'h')((h'^{-1}n_1h')n_2n) \in (g'h')N.$$

Similarly,  $g'h'n \in (gh)N$  for all  $n \in N$ , so  $(gh)N = (g'h')N$ . That is, the operation  $(gN) * (hN) = (gh)N$  is well-defined on  $G/N$ .  $\square$

**Definition 6.25.** The group  $G/N$  is called *quotient group* of  $G$  by  $N$  (or sometimes *factor group* of  $G$  by  $N$ ). The canonical map  $G \rightarrow G/N$  is sometimes called *canonical projection*.

*Example 6.26.* The group  $\mathbb{Z}/n\mathbb{Z}$  is the one we called  $\mathbb{Z}/n$ .

Next we prove, as promised, that any normal subgroup is the kernel of some homomorphism.

**Lemma 6.27.** *The kernel of the canonical homomorphism  $G \rightarrow G/N$  is exactly  $N$ .*

*Proof.* We have  $gN = eN$  if and only if  $g \in N$ .  $\square$

We can now prove the "first isomorphism theorem". If a map  $f$  is a composition of maps,  $f = f_n \circ \dots \circ f_2 \circ f_1$  we say that we have a *factorization* of  $f$  (into the maps  $f_1, \dots, f_n$ ), or that  $f$  *factors* as composition of  $f_1, \dots, f_n$ . If  $n = 2$  we also say that  $f$  *factors through*  $f_2$ .

**Theorem 6.28.** *Let  $\phi : G \rightarrow G'$  be a homomorphism of groups and  $K = \ker(\phi)$ . Then  $\phi$  factors as*

$$G \rightarrow G/K \rightarrow \phi(G) \rightarrow G'$$

where the first homomorphism is the canonical projection, the second is an isomorphism and the third is the inclusion of the subgroup  $\phi(G)$  into  $G'$ .

*Proof.* If we want the assertion to be true, we have to define the homomorphism  $\tilde{\phi} : G/K \rightarrow \phi(G)$  as  $\tilde{\phi}(gK) = \phi(g)$ . Since  $\phi(gk) = \phi(g)\phi(k) = \phi(g)$  for all  $g \in G$  and  $k \in K$ , the map  $\tilde{\phi}$  is well-defined. Moreover,  $\tilde{\phi}((gK)(hK)) = \tilde{\phi}(ghK) = \phi(gh) = \phi(g)\phi(h) = \tilde{\phi}(gK)\tilde{\phi}(hK)$  because  $\phi$  is a homomorphism, so  $\tilde{\phi}$  is a homomorphism. Clearly,  $\tilde{\phi}$  factors through the inclusion  $\phi(G) = \tilde{\phi}(G/K) \rightarrow G'$ , is surjective onto its image  $\phi(G)$  and is injective since the kernel of  $\tilde{\phi}$  is trivial:

$$\tilde{\phi}(gK) = e_{G'} \Leftrightarrow \phi(g) = e_{G'} \Leftrightarrow g \in K \Leftrightarrow gK = K = e_{G/K}.$$

That is,  $\tilde{\phi} : G/K \rightarrow \phi(G)$  is an isomorphism and we have the factorization asserted.  $\square$

*Remark 6.29.* The first isomorphism theorem contains two important assertions. First, that the groups  $G/K$  and  $\phi(G)$  are isomorphic. Second, that the isomorphism is induced by the homomorphism  $\phi$  and is not just a random isomorphism.

**Corollary 6.30.** *Let  $\phi : G \rightarrow G'$  be a homomorphism of finite groups. Then  $|\phi(G)|$  divides both  $|G|$  and  $|G'|$ .*

*Proof.* By the first isomorphism theorem,  $|\phi(G)| = [G : H]$ , which divides  $|G|$ . Also,  $\phi(G)$  is a subgroup of  $G'$ , hence  $|\phi(G)|$  divides  $|G'|$ .  $\square$

**Corollary 6.31.** *Let  $G$  be a cyclic group of order  $n$ . Then there is an isomorphism  $\mathbb{Z}/n \cong G$ .*

*Proof.* Choose a generator  $g$  of  $G$ . The map  $f_g : \mathbb{Z} \rightarrow G$  defined as  $f_g(n) = g^n$  is a homomorphism. Because  $g$  is a generator,  $f_g$  is surjective. On the other hand, the order of  $g$  is  $n$ , again because  $g$  is a generator of the cyclic group  $G$  of order  $n$ . Therefore, the kernel of  $f_g$  is  $n\mathbb{Z} < \mathbb{Z}$ . Now the first isomorphism theorem implies that  $\mathbb{Z}/n \cong G$ .  $\square$

*Remark 6.32.* Note that the isomorphism in the corollary depends on the choice of the generator  $g$ .

**Corollary 6.33.** *The index of the alternating group in the symmetric group is 2. Hence,  $|A_n| = n!/2$ .*

*Proof.* The alternating group is the kernel of the homomorphism  $\epsilon : S_n \rightarrow \{+1, -1\}$  (see Theorem 5.11 for the definition of  $\epsilon$ ). Since  $\epsilon$  is onto, the first isomorphism theorem implies that there is an isomorphism  $S_n/A_n \cong \{+1, -1\}$ . That is,  $[S_n : A_n] = 2$ . Finally,  $|S_n| = |A_n|[S_n : A_n]$  by Theorem 6.5, so that  $|A_n| = \frac{1}{2}|S_n| = n!/2$ .  $\square$

Another application of the first isomorphism theorem is the computation of the set of homomorphisms from one group to another. Namely, the isomorphism theorem tells us that a homomorphism  $\phi : G \rightarrow G'$  is the same thing as a triple  $(K, \psi, H)$  where  $K$  is a normal subgroup of  $G$  (the kernel of  $\phi$ ),  $H$  is a subgroup of  $G'$  (the image  $\phi(G)$ ) and  $\psi : G/K \rightarrow H$  is an isomorphism (the induced one, called  $\tilde{\phi}$  in the proof of Theorem 6.28). That is we can in principle compute  $\text{Hom}(G, G')$  if we know all subgroups of  $G'$ , all normal subgroups of  $G$ , and all isomorphisms from quotient groups of  $G$  to subgroups of  $G'$ . In practice this is of course very difficult in general, but it is of theoretical importance.

*Example 6.34.* Let  $G = S_3$  and  $G' = \mathbb{Z}/6$ . The normal subgroups of  $S_3$  are  $\{id\}$ ,  $A_3$  and  $S_3$  itself. Since every subgroup of  $\mathbb{Z}/6$  is abelian,  $\{id\}$  cannot be the kernel of a homomorphism  $G \rightarrow G'$ . Next,  $S_3$  is the kernel of the trivial homomorphism. Finally,  $S_3/A_3 \cong \mathbb{Z}/2$ , so any homomorphism with kernel  $A_3$  has image of order 2. The only subgroup of order 2 in  $\mathbb{Z}/6$  is the one generated by  $[3]$ . Since there is only one isomorphism  $S_3/A_3 \rightarrow \langle [3] \rangle$ , we conclude that  $\text{Hom}(S_3, \mathbb{Z}/6)$  has two elements. As a group (see homework), we have  $\text{Hom}(S_3, \mathbb{Z}/6) \cong \mathbb{Z}/2$ .

As a further application, we prove *Cauchy's theorem for abelian groups*. We need an easy preparatory result.

**Lemma 6.35.** *Let  $G$  be a cyclic group of order  $n$  and suppose  $m|n$ . Then  $G$  contains an element of order  $m$ .*

*Proof.* Choose a generator  $g$  of  $G$ . Let  $n = qm$ . Then  $g^q$  has order  $m$ .  $\square$

**Theorem 6.36.** *Let  $G$  be a finite abelian group and  $p$  a prime dividing the order of  $G$ . Then  $G$  contains an element of order  $p$ .*

*Proof.* We use induction on the order  $n$  of  $G$ . If  $n = 1$ , then the statement is vacuously true. So assume  $n > 1$  and we have know the assertion holds true for all abelian groups of order less than  $n$ . If  $G$  has no nontrivial subgroup, then it is cyclic, so the previous lemma completes the proof. Now suppose there is a nontrivial

subgroup  $H < G$ . If  $p$  divides the order of  $H$ , then the inductive hypothesis implies we have an element of order  $p$  in  $H$  and we are done. Otherwise,  $H$  is normal in  $G$  (because  $G$  is abelian), and the order of  $G/H$  is less than  $n$ . Again by the inductive hypothesis,  $G/H$  contains an element of order  $p$  (note  $p$  divides  $[G : H]$  since we assumed it does not divide  $|H|$ ), say  $bH$ . Since  $bH$  has order  $p$ , we conclude that  $b^p \in H$ . Let  $q$  be the order of  $b^p$ . Then  $\gcd(p, q) = 1$ , or else  $p$  divides the order of  $H$ , a contradiction. Now  $b^q \neq e_G$ . Indeed suppose that  $b^q = e_G$ . Write  $1 = xp + yq$  for suitable  $x, y \in \mathbb{Z}$ . Then  $(bH) = (bH)^{xp+yq} = e_{G/H}$  (because  $b^p \in H$  and  $b^q \in H$ ). Hence  $bH$  has order 1, in contradiction to our assumption. So  $b^q \neq e_G$ . Since  $(b^q)^p = e_G$ , we conclude that  $b^q$  has order  $p$ , completing the induction step and proving the theorem.  $\square$

## 7. AUTOMORPHISMS OF GROUPS

In this section, we study the set  $\text{Aut}(G)$  of automorphisms of a group  $G$  (recall that an automorphism of a  $G$  is an isomorphism  $G \rightarrow G$ ). We will see that  $\text{Aut}(G)$  is a group, we will calculate this group for  $G$  a cyclic group, and we will in general break the group of automorphisms into two parts, the so called inner and outer automorphisms.

**Lemma 7.1.** *Let  $G$  be a group. The operation of composition of maps defines a group structure on  $\text{Aut}(G)$ .*

*Proof.* The set of automorphisms is closed under composition since the composition of bijective maps is bijective and the composition of homomorphisms is a homomorphism. The identity map of  $G$  is clearly an automorphism and a neutral element with respect to composition. Finally, we saw in Lemma 4.15 that the inverse map of an isomorphism is an isomorphism, so the inverse  $\phi^{-1}$  to an automorphism  $\phi$  is an automorphism and is inverse with respect to the operation of composition. Finally, composition of maps is associative.  $\square$

*Remark 7.2.* Note that  $\text{Aut}(G)$  is a subgroup of the group  $S_G$  of permutations of the group  $G$ .

If two groups  $G$  and  $G'$  are isomorphic, then so are their groups of automorphisms.

**Theorem 7.3.** *Let  $G \cong G'$  be two isomorphic groups. Then  $\text{Aut}(G) \cong \text{Aut}(G')$ .*

*Proof.* Let  $\phi : G \rightarrow G'$  be an isomorphism with inverse  $\phi^{-1}$ . We define a map  $\phi_{\#} : \text{Aut}(G) \rightarrow \text{Aut}(G')$  by  $\phi_{\#}(f) = \phi \circ f \circ \phi^{-1}$ . It is easy to check that this is a homomorphism with inverse  $(\phi^{-1})_{\#}$ , hence an isomorphism.  $\square$

Now we can easily compute the automorphism group of a cyclic group (up to isomorphism, of course).

**Theorem 7.4.** *Suppose  $G$  is a cyclic group of order  $n$ . Then  $\text{Aut}(G) \cong \mathbb{Z}/n^*$ .*

*Proof.* By Theorem 7.3 and Corollary 6.31, we may as well assume  $G = \mathbb{Z}/n$ . We define a map  $f : \text{Aut}(\mathbb{Z}/n) \rightarrow \mathbb{Z}/n^*$  by  $f(\phi) = \phi([1])$ . First, since  $\phi$  is an automorphism and  $[1]$  is a generator of  $\mathbb{Z}/n$ , we conclude that  $\phi([1])$  is a generator, too; that is,  $\phi([1]) \in \mathbb{Z}/n^*$ . That is,  $f$  really is a map  $\text{Aut}(\mathbb{Z}/n) \rightarrow \mathbb{Z}/n^*$ . Now  $\phi([k]) = \phi([1])[k]$  for all  $[k] \in \mathbb{Z}/n$  (because  $\phi$  is a homomorphism). In particular,  $f(\phi \circ \psi) = \phi(\psi([1]) = \phi([1])\psi([1]) = f(\phi)f(\psi)$ , so  $f$  is a homomorphism.

Since  $[1]$  is a generator,  $\phi([1]) = \psi([1])$  implies that  $\phi = \psi$ , so that  $f$  is injective. Finally, the "multiplication by  $m$ " homomorphism  $m \cdot : \mathbb{Z}/n \rightarrow \mathbb{Z}/n$  is an automorphism if  $\gcd(m, n) = 1$ , and then  $f(m \cdot) = [m]$ , so that  $f$  is surjective.

To summarize,  $f$  is a one-to-one and onto homomorphism, that is, an isomorphism.  $\square$

We will see later how to analyze more general abelian groups. Next, we will study the automorphisms of groups that are not abelian.

**Lemma 7.5.** *Let  $G$  be a group,  $g \in G$ . Then the map  $c_g : G \rightarrow G$ , defined as  $c_g(h) = ghg^{-1}$  is an automorphism of  $G$ .*

*Proof.* The map  $c_{g^{-1}}$  is an inverse. Also,  $c_g(hh') = g(hh')g^{-1} = ghg^{-1}gh'g^{-1} = c_g(h)c_g(h')$ .  $\square$

**Definition 7.6.** The automorphism  $c_g$  for a  $g \in G$  is called an *inner automorphism*. The set of all inner automorphisms of  $G$  is denoted  $\text{Inn}(G)$ .

