Basic Algebra
(only a draft)

Ali Nesin
Mathematics Department
Istanbul Bilgi University
Kuştepe Şişli
Istanbul Turkey
anesin@bilgi.edu.tr

February 12, 2004

Contents

Part I

Basic Group Theory

Chapter 1

Definition and Examples of Groups

1.1 Definition and Basics

A **binary operation** or a **multiplication** on a set G is just a map from the cartesian product $G \times G$ into G. The binary operations are usually denoted by such symbols as $*$, $\times$, $\cdot$, $+$, $\circ$, $\perp$,... The image of a pair $(x, y) \in G \times G$ is then denoted by $x * y$, $x \times y$, $x \cdot y$, $x + y$, $x \circ y$, $x \perp y, \ldots$

A **group** is a set G together with a binary operation $*$ and a constant e satisfying the following properties:

G1. Associativity. For all x, y, $z \in G$, $(x * y) * z = x * (y * z)$.
G2. Identity Element. For all $x \in G$, $x * e = e * x = x$.
G3. Inverse Element. For all $x \in G$, there is a $y \in G$ such that

$$x * y = y * x = e.$$

Thus a group is a triple $(G, *, e)$ satisfying the properties G1, G2 and G3.

Remarks. **1.** On the same set G we may have several different binary operations that turn G into a group. These are considered to be different groups. In other words, a group is more than just a set.

2. G3 does not say that $x*y = y*x$ for all x, $y \in G$; it only says that, given x, the equality $x * y = y * x$ holds for at least one y, but not necessarily for all y.

3. G1 says that parentheses are useless. For example, instead of $(x*y)*(z*t)$ we can just write $x * y * z * t$.

4. We will see that the element e of a group satisfying G2 is unique. This element is called the **identity element** of the group.

Examples.

1. The following are groups: $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$. We denote these groups by $\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ or even by $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ simply if there is no room for confusion.

2. The following are groups: $(\{1, -1\}, \cdot, 1)$, $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$, $(\mathbb{R} \setminus \{0\}, \cdot, 1)$. We denote the last two groups by $\mathbb{Q}^*$ and $\mathbb{R}^*$ respectively.

3. The following are groups: $(\{q \in \mathbb{Q} : q > 0\}, \cdot, 1)$, $(\{r \in \mathbb{R} : r > 0\}, \cdot, 1)$. We denote these groups by $\mathbb{Q}^{>0}$ and $\mathbb{R}^{>0}$ respectively.

4. Let X be any set and $G = \mathrm{Sym}(X)$, the set of all bijections from X into X. Consider the composition operation $\circ$ on $\mathrm{Sym}(X)$. The triple $(\mathrm{Sym}(X), \circ, \mathrm{Id}_X)$ is a group. We denote this group by $\mathrm{Sym}(X)$ simply and call it the **symmetric group on** X. If $X = \{1, \ldots, n\}$, the group $\mathrm{Sym}(X)$ is denoted by $\mathrm{Sym}(n)$ and is called the **symmetric group on** n **letters**. The group $\mathrm{Sym}(n)$ has $n!$ many elements. At Section 1.2 we will have a closer look at this group.

5. Let I be a set and $(G, *, e)$ a group. The set of all functions ${}^IG$ from I into G is a group via the following operation: For f, $g \in {}^IG$, define $f * g \in {}^IG$ by the rule $(f * g)(i) = f(i) * g(i)$. The identity element of this group is the function that sends all the elements of I to the identity element of G.

   For $f \in {}^IG$ and $i \in I$, let us denote $f(i)$ by f_i. We can represent the function f by its values $(f_i)_{i \in I}$. With this representation,

   $$ {}^IG = \{(f_i)_{i \in I} : f_i \in G\}$$

   and

   $$(f_i)_{i \in I} * (g_i)_{i \in I} = (f_i * g_i)_{i \in I}$$

   (the componentwise multiplication). When this notation is used, the group ${}^IG$ is denoted by by $\prod_{i \in I} G$ and we call it the **direct product** of the group G over the index set I. If I has just two elements we denote the group by $G \times G$ or by G^2. Similarly, if I has n elements we denote the group by G^n or by $G \times \ldots \times G$ or by $G \oplus \ldots \oplus G$.

6. ¶ The set of all n times differentiable functions from $\mathbb{R}$ into $\mathbb{R}$ is a group under the addition of functions (see the above example), more precisely, given f and g, two n times differentiable functions from $\mathbb{R}$ into $\mathbb{R}$, we define $f + g$ as in the example above:

   $$(f + g)(x) = f(x) + g(x)$$

   for all $x \in \mathbb{R}$.

   The set of all integrable functions from $\mathbb{R}$ into $\mathbb{R}$ is a group under the addition of functions.

Given $a \in \mathbb{R}$, the set of all functions f from $\mathbb{R}$ into $\mathbb{R}$ such that f is differentiable n times and $f^{(n)}(a) = 0$ is a group