**Proposition 7.7.** *The subset  $\text{Inn}(G) \subset \text{Aut}(G)$  is a normal subgroup.*

*Proof.* We have  $c_{gh} = c_g \circ c_h$  and  $c_g^{-1} = c_{g^{-1}}$ , so  $\text{Inn}(G)$  is closed under composition and inverses and hence is a subgroup of  $\text{Aut}(G)$ . If  $\phi \in \text{Aut}(G)$ , then  $\phi c_g \phi^{-1} = c_{\phi(g)}$ , and therefore  $\text{Inn}(G)$  is normal.  $\square$

**Definition 7.8.** The quotient group  $\text{Aut}(G)/\text{Inn}(G)$  is called the group of *outer automorphisms* of  $G$  and written  $\text{Out}(G)$ . Note that an element in this group, an "outer automorphism", is not really an automorphism of  $G$  at all, but rather a coset of automorphisms.

The group of inner automorphisms is pretty easy to compute from  $G$  itself.

**Theorem 7.9.** *Let  $G$  be a group. The map  $g \mapsto c_g$  induces an isomorphism of groups  $G/Z(G) \cong \text{Inn}(G)$ .*

*Proof.* Clearly, the map is surjective. Since  $c_{gh} = c_g c_h$ , it is a homomorphism. Now, if  $g$  is in the kernel of this homomorphism, then  $c_g(h) = ghg^{-1} = h$  for all  $h \in G$ , hence  $gh = hg$  for all  $h \in G$ . That is, the kernel is precisely the center  $Z(G)$  of  $G$ . Now the first isomorphism theorem 6.28 implies the assertion.  $\square$

*Example 7.10.* (1) Abelian groups have no non-trivial inner automorphisms.  
(2) For  $n > 2$ ,  $\text{Inn}(S_n) \cong S_n$ , since the center of  $S_n$  is trivial.

## 8. ABELIAN GROUPS

We want to break groups down into their basic parts, and start by showing how finite abelian groups can be decomposed. We start by defining a group structure on the cartesian product of groups.

**Definition 8.1.** Let  $G$  and  $H$  be groups. The group  $G \times H$ , called (*direct*) *product* of  $G$  and  $H$ , is the set of ordered pairs  $(g, h)$  with  $g \in G$  and  $h \in H$  with the following group structure:

- (1) The group operation is defined componentwise:  $(g, h) * (g', h') = (gg', hh')$ .
- (2) The neutral element is  $(e_G, e_H)$ .
- (3) The inverse is also defined componentwise:  $(g, h)^{-1} = (g^{-1}, h^{-1})$ .

More generally, suppose  $\{G_i | i \in I\}$  is a family of groups indexed by a set  $I$ . Then we define the product group  $\prod_{i \in I} G_i$  to be the set of ordered families  $(g_i | i \in I)$  with  $g_i \in G_i$ , with componentwise operation as group operation, neutral element  $(e_{G_i} | i \in I)$  and componentwise inverses.

*Remark 8.2.* For any family  $\{G_i | i \in I\}$  of groups and index  $j \in I$  the projection  $p_j : \prod_{i \in I} G_i \rightarrow G_j$  defined as  $p_j((g_i | i \in I)) = g_j$  is a homomorphism.

**Lemma 8.3.** *Let  $G$  and  $H$  be groups. Then the twisting map*

$$\tau : G \times H \longrightarrow H \times G$$

*defined as  $\tau(g, h) = (h, g)$  is an isomorphism.*

**Lemma 8.4.** *Let  $\{G_i | i \in I\}$  be a family of groups indexed by a set  $I$ . Then the product  $\prod_{i \in I} G_i$  is abelian if and only if every one of the groups  $G_i$  is abelian.*

*Proof.* The projections are surjective, so if the product is abelian, so are all the factors. The converse is trivial.  $\square$

If we are dealing with a collection of abelian groups, then there is another way to collect them into a new group, called direct sum. If  $X$  is a set, we say that *almost all* elements  $x \in X$  have a property if that property is true for all but finitely many  $x$  (this includes the possibility that the property is true for all  $x$ ). If  $X$  is finite, this is an empty condition, that is, every property is satisfied by almost all  $x$  (for example, almost all humans have green hair).

**Definition 8.5.** Let  $\{A_i | i \in I\}$  be a family of abelian groups indexed by a set  $I$ ; write the group operations as addition. We define a new abelian group, the *direct sum* of the groups  $A_i$ , to be the set

$$\bigoplus_{i \in I} A_i = \{(a_i | i \in I) | a_i = 0_{A_i} \text{ for almost all } i\}.$$

The group operation is defined componentwise, the neutral element is  $(0_{A_i} | i \in I)$  and inverses are taken componentwise (exercise: check that the direct sum is closed under the group operation).

**Lemma 8.6.** *Let  $\{A_i | i \in I\}$  be a family of abelian groups indexed by a set  $I$ . There is a natural homomorphism*

$$\bigoplus_{i \in I} A_i \longrightarrow \prod_{i \in I} A_i$$

*which is an isomorphism if  $I$  is a finite set.*

*Proof.* Clearly, the set  $\bigoplus_{i \in I} A_i$  is just a subset of  $\prod_{i \in I} A_i$  and the inclusion map is a homomorphism. As noted above, the "almost all" condition in the definition of the direct sum is empty if  $I$  is finite, so that the sets  $\bigoplus_{i \in I} A_i$  and  $\prod_{i \in I} A_i$  are just equal in this case.  $\square$

So finite direct sums are "the same" as finite direct products; this is absolutely false for infinite sums/products.

**Lemma 8.7.** *Let  $A$  be an abelian group and  $\{B_i < A | i \in I\}$  a family of subgroups indexed by a set  $I$ . Then there is a natural homomorphism*

$$s : \bigoplus_{i \in I} B_i \longrightarrow A$$

defined by  $s((b_i|i \in I)) = \sum_{i \in I} b_i$  (note that the sum on the right hand side is actually finite, since  $b_i = 0$  for almost all  $i \in I$ ).

*Proof.* The assignment  $(b_i|i \in I) \mapsto s((b_i|i \in I))$  clearly defines a map; it is a homomorphism because  $A$  is abelian.  $\square$

*Notation 8.8.* In a situation as above, we call the image of  $s$  the *sum* of the subgroups  $B_i$ , denoted  $\sum_{i \in I} B_i$  (if there also finitely many subgroups, we also write  $B_1 + \cdots + B_n$  for the sum of  $B_1, \dots, B_n$ ).

Let  $A$  be an abelian group and  $p$  a prime number. We write  $A(p)$  for the group of elements of  $A$  that are annihilated by some power of  $p$ :

$$A(p) = \{a \in A | \exists n \geq 0 : p^n a = 0\}.$$

The *torsion subgroup*  $A_{tors}$  of  $A$  is the group of all elements annihilated by some integer:

$$A_{tors} = \{a \in A | \exists n > 0 : na = 0\}.$$

We say that  $A$  is a torsion (abelian) group if  $A_{tors} = A$ . Clearly, any finite abelian group is a torsion group.

For a positive integer  $r$ , let  $A_r$  denote the subgroup of elements of  $A$  annihilated by  $r$ , that is, the kernel of the multiplication by  $r$  homomorphism.

**Theorem 8.9.** *Let  $A$  be a torsion abelian group. Then the natural homomorphism (see Lemma 8.7)*

$$s : \bigoplus_{p \text{ prime}} A(p) \longrightarrow A$$

*is an isomorphism.*

*Proof.* Suppose  $(a_p) \in \bigoplus_{p \text{ prime}} A(p)$  is an element such that  $s((a_p)) = \sum_p a_p = 0$ . Let  $l$  be a prime number. Then  $a_l = -\sum_{q \neq l} a_q$ , where the right hand side is actually a finite sum, say, over primes  $\{q_1, \dots, q_r\}$ . For each  $q_i$  there is a natural number  $k_i$  such that  $q_i^{k_i} a_{q_i} = 0$ . Let  $N = \prod_{i=1}^r q_i^{k_i}$ . Then  $N a_l = 0$ . On the other hand, there is a  $k$  such that  $l^k a_l = 0$ , since  $a_l \in A(l)$ . We conclude that  $\gcd(N, l^k) a_l = 0$ . But  $\gcd(N, l^k) = 1$ . That is,  $a_l = 0$ . Since  $l$  was arbitrary, we conclude that  $a_p = 0$  for all  $p$ . Thus, the kernel of  $s$  is 0 and  $s$  is injective.

On the other hand, to see that  $s$  is onto it suffices to prove the following.

**Claim:** Suppose  $r$  and  $t$  are relatively prime positive integers. Then  $A_{rt} = A_r + A_t$ .

To prove the claim, let  $a \in A_{rt}$  and suppose the order of  $a$  is  $n$ . Because  $(rs)a = 0$ , we know that  $n|rs$ . Since  $\gcd r, t = 1$ , we can write  $n = uv$  with  $u|r$  and  $v|t$  in a unique way; clearly  $\gcd(u, v) = 1$ . Write  $1 = ux + vy$ . Now the order of  $ua$  is  $v$ , so  $ua \in A_t$ , and the order of  $va$  is  $u$ , so  $va \in A_r$ . Consequently,  $a = yva + xua \in A_r + A_t$ ; since  $a$  was arbitrary, we conclude that  $A_{rt} = A_r + A_t$ .

Given the claim, the surjectivity of  $s$  follows by an easy induction argument. Indeed, if  $a \in A$  has order  $n$  and  $n = p_1^{k_1} \cdots p_i^{k_i}$  is the prime factor decomposition, then induction shows that  $a \in \sum_{j=1}^i A_{p_j^{k_j}} \subset \sum_{j=1}^i A(p_j)$ .  $\square$

**Corollary 8.10.** *Let  $A$  be a finite abelian group. Then there is an isomorphism*

$$A \cong \prod_{p \text{ prime}} A(p)$$

*Proof.* A finite abelian group is always a torsion group. Thus Theorem 8.9 together with Lemma 8.6 proves the assertion.  $\square$

Next, we will analyze the groups  $A(p)$ .

**Lemma 8.11.** *Suppose  $A$  is a finite abelian group such that  $A = A(p)$ . Then  $A$  is a  $p$ -group, that is, the order of  $A$  is a power of  $p$ .*

*Proof.* Follows immediately from Theorem 6.36.  $\square$

*Remark 8.12.* Let  $A$  be a finite abelian  $p$ -group. Let  $b$  be an element of  $A$ , not equal to 0. Let  $k \geq 0$  be an integer such that  $p^k b \neq 0$ , and let  $p^m$  be the order of  $p^k b$ . Then  $b$  has order  $p^{k+m}$ .

**Definition 8.13.** Let  $A$  be a finite abelian  $p$ -group. Let  $r_1, \dots, r_s$  be integers  $\geq 1$ . We say that  $A$  is of *type*  $(p^{r_1}, \dots, p^{r_s})$  if there is an isomorphism

$$A \cong \mathbb{Z}/p^{r_1} \times \mathbb{Z}/p^{r_2} \times \dots \times \mathbb{Z}/p^{r_s}$$

Now we come to the main structure result for finite abelian  $p$ -groups.

**Theorem 8.14.** *Every finite abelian  $p$ -group  $A$  is isomorphic to a product of cyclic  $p$ -groups. If it is of type  $(p^{r_1}, \dots, p^{r_s})$  with  $r_1 \geq r_2 \geq \dots \geq r_s \geq 1$ , then the sequence of integers  $(r_1, \dots, r_s)$  is uniquely determined.*

*Proof.* The proof is by induction on the order of  $A$ . Choose an element  $a_1$  of maximal order  $p^{r_1}$ , say, and let  $A_1 = \langle a_1 \rangle$  be the cyclic subgroup generated by  $a_1$ . If  $A$  is cyclic, then  $A = A_1$  and we are done.

**Claim:** Let  $\bar{b}$  be an element of  $A/A_1$  of order  $p^k$ . Then there exists a representative  $a$  of  $\bar{b}$  such that the order of  $a$  is also  $p^k$ .

Indeed, let  $b$  be a representative of  $\bar{b}$ . Then  $p^k b \in A_1$ ; say,  $p^k b = na_1$  for some integer  $n \geq 0$ . We can as well assume that  $n = p^i$  for some  $i \leq r_1$  (by replacing the generator  $a_1$ , if necessary). By the preceding remark, the order of  $b$  is  $p^{k+r_1-i}$ . Since  $a_1$  had maximal order, we conclude that  $k+r_1-i \leq r_1$  or  $k \leq i$ . This means there is  $c \in A_1$  such that  $p^k b = p^k c$ . Set  $a = b - c$ . Then  $a$  is a representative of  $\bar{b}$  and  $p^k a = 0$ ; since the order of  $a$  is at least  $p^k$ , we conclude it is actually equal to  $p^k$ .

Now back to the proof of the theorem. By induction,

$$A/A_1 \cong \overline{A_2} \times \dots \times \overline{A_s}$$

where  $\overline{A_i}$  is a cyclic group of order  $p^{r_i}$  and  $r_2 \geq r_3 \geq \dots \geq r_s$ . Choose generators  $\overline{a_i}$  of  $\overline{A_i}$ , and use the claim to lift them to elements  $a_2, \dots, a_s$  with  $a_i$  an element of  $A$  of order  $p^{r_i}$ . Let  $A_i$  be the subgroup generated by  $a_i$ . We have a natural homomorphism (see Lemma 8.7)

$$S : \bigoplus_{i=1}^s A_i \longrightarrow A.$$

We claim this is an isomorphism. Since the source and target of  $S$  are finite groups of the same order, it suffices to show that  $S$  is injective. So, let  $x = m_1 a_1 + \dots + m_s a_s$  be in the kernel of  $S$ , with  $0 \leq m_i < p^{r_i}$ . Then  $m_2 \overline{a_2} + \dots + m_s \overline{a_s} = 0$  in  $A/A_1$ , so  $m_2 = \dots = m_s = 0$  and hence  $m_1 = 0$ , too. Thus,  $x = 0$  and  $S$  is injective, as claimed. Now the existence of the product decomposition follows from the fact that finite products and direct sums are isomorphic.

Finally, the uniqueness of type is also proved easily by induction on the order of  $A$ .  $\square$

Now Theorem 8.9 and Theorem 8.14 imply immediately the structure theorem for finite abelian groups:

**Theorem 8.15.** *Let  $A$  be a finite abelian group. Then there is a decomposition, unique up to re-ordering,*

$$A \cong \prod_i A_i$$

where  $A_i$  is a cyclic group of prime-power order.

We also note the following fact about products of cyclic groups.

**Proposition 8.16.** *If  $A$  is cyclic of order  $n$ ,  $B$  is cyclic of order  $m$  and  $\gcd n, m = 1$ , then  $A \times B$  is cyclic of order  $mn$ .*

*Proof.* Let  $a$  be a generator of  $A$  and  $b$  a generator of  $B$ . Let  $d$  be the order of  $(a, b) \in A \times B$ . That is,  $d(a, b) = (da, db) = (0_A, 0_B)$ . Therefore,  $n|d$  and also  $m|d$ . Since  $n$  and  $m$  are relatively prime, this implies that  $mn|d$  and  $d \geq mn$ . But clearly,  $d \leq mn$ , so  $d = mn = |A \times B|$  and  $A \times B$  is cyclic.  $\square$

Let us use this theorem to make a list of all abelian groups of a given order, up to isomorphism:

*Example 8.17.* The following is a list of all abelian groups of order 60:

- (1)  $\mathbb{Z}/60 \cong \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/5$ .
- (2)  $\mathbb{Z}/30 \times \mathbb{Z}/2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5$

That is it, already.

This example shows that to get "many" abelian groups of a given order  $n$ , the number  $n$  needs to have prime factors in high powers. In particular, we conclude the following.

**Corollary 8.18.** *Let  $n$  be a squarefree positive integer (that is, all its prime factors occur in the first power only). Then any abelian group  $A$  of order  $n$  is cyclic.*

*Proof.* Let  $n = p_1 p_2 \cdots p_r$  be the prime factor decomposition of  $n$  (note the primes  $p_i$  are pairwise different). Then

$$A \cong \mathbb{Z}/p_1 \times \mathbb{Z}/p_2 \times \cdots \times \mathbb{Z}/p_r \cong \mathbb{Z}/n$$

by Theorem 8.15. Here the second isomorphism follows from Proposition 8.16 and the fact that any cyclic group of order  $n$  is isomorphic to  $\mathbb{Z}/n$  (see Corollary 6.31).  $\square$

## 9. GROUP ACTIONS

Up to now we have studied groups as abstract objects, and in relation to one another. Now we will investigate how groups *act* on sets; for example (as we already know from examples), groups can describe the symmetries of a geometric object. We will then study in detail various naturally defined actions of the group on itself and on its set of subgroups and use those actions to gain further insight into the structure of groups (particularly those that are not abelian).

**Definition 9.1.** Let  $G$  be a group. A (left) action of  $G$  on a set  $X$  is a map  $G \times X \rightarrow X$ , usually denoted by  $(g, x) \mapsto gx$ , or  $(g, x) \mapsto g \cdot x$ , or  $(g, x) \mapsto g(x)$ , such that

- (1) For all  $x \in X$ ,  $e \cdot x = x$ .
- (2) For all  $g, h \in G$  and  $x \in X$ , we have  $g \cdot (h \cdot x) = (gh) \cdot x$ .

If  $G$  acts on  $X$  we also say that  $X$  (with this specified action) is a  $G$ -set.

*Example 9.2.* (1) The group  $D_8$  of symmetries of the square acts on the set of vertices of the square, the set of edges of the square, the set consisting of the points on the boundary of the square,...

- (2) The group  $S_n$  acts on the set  $\{1, 2, \dots, n\}$ .
- (3) The group  $Gl(n, \mathbb{R})$  acts on  $\mathbb{R}^n$  via matrix multiplication.
- (4) Any group  $G$  acts on itself by left multiplication: an element  $g \in G$  acts via  $h \mapsto gh$ .
- (5) Every group  $G$  acts on itself by conjugation: an element  $g \in G$  acts via  $h \mapsto ghg^{-1}$ .
- (6) Every group  $G$  acts on the set of its subgroups  $\text{Sub}(G)$  by conjugation: an element  $g \in G$  acts via  $H \mapsto gHg^{-1}$  on subgroups  $H < G$  (see Proposition 6.19 for the fact that the conjugate of a subgroup is again a subgroup).

In fact, the example of the symmetric group acting on the set  $\{1, 2, \dots, n\}$  is especially instructive and in some sense universal.

**Proposition 9.3.** Suppose a group  $G$  acts on a set  $X$ , and let  $S_X$  be the group of permutations of  $X$ . For each  $g \in G$ , the translation map

$$\tau_g : X \longrightarrow X, \tau_g(x) = g \cdot x$$

is a permutation of  $X$  and the map  $\rho : G \rightarrow S_X$  defined by  $\rho(g) = \tau_g$  is a homomorphism.

*Proof.* The first assertion is that the map  $\tau_g$  is bijective. In fact, the map  $\tau_{g^{-1}}$  is inverse to  $\tau_g$  since for all  $x \in X$ ,  $\tau_g(\tau_{g^{-1}}(x)) = g \cdot (g^{-1} \cdot x) = e \cdot x = x$  by the properties of a group action, and similarly  $\tau_{g^{-1}}(\tau_g(x)) = x$ . So  $\tau_g$  is a permutation of  $X$ .

Now for all  $x \in X$ , we have  $\rho(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \rho(g)(\rho(h)(x))$  so that  $\rho(gh) = \rho(g)\rho(h)$  and  $\rho$  is a homomorphism.  $\square$

The converse of Proposition 9.3 is also true.

**Proposition 9.4.** Let  $G$  be a group,  $X$  a set and  $\rho : G \rightarrow S_X$  a homomorphism. Then the map  $G \times X \rightarrow X$  defined as  $(g, x) \mapsto \rho(g)(x)$  is an action of  $G$  on  $X$

*Proof.* Exercise.  $\square$

**Corollary 9.5.** Let  $G$  be a group acting on a set  $X$  via a homomorphism  $\rho : G \rightarrow S_X$  and let  $\phi : H \rightarrow G$  be a homomorphism. Then  $H$  acts on  $X$  by "restricting" the  $G$ -action, that is via the homomorphism  $\rho \circ \phi : H \rightarrow S_X$ .

The action of a group on itself via left multiplication has the following very helpful consequence.

**Theorem 9.6 (Cayley).** Let  $G$  be a group. Then  $G$  is isomorphic to a subgroup of the group of permutations  $S_G$ .

*Proof.* The action by left multiplication defines a homomorphism  $\rho : G \rightarrow S_G$ . Since for  $g, h \in G$ ,  $gh = h$  implies  $g = e$ , the kernel of this homomorphism is  $\{e\}$ . By the first isomorphism theorem 6.28,  $G$  is isomorphic to the image of  $\rho$ , a subgroup of  $S_G$ .  $\square$

*Remark 9.7.* Suppose  $X$  and  $Y$  are sets such that there is a bijective map  $\phi : X \rightarrow Y$ . Then  $S_X \cong S_Y$ . Indeed, there is a natural isomorphism  $\phi_{\#} : S_X \rightarrow S_Y$  defined by  $\phi_{\#}(\sigma) = \phi \circ \sigma \circ \phi^{-1}$ . Compare with Theorem 7.3.

The preceding remark and Cayley's theorem imply the next corollary.

**Corollary 9.8.** *Let  $G$  be a finite group. Then there is a positive integer  $n$  and a subgroup  $H < S_n$  such that  $G \cong H$ .*

*Proof.* Choose  $n = |G|$ . The fact that the order of  $G$  is  $n$  exactly means that there is a bijective map  $G \rightarrow \{1, 2, \dots, n\}$ . Now apply the remark and Cayley's theorem 9.6.  $\square$

**Definition 9.9.** Suppose a group  $G$  acts on a set  $X$  via the homomorphism  $\rho : G \rightarrow S_X$ . We say that the action is *faithful* if  $\rho$  is injective, that is,  $g \cdot x = x \forall x \in X \Rightarrow g = e$ .

*Example 9.10.* (1) The action of  $Gl(n, \mathbb{R})$  on  $\mathbb{R}^n$  is faithful.  
 (2) The action of a group on itself via left multiplication is faithful.  
 (3) The action of a group  $G$  on itself via conjugation has the center  $Z(G)$  as kernel, so it is faithful if and only if the center is trivial (note that in this example, the homomorphism  $\rho$  is the natural map from  $G$  to  $\text{Inn}(G)$ ).

Next we study how a group action on the set  $X$  decomposes it into equivalence classes, called orbits, and determine the size of the orbits.

**Proposition 9.11.** *Let  $G$  be a group acting on a set  $X$ . The relation on  $x$  such that*

$$x \sim x' \iff \exists g \in G : g \cdot x = x'$$

*is an equivalence relation.*

*Proof.* (Compare the proof of 6.1). First of all,  $e \cdot x = x$ , so the relation is reflexive. Moreover,  $g \cdot x = x' \iff g^{-1}x' = x$ , so the relation is symmetric. Finally, if  $g \cdot x = x'$  and  $h \cdot x' = x''$ , then  $(hg) \cdot x = x''$ , so the relation is transitive.  $\square$

The equivalence classes of the relation defined above are called the *orbits* of the action; if  $x \in X$ , its equivalence class is *the orbit of  $x$* , often denoted  $G \cdot x$ . The set of all the orbits is usually denoted  $X/G$ .

Now, if  $G$  acts on  $X$  and  $x \in X$ , how can we describe the orbit of  $x$ ? To do that, we first need to look at all those group elements fixing  $x$ .

**Lemma 9.12.** *Let  $G$  be a group acting on a set  $X$  and  $x \in X$ . The subset  $G_x = \{g \in G | g \cdot x = x\}$  is a subgroup, called the stabilizer of  $x$  in  $G$ .*

*Proof.* If  $g \in G_x$  and  $h \in G_x$  then  $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$  so  $gh \in G_x$ . Moreover,  $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ , so  $g^{-1} \in G_x$ . Hence  $G_x$  is a subgroup.  $\square$

We need a technical result about equivalence relations.

**Lemma 9.13.** *Let  $X$  be a set and  $\sim$  an equivalence relation on  $X$ . Write  $X/\sim$  for the set of equivalence classes. Suppose  $f : X \rightarrow Y$  is a map such that  $x \sim x' \Leftrightarrow f(x) = f(x')$ . Then  $f$  induces an injective map  $\bar{f} : X/\sim \rightarrow Y$ .*

*Proof.* Write  $[x]$  for the equivalence class of  $x \in X$ . The induced map is defined as  $\bar{f}([x]) = f(x)$ . The hypothesis ensures this is well-defined and injective. (Compare to the proof of the first isomorphism theorem 6.28).  $\square$

Now we can describe the orbits of an action.

**Theorem 9.14.** *Let  $G$  be a group acting on a set  $X$  and  $x \in X$ . Then there is a natural bijection  $G/G_x \rightarrow G \cdot x$ . In particular,  $|G \cdot x| = [G : G_x]$ .*

*Proof.* There is a map  $f_x : G \rightarrow X$  defined as  $f_x(g) = g \cdot x$ . If  $h \in G_x$  then  $g \cdot x = (gh) \cdot x$  and vice versa, so  $f_x$  is constant on the cosets  $gG_x$  and induces an injective map  $G/G_x \rightarrow X$ , with image the orbit  $G \cdot x$  of  $X$ , by the preceding lemma. Thus, we obtain the asserted bijection  $G/G_x \rightarrow G \cdot x$ .  $\square$

**Definition 9.15.** Let  $G$  be a group acting on a set  $X$ . We say the action is *transitive* if there is only one orbit, that is,  $G \cdot x = X$  for any  $x \in X$ .

*Example 9.16.* The preceding result enables us to compute the order of the symmetry group of an object. For example, suppose we want to compute the order of the symmetry group  $G$  of the cube.  $G$  acts on the set  $\mathcal{F}$  of faces of the cube transitively, and the stabilizer of a face is isomorphic to the symmetry group of a square, which we know to have 8 elements. Since there are 6 faces, we conclude that  $|G| = 48$ .

The following result is also called the *orbit formula*.

**Theorem 9.17.** *Let  $G$  be a group acting on a finite set  $X$ . Let  $\{x_1, \dots, x_r\}$  be a set of representatives for the orbits of the action (that is, the disjoint union of the orbits  $G \cdot x_i$  is  $X$ ). Then we have the equation*

$$|X| = \sum_{i=1}^r [G : G_{x_i}]$$

*Proof.* By hypothesis, we have

$$|X| = \sum_{i=1}^r |G \cdot x_i|.$$

Now apply Theorem 9.14.  $\square$

Next, we calculate the number of orbits of an action. For a group  $G$  acting on a set  $X$  and  $g \in G$ , we write  $\text{fix}(g) = X^g = \{x \in X | g \cdot x = x\}$  for the set of elements fixed by  $g$ .

**Theorem 9.18** (Burnside's Theorem). *Let  $G$  be a finite group acting on a finite set  $X$ . Then the number of orbits can be expressed as*

$$|X/G| = (1/|G|) \sum_{g \in G} |X^g|$$

*Proof.* Since  $X$  is the disjoint union of its orbits, we may as well assume that the action is transitive. In that case there is only one orbit, so we only have to show that  $|G| = \sum_{g \in G} |X^g|$ . We can re-write the right hand side of this equation as  $\sum_{x \in X} |G_x|$ . Since the action is transitive,  $|G_x|$  does not depend on  $x$  and in fact, by Theorem 9.14,  $|X||G_x| = |G|$ , proving our assertion.  $\square$

The most important example where we apply these results is the action of a group on itself by conjugation.

**Definition 9.19.** Let  $G$  be a group. Recall that  $G$  acts on itself via conjugation. If  $h \in G$ , then the orbit of  $h$  with respect to the conjugation action is called the *conjugacy class* of  $h$  (in  $G$ ),

$$K_G(h) = \{h' \in G \mid \exists g \in G : ghg^{-1} = h'\}.$$

**Lemma 9.20.** Let  $G$  be a group acting on itself via conjugation,  $h \in G$ . The stabilizer of  $h$  under this action is equal to the centralizer of  $h$  in  $G$ ,

$$G_h = C_G(h) = \{g \in G \mid ghg^{-1} = h\}.$$

*Proof.* Obvious from the definitions.  $\square$

Now Theorem 9.14 implies

**Proposition 9.21.** Let  $G$  be a group and  $h \in G$ . Then

$$|K_G(h)| = [G : C_G(h)].$$

In this context, Theorem 9.17 becomes the *class equation*.

**Theorem 9.22.** Let  $G$  be a finite group,  $Z(G)$  the center of  $G$  and  $\{a_1, \dots, a_s\}$  a set of representatives for the conjugacy classes of  $G$  not contained in  $Z(G)$  (that is, each of the conjugacy classes of  $G$  that is not contained in the center contains exactly one of the  $a_i$ ). Then

$$|G| = |Z(G)| + \sum_{i=1}^s [G : C(a_i)].$$

*Proof.* A conjugacy class not contained in  $Z(G)$  is disjoint from  $Z(G)$ , since every element in the center is the only element of its conjugacy class. Therefore  $G - Z(G) = \bigcup_{i=1}^s K_G(a_i)$ . In light of Definition 9.19 and Proposition 9.21, Theorem 9.17 implies that

$$|G| = |Z(G)| + \sum_{i=1}^s [G : C_G(a_i)]$$

as asserted.  $\square$

**Corollary 9.23.** Let  $p$  be a prime and  $G$  a finite  $p$ -group. Then  $Z(G)$  is non-trivial, that is,  $|Z(G)| > 1$ .

*Proof.* For any  $g \in G$ ,  $[G : C_G(g)] \mid |G|$  and therefore is a power of  $p$ . The class equation implies that the order of  $Z(G)$  must be divisible by  $p$ . On the other hand, it is at least 1. This implies that  $|Z(G)| \geq p > 1$ .  $\square$

Many more important applications of the orbit formula arise from studying the action of a group  $G$  by conjugation on the set of subgroups of  $G$ . As for elements, we call the orbit of a subgroup  $H$  of  $G$  under this action the conjugacy class of the subgroup, denoted  $K_G(H)$ . Write  $\text{Sub}(G)$  for the set of subgroups of  $G$ .

**Lemma 9.24.** *Let  $G$  be a group,  $H < G$  a subgroup. Then the stabilizer of  $H$  in  $G$  with respect to the conjugation action of  $G$  on  $\text{Sub}(G)$  is the normalizer  $N_G(H)$  of  $H$  in  $G$  (see 6.21 for the definition of the normalizer subgroup).*

*Proof.* Immediate from the definitions.  $\square$

**Theorem 9.25.** *Let  $G$  be a finite group and  $p$  the smallest prime dividing the order of  $G$ . Suppose  $H < G$  is a subgroup of index  $p$ . Then  $H$  is normal.*

*Proof.*  $G$  acts on  $K_G(H)$ , with the stabilizer of  $H$  being  $N_G(H)$ . Since  $H < N_G(H)$  and the index of  $H$  is prime, we have that either  $N_G(H) = G$  or  $N_G(H) = H$ . In the former case,  $H$  is normal and we are done.

In the latter case,  $|K_G(H)| = [G : N_G(H)] = [G : H] = p$ , so the action of  $G$  on  $K_G(H)$  defines a homomorphism  $\rho : G \rightarrow S_p \cong S_{K_G(H)}$ . Let  $K$  be the kernel of  $\rho$ . Then  $K = \bigcap_{g \in G} ghg^{-1} < H$ . In particular,  $[G : K] \geq p$ . On the other hand,  $G/K$  is isomorphic to a subgroup of  $S_p$  by the first isomorphism theorem, so  $[G : K]$  divides both  $|G|$  and  $p! = |S_p|$ . Since  $p$  is the smallest prime dividing  $|G|$ , we have  $\gcd(|G|, p!) = p$ . Therefore  $[G : K] = p$  and  $K = H$ . Hence  $H$  is the kernel of a homomorphism, so it is normal.  $\square$

## 10. SYLOW THEOREMS

In group theory, finite groups are often studied by investigating their subgroups of prime-power order and the way these assemble to reconstruct the group. The Sylow Theorems assert that there is a plentiful supply of such subgroups of the maximal prime=power order possible, and give some information about how these are related. We begin by proving Cauchy's Theorem.

**Theorem 10.1 (Cauchy).** *Let  $G$  be a finite group,  $p$  a prime and assume  $p$  divides the order of  $G$ . Then  $G$  contains an element of order  $p$ .*

*Proof.* By induction on the group order. Clearly, if  $|G| = p$ , then we are done. So suppose  $|G| > p$  and we have proved the assertion for all groups of smaller order. If  $G$  contains any proper subgroup  $H$  of order divisible by  $p$ , we are done by induction.

Otherwise, let  $g \in G$ . The centralizer  $C(g)$  is a subgroup; it is either all of  $G$  (in which case  $g \in Z(G)$ ) or a proper subgroup of order not divisible by  $p$ . In the latter case,  $p \nmid |K_G(g)|$  by the orbit-stabilizer formula. Now the class equation 9.22 implies that  $p$  divides the order of the center of  $G$ , so by our assumption that there are no proper subgroups of order divisible by  $p$ ,  $G$  is abelian, and we are done by Cauchy's Theorem for abelian groups 6.36.  $\square$

**Definition 10.2.** Let  $G$  be a finite group and  $p$  a prime. assume  $n$  is maximal such that  $p^n \mid |G|$ . A subgroup  $P < G$  of order  $p^n$  is called a  $p$ -Sylow subgroup of  $G$ .

We will now prove that there always is a  $p$ -Sylow subgroup.

**Theorem 10.3.** *Let  $G$  be a finite group,  $p$  a prime and  $n$  maximal such that  $p^n \mid |G|$ . Then  $G$  has a subgroup  $P$  of order  $p^n$ .*

*Proof.* By induction on the order of  $G$ . The statement is trivial if the order is prime. Now assume the order of  $G$  is not prime, and we have proved the assertion for all groups of smaller order. If  $G$  has a proper subgroup of index prime to  $p$ , we are done. Otherwise, we show as in the proof of Cauchy's Theorem 10.1 that the center  $Z(G)$  is non-trivial and has order divisible by  $p$ . Choose an element  $g \in Z(G)$  of order  $p$ .

The subgroup  $H = \langle g \rangle$  is normal in  $G$  (as it is contained in the center). Note that the highest power of  $p$  dividing  $|G/H|$  is  $p^{n-1}$ . By induction on the group order,  $G/H$  has a  $p$ -Sylow subgroup  $Q$  of order  $p^{n-1}$ . Let  $P = HQ = \{g \in G \mid gH \in Q\}$ ; then  $P$  is a  $p$ -group that has  $H$  as normal subgroup such that  $P/H = Q$ ; that is,  $|P| = p^n$ .  $\square$

We proceed to study the conjugacy classes of  $p$ -Sylow subgroups.

**Theorem 10.4.** *Let  $G$  be a finite group,  $p$  a prime, and  $P$  and  $Q$  two  $p$ -Sylow subgroups of  $G$ . Then  $P$  is conjugate to  $Q$ .*

*Proof. Step 1:* Let  $N(P)$  be the normalizer of  $P$ . Suppose  $Q < N(P)$ . I claim then  $Q = P$ .

Indeed, to see that it suffices to show that  $Q \subset P$ ; assume  $q \in Q - P$  and let  $R = \langle P, q \rangle$ . Then any element in  $R$  can be written in the form  $pq^i$  for some  $p \in P$  and integer  $i$ , because  $q \in N(P)$ . Let  $pq^i$  be such an element; suppose  $|q^i| = p^r$  (it will always be a power of  $p$  since  $q \in Q$ , a  $p$ -group). Now for any  $n$ ,  $(pq^i)^n = p'q^{in}$  for some  $p' \in P$ , again because  $q \in N(P)$ . In particular,  $(pq^i)^{p^r} \in P$ , so that  $|pq^i| \mid p^{pr}$ . Therefore  $R$  is a  $p$ -group contained in  $G$  and containing  $P$  as a proper subgroup; this is a contradiction, as  $P$  is a maximal  $p$ -subgroup of  $G$ .

**Step 2:**  $G$  acts on the set  $X$  of all the conjugates of  $P$ . Since  $N(P)$  contains  $P$ , we have that  $|X|$  is prime to  $p$ . Now we observe that  $Q$  also acts on the set of conjugates of  $P$  (restrict from  $G$ ); by the orbit-stabilizer formula and since  $Q$  is a  $p$ -group, this action has to have a fixed point. That is, there is a conjugate  $P'$  of  $P$  such that  $Q < N(P')$ . By Step 1, this means  $Q = P'$ ; that is,  $Q$  is a conjugate of  $P$ , as asserted.  $\square$

**Corollary 10.5.** *Let  $G$  be a finite group and  $p$  a prime. Write  $n_p$  for the number of  $p$ -Sylow subgroups of  $G$  and  $r$  for the maximal integer such that  $p^r \mid |G|$ . Then:*

- (1)  $n_p \equiv 1 \pmod{p}$
- (2)  $n_p \mid |G|/p^r$

*Proof.* Let  $X$  be the set of all  $p$ -Sylow subgroups and  $P \in X$ . Then  $P$  acts on  $X$  by conjugation and this action has precisely one fixed point, namely  $P$  itself. This follows from Step 1 of the proof of Theorem 10.4. Since  $P$  is a  $p$ -group, the first assertion follows from the orbit-stabilizer formula.

The second assertion is an immediate consequence of the fact that the action of  $G$  on  $X$  by conjugation is transitive and the orbit-stabilizer formula.  $\square$

## 11. SOLVABLE AND SIMPLE GROUPS

**Definition 11.1.** A group  $G$  is called solvable if there exists a chain  $G = G^{(0)} > G^{(1)} > \dots > G^{(r)} = \{e\}$  of subgroups such that for all  $i \geq 0$

- (1)  $G^{(i+1)} \triangleleft G^{(i)}$  and
- (2) the quotient group  $G^{(i)}/G^{(i+1)}$  is abelian.

**Lemma 11.2.** *Let  $\pi : G \rightarrow \Gamma$  be a surjective homomorphism of groups with kernel  $H \triangleleft G$ . Then  $G$  is solvable if and only if  $H$  and  $\Gamma$  are both solvable.*

*Proof.* First suppose  $G$  is solvable, with chain  $G^{(i)}$ . Set  $H^{(i)} = G^{(i)} \cap H$ ; then  $H^{(i+1)} \triangleleft H^{(i)}$  and  $H^{(i)}/H^{(i+1)} < G^{(i)}/G^{(i+1)}$  and therefore abelian. Hence  $H$  is solvable. Now set  $\Gamma^{(i)} = \pi(G^{(i)})$ . Since  $\pi$  is surjective,  $\Gamma^{(i+1)} \triangleleft \Gamma^{(i)}$  and there

are induced epimorphisms  $\pi_{i,i+1} : G^{(i)}/G^{(i+1)} \rightarrow \Gamma^{(i)}/\Gamma^{(i+1)}$  so that the latter quotients are abelian as well; thus,  $\Gamma$  is solvable.

Assume conversely that  $H$  is solvable with chain  $H^{(0)} > \cdots > H^{(r)}$  and  $\Gamma$  is solvable with chain  $\Gamma^{(0)} > \cdots > \Gamma^{(s)}$ . Set  $G^{(i)} = \pi^{-1}(\Gamma^{(i)})$  for  $0 \leq i \leq s$ , and  $G^{(i)} = H^{(i-s)}$  for  $s \leq i \leq s+r$ . Then the subgroups  $G^{(i)}$  form a chain satisfying the conditions of definition 11.1, and therefore  $G$  is solvable.  $\square$

**Corollary 11.3.** *Let  $p$  be a prime and  $P$  a finite  $p$ -group. Then  $P$  is solvable.*

*Proof.* As shown in Corollary 9.23, the center  $Z(P)$  of  $P$  is non-trivial.  $Z(P)$  is abelian, and therefore trivially solvable; and  $P/Z(P)$  has smaller order than  $P$ . Now proceed by induction on the group order.  $\square$

**Definition 11.4.** Let  $G$  be a group.  $G$  is called simple if the only normal subgroups of  $G$  are  $\{e\}$  and  $G$  itself.

**Lemma 11.5.** *A finite abelian group  $A$  is simple if and only if its order is a prime.*

*Proof.* Any subgroup of an abelian group is normal, so  $A$  is simple if and only if it has no non-trivial subgroups. By the Cauchy theorem, this is the case precisely if  $A$  is cyclic of prime order.  $\square$

**Definition 11.6.** Let  $G$  be a group and  $g, h \in G$  be elements. The commutator of  $g$  and  $h$  is the element  $[g, h] = ghg^{-1}h^{-1}$ . Note that  $[g, h] = e$  if and only if  $gh = hg$ . The commutator subgroup of  $G$  is the subgroup  $G' = [G, G]$  generated by the set of all commutators.

**Lemma 11.7.** *Let  $G$  be a group and  $[G, G]$  its commutator subgroup.*

- (1) *The subgroup  $[G, G]$  is normal.*
- (2) *Let  $A$  be an abelian group and  $f : G \rightarrow A$  a homomorphism. Then  $[G, G] \subset \ker(f)$ .*
- (3) *The quotient group  $G/[G, G]$  is abelian.*
- (4) *Let  $A$  be an abelian group. There is a natural one-to-one correspondence between homomorphisms  $f : G/[G, G] \rightarrow A$  and homomorphisms  $\tilde{f} : G \rightarrow A$  given by  $\tilde{f} = f \circ \pi$  where  $\pi : G \rightarrow G/[G, G]$  is the natural projection.*

*Proof.* The first statement is proved by an easy direct calculation. We only need to show that for  $k \in G$  and  $[g, h]$  a commutator,  $k[g, h]k^{-1}$  is a product of commutators. In fact,  $k[g, h]k^{-1} = [kg, h][h, k]$ . The second assertion is immediate from the observation that  $f([g, h]) = [f(g), f(h)]$  and  $[f(g), f(h)] = e$  since  $A$  is abelian. The third assertion is also clear: if  $\pi$  is canonical projection, then  $[\pi(g), \pi(h)] = \pi([g, h]) = e$  for all  $g$  and  $h$  in  $G$ ; since  $\pi$  is surjective, this proves that the quotient is abelian. Finally, the fourth assertion follows from surjectivity of  $\pi$  and (2).  $\square$

**Corollary 11.8.** *Let  $G$  be a group. If  $G$  is solvable, then  $[G, G] \neq G$ .*

*Proof.* Suppose  $G$  is solvable. Then there exists a non-trivial abelian group  $A$  and surjective homomorphism  $p : G \rightarrow A$ . By Lemma 11.7, the kernel of  $p$  contains  $[G, G]$ . Since  $A \neq \{e\}$ , we conclude that  $[G, G] \neq G$ .  $\square$

**Corollary 11.9.** *The alternating group on five letters  $A_5$  is simple.*

*Proof.* It is an extended exercise to show that any group of order less than  $60 = |A_5|$  is solvable. Hence, if  $A_5$  were not simple, it would be solvable. Therefore it suffices to show that  $[A_5, A_5] = A_5$ , by the previous corollary. Now  $A_5$  is generated by 3-cycles, and it is an easy calculation that any 3-cycle is a commutator of 3-cycles. This finishes the proof.  $\square$

## 12. COMPOSITION SERIES AND JORDAN-HÖLDER THEOREM

In this section, we study how to build finite groups out of finite simple groups.  
**Content to come.**

## 13. RINGS AND FIELDS

Many of the algebraic objects in mathematics are not just groups, but have more than one operation.

*Example 13.1.* The set of integers  $\mathbb{Z}$  has two operations, addition and multiplication. Under addition,  $\mathbb{Z}$  is an abelian group; the multiplication is associative, commutative, has a unit 1 and both operation together satisfy a distributive law.

*Example 13.2.* The set  $M_2(\mathbb{R})$  of real  $2 \times 2$ -matrices has two operations, addition and multiplication of matrices. It is an abelian group with the addition operation, the multiplication is associative and has a unit  $I_2$ , but is not commutative, and there is a distributive law for addition and multiplication.

*Example 13.3.* The set  $2\mathbb{Z}$  of even integers has two operations, addition and multiplication. It is an abelian group with operation the addition, the multiplication is associative and commutative, but there is no unit, and there is a distributive law.

*Example 13.4.* The set  $C(\mathbb{R})$  of real-valued continuous functions on the real numbers has two operations, addition and multiplication. It is an abelian group with the addition operation, the multiplication is associative and commutative and has a unit (the constant function 1), and there is a distributive law.

*Example 13.5.* The set  $\mathbb{Z}/n$  of congruence classes mod  $n$  has addition and multiplication operations, is an abelian group with the addition operation, the multiplication is associative and commutative and has a unit, and there is a distributive law.

**Definition 13.6.** A ring  $R$  is a non-empty set together with two binary operation called addition  $(a, b) \mapsto a + b$  and multiplication  $(a, b) \mapsto ab$  such that the following are satisfied.

- (1)  $R$  with the operation  $+$  is an abelian group.
- (2) Multiplication is associative.
- (3) There are distributive laws  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .

*Remark 13.7.* Rings are in particular abelian groups, so we can apply what we know already.

*Example 13.8.* Let  $\{R_i | i \in I\}$  be a family of rings. Then the product  $\prod_{i \in I} R_i$  is a ring with componentwise addition and multiplication.

We always write 0 for the additive neutral element of a ring, and  $n \cdot a$  for  $n$ -fold sum of an element  $a$  of the ring with itself, for  $n \in \mathbb{Z}$  positive, as for abelian groups. If  $n$  is negative, we write  $n \cdot a$  for the  $|n|$ -fold sum of  $-a$  with itself.

**Lemma 13.9.** *Let  $R$  be a ring.*

- (1) *For all  $a \in R$ , we have  $a0 = 0a = 0$ .*
- (2)  *$(-a)b = a(-b) = -(ab)$ , for all  $a, b \in R$ .*
- (3)  *$(-a)(-b) = ab$ , for all  $a, b \in R$ .*
- (4)  *$(n \cdot a)(n \cdot b) = (nm) \cdot (ab)$ , for all  $n, m \in \mathbb{Z}$  and  $a, b \in R$ .*

*Proof.* All of this is straightforward. For example,  $a0 = a(0 + 0) = a0 + a0$  by distributive law, so  $a0 = 0$ . The other claims are similarly proven.  $\square$

**Definition 13.10.** A ring  $R$  is called *commutative* if the multiplication of  $R$  is commutative, that is,  $ab = ba$  for all  $a, b \in R$ . We say that  $R$  has a *unit* if there is an element  $1 \in R$  such that  $1a = a1 = a$  for all  $a \in R$ .

*Example 13.11.* Examples 13.1, 13.4, 13.5 are all commutative and with unit, while example 13.2 has a unit but is not commutative and example 13.3 is commutative but does not have a unit.

**Definition 13.12.** A non-empty subset  $S \subset R$  of a ring is called a *subring* of  $R$  if it is a ring with the operations inherited from  $R$ . In particular,  $S$  has to be a subgroup for the addition operation.

*Example 13.13.*  $\mathbb{Z}$  is a subring of  $\mathbb{Q}$ , which is a subring of  $\mathbb{R}$ ; and  $2\mathbb{Z}$  is a subring of  $\mathbb{Z}$ . On the other hand, the set of odd integers is not a subring of  $\mathbb{Z}$ , and the subring of  $\mathbb{R}$  generated by 1 and  $\pi$  is not a subring of  $\mathbb{R}$ , either.

**Lemma 13.14.** *A subset  $S \subset R$  of a ring  $R$  is a subring if and only if  $a, b \in S$  implies  $a - b \in S$  and  $ab \in S$ .*

*Proof.* By one of our subgroup criteria, the first condition shows that  $S$  is a subgroup. The second condition then ensures that  $S$  is a subring (the associativity of multiplication and the distributive law automatically hold because they hold in  $R$ ).

Conversely, if  $S$  is a subring, then it is a subgroup, so the first condition is satisfied. It also has to be closed under multiplication, that is, the second condition holds.  $\square$

*Example 13.15.* (1) The ring of Gaussian integers  $\mathbb{Z}[i]$  is a subring of  $\mathbb{C}$ .  
 (2) The subset  $\mathbb{Q}(\sqrt{p}) = \{x \in \mathbb{C} \mid x = x_1 + x_2\sqrt{p} \text{ for some } x_1, x_2 \in \mathbb{Q}\}$  is a subring for any integer (in fact, for any rational number)  $p$ .

**Definition 13.16.** Let  $R$  be a commutative ring with 1. A *polynomial*  $p(X)$  over  $R$  is a finite (formal) sum

$$p(X) = a_0 + a_1X + \dots + a_nX^n$$

where  $a_0, a_1, \dots, a_n \in R$  and  $X$  is an indeterminate. We usually write only those terms  $a_iX^i$  where  $a_i \neq 0$  and declare  $a_0 + a_1X + \dots + a_nX^n$  to be equal to  $a_0 + a_1X + \dots + a_nX^n + 0X^{n+1}$ . If  $n$  is maximal such that  $a_n \neq 0$ , we say that  $p(X)$  has degree  $n$ .

The set of polynomials over  $R$  is denoted  $R[X]$  and called the *polynomial ring over  $R$* .

**Definition 13.17.** We define the sum of two polynomials  $p(X) = a_0 + \dots + a_nX$  and  $q(X) = b_0 + \dots + b_nX$  to be the polynomial

$$(p + q)(X) = (a_0 + b_0)X + \dots + (a_n + b_n)X.$$

Note that any two polynomials can be added in this way - if one has more terms than the other in its sum, just add terms of the form  $0X^i$  until they have the same number of terms.

We define the product of  $p(X) = a_0 + a_1X + \dots + a_nX^n$  and  $q(X) = b_0 + b_1X + \dots + b_mX^m$  as the polynomial

$$(pq)(X) = d_0 + d_1X + \dots + d_{m+n}X^{m+n}$$

where  $d_k = \sum_{i=0}^k a_i b_{k-i}$ .

**Lemma 13.18.** *The polynomial ring  $R[X]$  with the addition and multiplication operations of Definition 13.17 is a commutative ring with 1.*

*Proof.* Clearly, addition and multiplication are commutative. The 0 element is the polynomial 0, the negative of  $a_0 + \dots + a_nX^n$  is  $(-a_0) + \dots + (-a_n)X^n$ , and the one element is 1. So  $R[X]$  is an abelian group under addition with a commutative multiplication and 1. It remains to check the distributive law - we leave that an exercise.  $\square$

**Definition 13.19.** Let  $R$  be a commutative ring. An element  $a \in R$  is called a *zero divisor* if  $a \neq 0$  and there exists  $b \neq 0$  in  $R$  such that  $ab = 0$ .

*Example 13.20.* In the ring  $\mathbb{Z}/n$  of congruence classes mod  $n$ , a congruence class  $[i] \neq [0]$  is a zero divisor if and only if  $\gcd(i, n) > 1$ . Indeed, if  $[i]$  is a zero divisor, then there is  $[j] \neq [0]$  such that  $ij \equiv 0 \pmod{n}$ , that is,  $n$  divides  $ij$ . Because  $[j] \neq [0]$ , we know that  $n$  does not divide  $j$ . Therefore  $\gcd(i, n) > 1$ . If, conversely,  $\gcd(i, n) = k > 1$ , let  $j = n/k$ ; but then  $ij = i(n/k) = (i/k)n$  where  $i/k \in \mathbb{Z}$ , so  $ij \equiv 0 \pmod{n}$  or  $[i][j] = [0]$ .

*Example 13.21.* Thus, the ring  $\mathbb{Z}/n$  contains *no* zero divisors if and only if  $n$  is a prime.

*Example 13.22.* The rings  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $2\mathbb{Z}$  all contain no zero divisors.

**Definition 13.23.** A commutative ring with one  $R$  is called an *integral domain* (or sometimes just *domain*) if and only if  $R$  contains no zero divisors.

*Example 13.24.* So the rings  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{Z}/p$  for a prime  $p$  are all integral domains, while  $\mathbb{Z}/n$  for  $n$  not a prime is not a domain, and  $2\mathbb{Z}$  is not a domain, either.

**Lemma 13.25.** *A commutative ring with one  $R$  is an integral domain if and only if the cancellation law hold in  $R$ , that is, if and only if for all  $a \neq 0$*

$$ab = ac \implies b = c$$

for  $b, c \in R$ .

*Proof.* Clearly, if the cancellation law holds, then  $R$  is a domain. Conversely, assume  $R$  is an integral domain,  $a \neq 0$  in  $R$  and  $ab = ac$  for some  $b, c \in R$ . Then  $a(b-c) = 0$  and since  $R$  is a domain this implies that  $b-c = 0 \implies b = c$ .  $\square$

**Proposition 13.26.** *Suppose that  $R$  is an integral domain. Then so is  $R[X]$ .*

*Proof.* Let  $p(X) = a_0 + \dots + a_nX^n \neq 0$  and  $q(X) = b_0 + \dots + b_mX^m$  be polynomials over  $R$  and assume that  $(pq)(X) = 0$ . We prove that  $q(X) = 0$  (in other words,

that  $b_0 = \cdots = b_m = 0$ ). Write the product  $(pq)(X) = d_0 + \cdots + d_{m+n}X^{m+n}$ . By assumption,  $d_s = 0$  for all  $s$ .

Suppose  $k \geq 0$  is the minimal index such that  $a_k \neq 0$ . Then  $d_k = \sum_{i=0}^k a_i b_{k-i} = a_k b_0 = 0$  by assumption. Since  $R$  is an integral domain and  $a_k \neq 0$ , we conclude that  $b_0 = 0$ . Now assume  $r > 0$  and we already proved  $b_0 = \cdots = b_{r-1} = 0$ . Then  $d_{r+k} = a_k b_r = 0$ , so we conclude that  $b_r = 0$ . By induction, we see that  $b_0 = \cdots = b_m = 0$ , as asserted.  $\square$

**Definition 13.27.** Let  $R$  be a ring with one. An element  $a \in R$  is called a *unit* in  $R$  if there exists  $b \in R$  such that  $ab = ba = 1$ . In that case, we write  $b = a^{-1}$ .

The set of units of  $R$  is denoted  $R^*$  or sometimes  $U(R)$ .

**Lemma 13.28.** Let  $R$  be a ring with 1. Then the set  $R^*$  of units is a group under multiplication.

*Proof.* If  $a$  and  $b$  are units with inverses  $a^{-1}$  and  $b^{-1}$ , then  $ab$  has inverse  $b^{-1}a^{-1}$ , so multiplication defines an operation on  $R^*$ . Apparently,  $1 \in R$  is a neutral element for this operation, and since  $a \in R^* \rightarrow a^{-1} \in R^*$ , there are inverses. Finally, multiplication in a ring is associative.  $\square$

*Example 13.29.* The group of units in  $\mathbb{Z}/n$  is  $\mathbb{Z}/n^*$ , which we have seen before.  $\mathbb{Z}^* = \{-1, 1\}$ , and  $\mathbb{R}^* = \mathbb{R} - \{0\}$ . Also,  $M_n(\mathbb{R})^* = Gl(n, \mathbb{R})$ .

**Definition 13.30.** A commutative ring with  $1 \neq 0$  is called a *field* provided  $R^* = R - \{0\}$ .

*Example 13.31.*  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p$  for a prime  $p$  are all fields, while  $\mathbb{Z}, \mathbb{Z}/n$  for  $n$  not a prime,  $\mathbb{Z}[i]$  are not fields. Also, the 0-ring consisting only of the one element 0 is not a field - a field has at least 2 elements.

**Lemma 13.32.** Every field  $k$  is an integral domain.

*Proof.* Let  $a \neq 0$  be an element of  $k$ . Suppose  $ab = ac$  for some  $b, c \in k$ . Then  $b = a^{-1}ab = a^{-1}ac = c$ . That is, the cancellation law holds and  $k$  is a domain.  $\square$

**Theorem 13.33.** Let  $R$  be a finite integral domain. Then  $R$  is a field.

*Proof.* Let  $R - \{0\} = \{1 = a_0, a_1, \dots, a_n\}$  and  $a \in R - \{0\}$ . Then  $aa_i = aa_j$  if and only if  $a_i = a_j$  by the cancellation law, so  $\{aa_0, aa_1, aa_2, \dots, aa_n\}$  is a subset of  $R - \{0\}$  with  $n + 1$  elements. Hence, it is equal to  $R - \{0\}$ . But that means that  $aa_i = 1$  for some  $i$ , so  $a$  is a unit. Since  $a \neq 0$  was arbitrary, we conclude that  $R$  is a field.  $\square$

Note this proves our assertion of Example 13.31 that  $\mathbb{Z}/n$  is a field if and only if  $n$  is a prime. This last observation has a generalization.

**Definition 13.34.** Let  $R$  be a ring. The smallest positive integer  $n$  such that  $n \cdot a = 0$  for all  $a \in R$  is called the *characteristic* of  $R$ . If no such integer exists, we say that the characteristic of  $R$  is 0. A ring of characteristic  $n > 0$  is said to have *positive* or *finite* characteristic.

*Example 13.35.*  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  all have characteristic 0, while  $\mathbb{Z}/n, \mathbb{Z}/n[X]$  has characteristic  $n$ .

**Lemma 13.36.** If  $R$  is a commutative ring with one having characteristic  $n$ , then  $R[X]$  also has characteristic  $n$ .

*Proof.* Exercise. □

**Theorem 13.37.** *Let  $A$  be an integral domain. Then the characteristic of  $A$  is either 0 or a prime.*

*Proof.* Suppose the characteristic of  $A$  is  $n > 0$ . I claim  $m \cdot 1 \neq 0$  for  $0 < m < n$ . For suppose it was for some such  $m$ , then  $m \cdot a = m \cdot (1a) = (m \cdot 1)a$  for all  $a \in A$ , contradicting the minimality of  $n$ . Now if  $n = rs$  with  $1 \leq r < n$ , then  $(r \cdot 1)(s \cdot 1) = (rs) \cdot 1 = n \cdot 1 = 0$  by assumption; since  $A$  is a domain, we conclude that  $s \cdot a = 0$  and thus  $s = n$ . That is,  $n$  is a prime. □

**Theorem 13.38.** *Suppose  $A$  is a domain of positive characteristic. Then  $A$  contains a field as subring.*

*Proof.* By Theorem 13.37, the characteristic is a prime number  $p$ . I claim the set  $k = \{0, 1, 2 \cdot 1, \dots, (p-1) \cdot 1\}$  is a subring of  $A$ . Indeed, the sum, product or difference of two integer multiples of 1 is an integer multiple of 1 and the above is a complete list of all integer multiples of 1 in light of the fact that  $n \cdot 1 = (n+p) \cdot 1$  for all  $n \in \mathbb{Z}$ . By the subring criterion,  $k$  is a subring of  $A$ .

Now  $k$  is a subring of the integral domain  $A$  and therefore is a domain. Since it is also finite, it is a field, by Theorem 13.33. □

Note the conclusion of the theorem is false if the characteristic is 0, as evidenced by the example  $\mathbb{Z}$ .

#### 14. RING HOMOMORPHISMS AND IDEALS

**Definition 14.1.** Let  $R_1$  and  $R_2$  be rings. A homomorphism  $f : R_1 \rightarrow R_2$  is a map such that

- (1) For all  $a, b \in R_1$ ,  $f(a + b) = f(a) + f(b)$ .
- (2) For all  $a, b \in R_1$ ,  $f(ab) = f(a)f(b)$ .

If, in addition,  $R_1$  and  $R_2$  are rings with 1, we usually require that  $f(1) = 1$ .

The set of homomorphisms from  $R_1$  to  $R_2$  is written  $\text{Hom}(R_1, R_2)$ , or  $\text{Hom}_{\text{rings}}(R_1, R_2)$  if we want to emphasise that we are talking about *ring* homomorphisms as opposed to homomorphisms of abelian groups.

*Example 14.2.* (1) For any ring with one  $R$  there is a unique homomorphism  $f : \mathbb{Z} \rightarrow R$  such that  $f(1) = 1$ .

- (2) For any ring  $R$  with one, there is a bijection  $\text{Hom}(\mathbb{Z}[X], R) \cong R$ , defined by sending a homomorphism  $f : \mathbb{Z}[X] \rightarrow R$  (such that  $f(1) = 1$ ) to  $f(X)$ .

**Definition 14.3.** Let  $f : R \rightarrow R'$  be a homomorphism of rings. The *kernel* of  $f$  is the subset

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

**Lemma 14.4.** *Let  $f : R \rightarrow R'$  be a homomorphism of rings. Then  $\ker(f) \subset R$  is a subring.*

*Proof.* Note that any homomorphism of rings is in particular a homomorphism of abelian groups  $(R, +) \rightarrow (R', +)$ . Hence  $\ker(f)$  is a subgroup. Moreover, if  $a, b \in \ker(f)$ , then  $f(ab) = f(a)f(b) = 0$ , so  $ab \in \ker(f)$ . □

**Lemma 14.5.** *Let  $f : R \rightarrow R'$  be a homomorphism of rings. Then the image  $f(R) \subset R'$  is a subring.*

*Proof.* Exercise. □

**Definition 14.6.** A ring homomorphism is called an *isomorphism* of rings if it is a bijective map.

**Lemma 14.7.** *Let  $f : R \rightarrow R'$  be an isomorphism of rings. Then the inverse map  $f^{-1} : R' \rightarrow R$  is also an isomorphism of rings.*

*Proof.* Exercise. □

*Remark 14.8.* In particular, if there is a ring isomorphism  $R \rightarrow R'$ , then  $R$  is commutative (with one) if and only if  $R'$  is commutative (with one).

**Lemma 14.9.** *Let  $f : R \rightarrow R'$  be a homomorphism of commutative rings with one. Then  $f$  induces a homomorphism*

$$f_* : R[X] \longrightarrow R'[X]$$

such that  $f_*(X) = X$  and  $f_*(a) = f(a)$  for  $a \in R$ .

*Proof.* If  $p(X) = a_0 + a_1X + \dots + a_nX^n$ , then define  $f_*(p)(X) = f(a_0) + f(a_1)X + \dots + f(a_n)X^n$ . □

The following is a very important application of ring homomorphisms. Suppose  $R$  is a commutative ring with one. Generalizing Example 14.2, (2), we observe there is a bijection between ring homomorphisms  $f : R[X] \rightarrow R$  with  $f(a) = a$  for constant polynomials  $a$  and elements of  $R$ , defined by  $f \mapsto f(X)$ . Call the homomorphism corresponding to  $x \in R$ ,  $f_x$ . Now suppose  $p(X) \in R[X]$ . Then we write  $p(x)$  for the element  $f_x(p(X))$  of  $R$ , and call this the *evaluation* of the polynomial  $p(X)$  at  $x \in R$  (to say it in an easier way, one obtains  $p(x)$  by just "plugging in"  $x$  for the "variable"  $X$ ).

We say that  $x$  is a zero of the polynomial  $p(X)$  if  $p(x) = 0 \in R$ .

**Proposition 14.10.** *Let  $f : R \rightarrow R'$  be a homomorphism of commutative rings with one. If  $x \in R$  is a zero of  $p(X) \in R[X]$ , then  $f(x) \in R'$  is a zero of  $f_*(p)(X)$ . Also note that  $f(y)$  is another zero of  $f_*(p)(X)$  provided  $x - y \in \ker(f)$ .*

*Proof.*  $f(p(x)) = f_*(p)(f(x))$ . □

Now let  $R = \mathbb{Z}$  and  $R' = \mathbb{Z}/l$  for a prime  $l$ , and  $f : \mathbb{Z} \rightarrow \mathbb{Z}/p$  the natural projection (that is,  $f(n) = [n]$ ). Let  $p(X) = a_0 + a_1X + \dots + a_nX^n$  be a polynomial with integer coefficients. Then  $f_*(p)(X) = [a_0] + [a_1]X + \dots + [a_n]X^n$ . In particular, if  $n \in \mathbb{Z}$  is a zero of  $p(X)$ , then the preceding proposition implies that  $p(n) \equiv 0 \pmod{l}$ . This is usually used in the contrapositive, as demonstrated by the following example.

*Example 14.11.* The polynomial  $X^2 + 1$  has *no* integer zero. Indeed, if it had a zero  $x$ , then  $x^2 + 1 \equiv 0 \pmod{3}$ , which is impossible (we only need to check this for  $x = 0, 1, 2$ ).

**Definition 14.12.** Let  $R$  be a ring. A (two-sided) *ideal*  $I$  of  $R$  is a subring  $I \subset R$  such that for all  $x \in I$  and  $y \in R$  we have  $xy \in I$  and  $yx \in I$ .

*Example 14.13.* The trivial subring  $\{0\} \subset R$  is always an ideal, as is the improper subring  $R \subset R$ .

**Lemma 14.14.** *Let  $f : R \rightarrow R'$  be a homomorphism of rings. Then the kernel  $\ker(f)$  of  $f$  is an ideal of  $R$ .*

*Proof.* Exercise. □

**Proposition 14.15.** *Let  $A$  be a commutative ring and  $x \in A$ . Then the subset  $(x) = xA = \{z \in A \mid \exists y \in A : z = xy\}$  is an ideal of  $A$ , called the principal ideal generated by  $x$ .*

*Proof.* Obvious. □

**Lemma 14.16.** *If  $I$  is an ideal of a commutative ring  $A$  and  $x \in A$ , then  $(x) \subset I$ .*

*Proof.* Direct from the definitions. □

*Example 14.17.* The ideals of  $\mathbb{Z}$  are all principal, namely any ideal is of the form  $n\mathbb{Z}$  for some integer  $n \geq 0$ .

For any commutative ring with one  $A$ , the ideal  $(1) = A$ .

**Theorem 14.18.** *Let  $A$  be a commutative ring with  $1 \neq 0$ . Then  $A$  is a field if and only if the only ideals of  $A$  are the trivial ideal  $(0)$  and the improper ideal  $(1)$ .*

*Proof.* Suppose first that  $A$  is field and  $I \subset A$  is an ideal. If  $I \neq (0)$ , choose an element  $x \neq 0$  in  $I$ . Then  $x^{-1}x = 1 \in I$ , so  $(1) = A \subset I$  and hence  $I = A$ .

Conversely, assume there is no nontrivial proper ideal of  $A$ . Let  $x \in A$  be a non-zero element. Then  $(x) \neq (0)$ , hence by assumption,  $(x) = (1)$ . That is, there is an element  $y \in A$  such that  $xy = yx = 1$ , so  $x \in A^*$ . Thus,  $A$  is a field. □

**Proposition 14.19.** *Let  $R$  be a ring and  $I \subset R$  an ideal. Then there is a unique ring structure on the quotient group  $A/I$  such that the natural map  $A \rightarrow A/I$  is a ring homomorphism.*

*Proof.* The elements of  $A/I$  are cosets of the form  $a + I$ ,  $b + I$  and such. We define a multiplication on  $A/I$ . Namely, define

$$(a + I)(b + I) = (ab + I).$$

We need to show this is well-defined. So assume  $a + I = a' + I$  and  $b + I = b' + I$ , that is,  $a = a' + x$  and  $b = b' + y$  for some  $x, y \in I$ . Then

$$(ab - a'b') = (a' + x)(b' + y) - a'b' = a'y + xb' + xy \in I$$

since  $I$  is an ideal. That is,  $ab + I = a'b' + I$ , so the multiplication is well-defined. It is clearly associative, because the multiplication of  $R$  is.

Recall that  $(a+I)+(b+I) = (a+b)+I$  by definition of the quotient group. Therefore the distributive laws for  $R/I$  also follow immediately from the corresponding laws for  $R$ .

In conclusion, the addition and multiplication on  $R/I$  as defined above define a ring structure on  $R/I$ . It is evident that the natural map  $\pi : R \rightarrow R/I$  sending  $a$  to  $a + I$  is a homomorphism. Finally, this natural homomorphism is onto, so that the ring structure on  $R/I$  is unique with the property that  $\pi$  is a homomorphism. □

**Theorem 14.20.** *Let  $\phi : R \rightarrow R'$  be a homomorphism of rings with kernel  $I \subset R$ . Then there is a natural factorization of  $\phi$  as*

$$R \rightarrow R/I \rightarrow \phi(R) \rightarrow R'$$

where the first map is natural projection, the second map is an isomorphism, and the third is the embedding.

In particular, the rings  $R/I$  and  $\phi(R)$  are isomorphic (as rings).

*Proof.* In light of the first isomorphism theorem for groups (cf. Theorem 6.28), the factorization exists and we only need to show that the map  $\tilde{\phi} : R/I \rightarrow R'$  defined by  $\tilde{\phi}(a + I) = \phi(a)$  is a ring homomorphism. In fact,  $\tilde{\phi}((a + I)(b + I)) = \phi(ab) = \phi(a)\phi(b) = \tilde{\phi}(a + I)\tilde{\phi}(b + I)$ .  $\square$

#### 15. POLYNOMIAL RINGS OVER FIELDS.

Content: Euclidean algorithm for polynomials. Irreducible polynomials. All ideals are principal. Prime ideals and maximal ideals in polynomial rings.

#### 16. FIELD EXTENSIONS.

Content: Finite extensions. Subextensions generated by a set of elements. Finitely generated extensions. Extensions associated to irreducible polynomials. Degree of a finite extension.

#### 17. ALGEBRAIC EXTENSIONS.

Content: Algebraic elements. Minimal polynomials. Splitting fields. Finite extensions are algebraic. The subfield of algebraic elements in an extension. Transitivity of algebraic extensions. Multiple roots. Perfect fields.

#### 18. ALGEBRAIC CLOSURE AND NORMAL EXTENSIONS.

**Definition 18.1.** A field  $F$  is called algebraically closed if any algebraic extension  $F \subseteq E$  is equal to  $F$ . Equivalently, if all polynomials over  $F$  split into linear factors over  $F$ .

**Lemma 18.2.** Suppose  $F$  is a field such that any non-constant polynomial over  $F$  has a root in  $F$ . Then  $F$  is algebraically closed.

*Proof.* Let  $p(X)$  be an irreducible polynomial over  $F$  and  $\alpha$  a root of  $p$ . Then  $p(X) = (X - \alpha)f(X)$ . Since  $p$  is irreducible,  $f$  is constant. That is, all irreducible polynomials over  $F$  have degree 1. Since any polynomial over a field factors into irreducibles, all polynomials over  $F$  split into linear factors, that is,  $F$  is algebraically closed.  $\square$

**Theorem 18.3.** *Let  $F$  be a field. Then there exists an extension  $E/F$  such that  $E$  is algebraically closed.*

*Proof.* Let  $S$  be the set of all polynomials over  $F$  of degree at least 1. To each  $f \in S$ , associate a variable  $X_f$  and let  $F[S]$  be the polynomial ring in these variables. (Warning: this is as many variables as  $F$  has elements, that is, possibly quite a lot.) Let  $I$  be the ideal of  $F[S]$  generated by the polynomials  $f(X_f)$ . It is easy to see that  $I \neq F[S]$ . By Zorn's lemma, there is a maximal ideal  $\mathfrak{m}$  of  $F[S]$  containing  $I$ . Let  $F_1 = F[S]/\mathfrak{m}$ . Then  $F_1$  is a field extension of  $F$  such that all polynomials over  $F$  have a root in  $F_1$ . Inductively, construct extensions  $F_{n+1}$  of  $F_n$  with the property that any polynomial over  $F_n$  has a root in  $F_{n+1}$ .

Let  $E = \bigcup_{n \geq 1} F_n$ . Clearly,  $E$  is a field containing  $F$ . If  $f(X) \in E[X]$  is a polynomial, then the (finitely many) coefficients of  $f$  lie in some field  $F_n$ , hence  $f$  has a root in  $F_{n+1}$ , and hence has a root in  $E$ . By the lemma,  $E$  is algebraically closed.  $\square$

**Corollary 18.4.** *Let  $F$  be a field. Then there exists an algebraic extension  $F \subseteq \overline{F}$  such that  $\overline{F}$  is algebraically closed. The field  $\overline{F}$  is called an algebraic closure of  $F$ .*

*Proof.* Let  $E$  be an algebraically closed field containing  $F$ . Set  $\overline{F}$  to be the subfield of  $E$  consisting of elements algebraic over  $F$ . Tautologically, it is an algebraic extension. If  $p(X)$  is a polynomial over  $\overline{F}$ , then  $p$  has a root in  $E$ , which is algebraic over  $\overline{F}$  and hence algebraic over  $F$ ; that is, the root is contained in  $\overline{F}$ . Therefore  $\overline{F}$  is algebraically closed.  $\square$

**Lemma 18.5.** *Let  $F \subseteq E$  be an algebraic extension. If  $\sigma : E \rightarrow E$  is a homomorphism fixing  $F$ , then  $\sigma$  is an automorphism of  $E$ .*

*Proof.*  $\sigma(1) = 1$ , so since  $E$  is a field,  $\sigma$  is injective.

Suppose  $E$  is finite over  $F$ . Since  $\sigma|_F = id$ ,  $\sigma : E \rightarrow E$  is  $F$ -linear. Because  $E$  is a finite dimensional  $F$ -vector space and  $\sigma$  is injective, it is an automorphism.

In the general case, suppose  $\alpha \in E$ . Let  $p(X)$  be the minimal polynomial of  $\alpha$  and let  $F' \subseteq E$  be the subfield generated by  $\alpha$  and all the other roots of  $p$  contained in  $E$ . Then  $\sigma(F') \subseteq F'$  and  $F'$  is finite over  $F$ ; by the first part of the proof,  $\sigma(F') = F'$ . Consequently,  $\alpha$  is in the image of  $\sigma$ . since  $\alpha$  was arbitrary,  $\sigma$  is surjective.  $\square$

**Lemma 18.6.** *Let  $F \subseteq E$  be an algebraic extension and  $\overline{F}$  an algebraic closure of  $F$ . Suppose  $\alpha \in E$  and  $\sigma : F(\alpha) \rightarrow \overline{F}$  is a homomorphism fixing  $F$ . Then there exists a homomorphism  $\tau : E \rightarrow \overline{F}$  such that  $\tau|_{F(\alpha)} = \sigma$ .*

*Proof.* We may assume  $E$  is finite over  $F$ , and in fact (by induction) that  $E = F(\alpha, \beta)$  for some  $\beta$ . Let  $p(X) \in F(\alpha)[X]$  be the minimal polynomial of  $\beta$  over  $F(\alpha)$ , and choose a root  $\gamma \in \overline{F}$  of  $\sigma p(X) \in \overline{F}[X]$ . Then there is a homomorphism  $\tau$  as required, defined by  $\tau(f(\beta)) = \sigma f(\gamma)$  for any  $f(X) \in F(\alpha)[X]$ .  $\square$

**Theorem 18.7.** *Let  $F$  be a field, and  $E \subseteq \overline{F}$  an algebraic extension contained in some algebraic closure of  $F$ . Then the following are equivalent.*

- (1) *If  $\sigma : E \rightarrow \overline{F}$  is a homomorphism fixing  $F$ , then  $\sigma(E) = E$ .*
- (2) *Let  $p(X) \in F[X]$  be irreducible. If  $p$  has a root in  $E$ , then  $p$  splits into linear factors over  $E$ .*
- (3)  *$E$  is a splitting field for some family of polynomials over  $F$ . If  $E$  is finite, then there exists one polynomial  $f(X) \in F[X]$  such that  $E$  is a splitting field for  $f$ .*

*Proof.* Assume (1) holds, and that  $p(X)$  is irreducible with a root  $\alpha$  in  $E$ . Let  $\beta \in \overline{F}$  be another root. Then there exists a homomorphism  $\sigma : F(\alpha) \rightarrow \overline{F}$  such that  $\sigma(\alpha) = \beta$ . By Lemma 18.6, there is a homomorphism  $\tau : E \rightarrow \overline{F}$  such that  $\tau(\alpha) = \beta$ . By (1),  $\tau(E) = E$ , so that  $\beta = \tau(\alpha) \in E$ , as (2) asserts.

Now assume (2). Let  $\mathcal{F}$  be the family of all minimal polynomials of elements of  $E$  over  $F$ . Clearly,  $E$  is contained in the splitting field of  $\mathcal{F}$  inside  $\overline{F}$ . By (2), the converse also holds. Therefore,  $E$  is a splitting field for  $\mathcal{F}$ . Suppose  $[E : F] < \infty$ . Then there are finitely many elements  $\alpha_i$  generating  $E$ , and  $E$  is the splitting field of the product of their minimal polynomials.

Finally, suppose (3) holds, so that  $E$  is a splitting field for some family  $\mathcal{F}$  of polynomials over  $F$ . By Lemma 18.5, to prove (1) it suffices to show that  $\sigma(E) \subseteq E$ . Let  $S = \{\alpha_{f,i} | f \in \mathcal{F}\}$  be the set of roots of the polynomials in  $\mathcal{F}$ . By assumption, this set generates the extension  $E$ . If  $\alpha_{f,i}$  is one of these roots, then  $\sigma(\alpha_{f,i})$  is also a root of  $f$ , hence  $\sigma(\alpha_{f,i}) \in S$ . Therefore,  $\sigma(S) \subseteq S$ , whence  $\sigma(E) \subseteq E$ , as asserted.  $\square$

**Definition 18.8.** An algebraic extension  $E/F$  satisfying the equivalent conditions of Theorem 18.7 is called *normal*. If  $E/F$  is any extension, then there is a smallest normal extension  $E'$  containing  $E$ , namely the splitting field of the collection of minimal polynomials of the elements in  $E$ . We call  $E'$  a *normal hull* of  $E$  over  $F$ .

## 19. SEPARABLE EXTENSIONS

**Definition 19.1.** Let  $F \subseteq E$  be an algebraic field extension, and let  $\alpha \in E$ . We say that  $\alpha$  is *separable* over  $F$  if its minimal polynomial has no multiple roots in any extension. We say that the extension  $E/F$  is separable if all elements of  $E$  are separable over  $F$ .

**Definition 19.2.** Let  $F \subseteq E$  be an algebraic extension. We say that an element  $\alpha \in E$  is *purely inseparable* over  $F$  if  $\alpha$  is the only root of its minimal polynomial in a splitting field. For example, all elements of  $F$  are purely inseparable (and also, separable) over  $F$ . We say that the extension  $E/F$  is purely inseparable if all elements of  $E$  are purely inseparable over  $F$ .

**Lemma 19.3.** *Let  $F \subseteq E \subseteq \overline{F}$  be an extension contained in an algebraic closure. Let  $S$  be the set of embeddings of  $E$  into  $\overline{F}$  fixing  $F$ . Set  $E_{ins} = \{\alpha \in E | \forall \sigma \in S : \sigma(\alpha) = \alpha\}$ . Then  $E_{ins}$  is a subfield containing  $F$ , and  $\alpha \in E_{ins}$  if and only if  $\alpha$  is purely inseparable over  $F$ .*

*Proof.* Let  $\sigma \in S$ . Clearly, the set of elements in  $E$  fixed by  $\sigma$  forms a subfield containing  $F$ . Now the first assertion follows as the intersection of subfields is a subfield. Suppose  $\alpha \in E$  and let  $p(X) \in F[X]$  be its minimal polynomial. If  $p(X)$  has a different root  $\beta \in \overline{F}$  then there is an embedding  $\tau : E \rightarrow \overline{F}$  such that

$\tau(\alpha) = \beta$ . This shows that  $E_{ins}$  consists of purely inseparable elements. Conversely, if  $\alpha$  is purely inseparable with minimal polynomial  $p(X)$ , and  $\sigma \in S$ , then  $\sigma(\alpha)$  is a root of  $p$ , hence equal to  $\alpha$ ; that is,  $\alpha \in E_{ins}$ .  $\square$

**Corollary 19.4.** *Any purely inseparable extension is normal.*

*Proof.* Suppose  $E/F$  is purely inseparable. Choose an embedding  $E \rightarrow \overline{F}$  into an algebraic closure. By the lemma, this embedding is unique. Therefore, the extension is normal by Theorem 18.7, (1).  $\square$

**Corollary 19.5.** *Let  $F \subseteq E \subseteq \overline{F}$  be an extension contained in an algebraic closure. Suppose that  $E$  is normal over  $F$ . Then  $E$  is separable over  $E_{ins}$ ; in particular,  $E/F$  is separable if and only if  $E_{ins} = F$ .*

*Proof.* The statement is vacuous if the characteristic of  $F$  is 0. Suppose the characteristic is  $p > 0$ . Let  $\alpha \in E$  and  $f(X)$  its minimal polynomial over  $F$ . Since  $E/F$  is normal, it splits  $f$ , so in  $E[X]$ , we can write  $f(X) = \prod_{i=1}^r (X - \alpha_i)^{p^j} = g(X)^{p^j}$  for some  $j \geq 0$ , where  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$  are the distinct conjugates of  $\alpha$  and  $g(X) = \prod_{i=1}^r (X - \alpha_i)$ . An embedding  $\sigma : E \rightarrow \overline{F}$  over  $F$  simply permutes the conjugates  $\alpha_i$ , whence we conclude that  $\sigma g = g$ . That is, the coefficients of  $g$  are in  $E_{ins}$ . Since  $g(\alpha) = 0$  and  $g$  has no multiple roots, we conclude that  $\alpha$  is separable over  $E_{ins}$ , as asserted.  $\square$

**Lemma 19.6.** *Let  $F$  be a field,  $E/F$  a purely inseparable extension, and  $f(X)$  an irreducible polynomial over  $F$  with no multiple roots in  $\overline{F}$ . Then  $f(X)$  is irreducible over  $E$ .*

*Proof.* Let  $\alpha$  be a root of  $f(X)$  in  $\overline{F}$ , and  $S_\alpha$  the set of embeddings of  $F(\alpha)$  into  $\overline{F}$  over  $F$ . Since  $\alpha$  is separable, we have  $|S_\alpha| = \deg(f)$ . Let  $\tau : E \rightarrow \overline{F}$  be the (unique since  $E$  is purely inseparable) embedding over  $F$  and write  $T_\alpha$  for the set of embeddings of  $E(\alpha)$  into  $\overline{F}$  over  $(E, \tau)$  (that is, embeddings whose restriction to  $E$  is equal to  $\tau$ ). If  $\sigma \in S_\alpha$ , then there is an extension  $\tilde{\sigma} : E(\alpha) \rightarrow \overline{F}$  to an embedding over  $F$ . The restriction  $\tilde{\sigma}|_E$  is an embedding over  $F$ , hence necessarily equal to  $\tau$ . That is,  $\tilde{\sigma} \in T_\alpha$ , so that  $\sigma \mapsto \tilde{\sigma}$  is a map  $S_\alpha \rightarrow T_\alpha$ . Clearly, this map is injective; therefore,  $|T_\alpha| \geq |S_\alpha|$ . But this implies that the minimal polynomial of  $\alpha$  over  $E$  has degree at least  $\deg(f)$ ; on the other hand, it divides  $f(X)$ . We conclude that the minimal polynomial of  $\alpha$  over  $E$  is equal to  $f(X)$ , which implies that  $f(X)$  is irreducible over  $E$ .  $\square$

**Theorem 19.7.** *Let  $E/F$  be an algebraic extension. Then the subset  $E_{sep}$  of separable elements is a subfield.*

*Proof.* We may assume that  $E/F$  is finite. Moreover, we can also assume that  $E/F$  is normal; in fact, suppose  $E'/E$  is a normal extension containing  $E$ . Then  $E_{sep} = E'_{sep} \cap E$ , and since the intersection of subfields is a subfield, we may as well replace  $E$  by  $E'$ .

So suppose  $E/F$  is finite and normal. Let  $E^s$  be the subfield generated by  $E_{sep}$  over  $F$ . Note that  $E^s$  is normal over  $F$ . Clearly, it suffices to show that  $E^s$  is separable over  $F$ . We can write  $E^s = F(\alpha_1, \dots, \alpha_k)$  where the  $\alpha_i$  are separable over  $F$ . Let  $f_1$  be the minimal polynomial of  $\alpha_1$  over  $F$ , and for  $2 \leq j \leq k$ , let  $f_j$  be the minimal polynomial of  $\alpha_j$  over  $F(\alpha_1, \dots, \alpha_{j-1})$ . then  $[E^s : F] = \prod_{i=1}^k \deg(f_i)$ .

We will prove that  $(E^s)_{ins} = F$ ; by Corollary 19.5, this will imply that  $E^s$  is separable.

For any  $1 \leq j \leq k$ , the extension  $(E^s)_{ins}(\alpha_1, \dots, \alpha_j)/F(\alpha_1, \dots, \alpha_j)$  is purely inseparable. By Lemma 19.6,  $f_{j+1}$  is irreducible over  $(E^s)_{ins}(\alpha_1, \dots, \alpha_j)$ . By induction, we conclude that  $[E^s : (E^s)_{ins}] = [E^s : F]$ , which immediately implies that  $F = (E^s)_{ins}$ , as asserted.  $\square$

**Corollary 19.8.** *Suppose  $E/F$  is an algebraic extension generated by separable elements. Then  $E$  is separable over  $F$ .*

*Proof.* This is immediate from Theorem 19.7.  $\square$

**Lemma 19.9.** *Let  $K/E/F$  be algebraic extensions. Let  $\alpha \in K$ . Then  $\alpha$  is separable over  $F$  if and only if  $\alpha$  is separable over  $E_{sep}$ .*

*Proof.* The "only if" part is obvious. Suppose  $\alpha$  is separable over  $E_{sep}$ . As usual we may assume all extensions are finite and that  $K/F$  and  $E/F$  are normal (this is because an element is separable if and only if the splitting field of its minimal polynomial is separable). Let  $f(X)$  be the minimal polynomial of  $\alpha$  over  $F$ . Since  $K$  is normal,  $f(X) = g(X)^{p^j}$  over  $K$ , for some  $j \geq 0$ . Note that the coefficients of  $g(X)$  lie in the subfield  $K_{ins}$  of purely inseparable (over  $F$ ) elements (argue as in the proof of Corollary 19.5).

I claim all the roots of  $f(X)$  are separable over  $E_{sep}$ . In fact, if  $\beta$  is such a root, then there is an automorphism of  $K$  over  $F$  sending  $\alpha$  to  $\beta$  (since  $K/F$  is normal). This automorphism will map  $E_{sep}$  into itself, as  $E_{sep}/F$  is normal. We conclude that  $\beta$  is separable over  $E_{sep}$  if and only if  $\alpha$  is, as asserted.

This implies that the coefficients of  $g(X)$  lie in  $E_{sep}$ . We noted before that they also are contained in  $K_{ins}$ . In other words, the coefficients of  $g(X)$  are in the intersection  $E_{sep} \cap K_{ins}$ . That intersection consists of elements that are both separable and purely inseparable over  $F$ ; therefore, it is equal to  $F$ . That is,  $g(X) \in F[X]$ , which implies that  $j = 0$ , and therefore  $\alpha$  is separable over  $F$ , as claimed.  $\square$

**Lemma 19.10.** *Suppose  $F \subseteq E \subseteq K$  are algebraic extensions.  $E$  is separable over  $F$  and  $K$  is separable over  $E$  if and only if  $K$  is separable over  $F$ .*

*Proof.* The "if" part is clear. Suppose now that  $E/F$  and  $K/E$  are separable. Let  $\alpha \in K$ . Then  $\alpha$  is separable over  $E$ , and since  $E/F$  is separable,  $E_{sep} = E$  so that  $\alpha$  is separable over  $E_{sep}$ . By the preceding Lemma 19.9,  $\alpha$  is separable over  $F$ .  $\square$

**Lemma 19.11.** *Let  $E/F$  be an algebraic extension. Then the extension  $E/E_{sep}$  is purely inseparable.*

*Proof.* If  $\alpha \in E$  is separable over  $E_{sep}$ , then  $\alpha \in E_{sep}$ , by Lemma 19.9. Hence we may as well assume that  $E_{sep} = F$ .

Take  $\alpha \in E$  and let  $f(X)$  be its minimal polynomial over  $F$ . Write  $f(X) = g(X)^{p^j}$  for some  $j \geq 0$  and polynomial  $g$  without multiple roots. Clearly,  $g(X)$  is irreducible, and  $\alpha^p$  is a root of  $g$ , hence separable over  $F$ . This implies that  $\alpha^p \in F$ ; in other words,  $\alpha$  is purely inseparable over  $F$ .  $\square$

**Definition 19.12.** Let  $E/F$  be an algebraic extension. We define the *separable degree* of  $E$  over  $F$  to be  $[E : F]_s = [E_{sep} : F]$

**Lemma 19.13.** *Let  $F \subseteq E \subseteq K$  be finite extensions. Then  $[K : F]_s = [K : E]_s[E : F]_s$ .*

*Proof.* Let  $K_s$  be the subfield of elements of  $K$  separable over  $E_{sep}$  and  $K_{sep}$  the subfield of elements separable over  $F$ . By Lemma 19.9,  $K_s = K_{sep}$ . By multiplicativity of degrees, we have  $[K : F]_s = [K_s : E_{sep}][E : F]_s$ .

Now let  $K^s$  be the subfield of elements separable over  $E$ . I claim that  $[K_s : E_{sep}] = [K^s : E]$ . By induction, we may assume that  $K_s = E_{sep}(\alpha)$  for some  $\alpha$  with minimal polynomial  $f(X)$  over  $E_{sep}$ . Since  $E/E_{sep}$  is purely inseparable by Lemma 19.11, Lemma 19.6 implies that  $f(X)$  is irreducible over  $E$ , so that  $[E(\alpha) : E] = [K_s : E_{sep}]$ . To complete the proof of the assertion in the lemma, we need to show that  $K^s = E(\alpha)$ . Obviously,  $K^s \supseteq E(\alpha) \supseteq K_s$ . Now observe that  $K^s$  is separable over  $E(\alpha)$  because it is separable over  $E$ , and is also purely inseparable over  $E(\alpha)$  because it is purely inseparable over  $K_s$ . Therefore,  $K^s = E(\alpha)$  as needed.  $\square$

**Theorem 19.14.** *Let  $E/F$  be a finite extension and  $S_{E/F}$  the set of embeddings of  $E$  into a fixed algebraic closure  $\bar{F}$  of  $F$ . Then  $|S_{E/F}| = [E : F]_s$ . In particular, if  $E/F$  is separable, then  $|S_{E/F}| = [E : F]$ .*

*Proof.* We first claim that  $S_{E/F} \cong S_{E_{sep}/F}$ . In fact, let  $\sigma$  be an embedding of  $E_{sep}$  over  $F$ . Then there is a unique extension  $\tilde{\sigma}$  of  $\sigma$  to an embedding of  $E$ , because  $E/E_{sep}$  is purely inseparable by Lemma 19.11. Therefore the maps  $\tau \mapsto \tau|_{E_{sep}}$  and  $\sigma \mapsto \tilde{\sigma}$  are mutually inverse bijections between the sets  $S_{E/F}$  and  $S_{E_{sep}/F}$ .

So we only need to show: if  $E/F$  is finite separable, then  $|S_{E/F}| = [E : F]$ . First assume  $E = F(\alpha)$  for some  $\alpha$  with minimal polynomial  $f(X)$  over  $F$ . In this case,  $[E : F] = \deg(f)$ ; on the other hand,  $\alpha$  is separable, so  $f(X)$  has precisely  $\deg(f)$  distinct roots in  $\bar{F}$ , and there is one embedding for each root, so that  $|S_{E/F}| = \deg(f)$  also.

We proceed by induction. We can write  $E = F(\alpha_1, \dots, \alpha_r) = E'(\alpha_r)$  where  $E' = F(\alpha_1, \dots, \alpha_{r-1})$ . By inductive hypothesis,  $|S_{E'/F}| = [E' : F]$ . We have a map  $\phi : S_{E/F} \rightarrow S_{E'/F}$  defined by restriction:  $\phi(\sigma) = \sigma|_{E'}$ . Let  $\tau \in S_{E'/F}$ , and let  $S_{E/\tau} = \phi^{-1}(\tau)$ . Observe that  $E/E'$  is separable and generated by one element, and that  $\bar{F}$  is an algebraic closure of  $E$ . We can apply the inductive hypothesis again to conclude that  $|S_{E/\tau}| = [E : E']$ .

Now we simply sum up:

$$|S_{E/F}| = \sum_{\tau \in S_{E'/F}} |S_{E/\tau}| = [E' : F][E : E'] = [E : F]$$

where the last equality is by multiplicativity of degrees.  $\square$

## 20. GALOIS THEORY

**Definition 20.1.** Let  $F \subseteq E$  be an algebraic extension. We define the *Galois group* of  $E$  over  $F$  as  $\text{Gal}(E/F) = \text{Aut}_{F\text{-alg}}(E)$  as the group of automorphisms of  $E$  fixing  $F$ .

**Definition 20.2.** Let  $E/F$  be an algebraic extension. We say that  $E$  is Galois over  $F$  if  $E$  is separable and normal over  $F$ .

**Theorem 20.3.** *Let  $E/F$  be a finite Galois extension with Galois group  $G = \text{Gal}(E/F)$ . Then the following hold.*

- (1) *There is a one-to-one correspondence of subgroups  $H < G$  and subextensions  $F \subseteq F' \subseteq E$ , where  $H$  corresponds to the subfield  $F' = E^H$  of elements fixed by  $H$ .*
- (2) *The extension  $E/F' = E^H$  is Galois with Galois group  $H$ .*
- (3) *Let  $H < G$  and  $F'/F$  the corresponding subextension. Then  $F'/F$  is normal (hence, Galois), if and only if  $H$  is a normal subgroup of  $G$ . In this case the natural homomorphism  $G/H \rightarrow \text{Gal}(F'/F)$  sending  $\sigma$  to  $\sigma|_{F'}$  is an isomorphism.*
- (4) *For  $F' = E^H$  a subextension, we have  $[E : F'] = |H|$  and  $[F' : F] = [G : H]$ . In particular,  $[E : F] = |G|$ .*

We prove the main theorem in a series of lemmas.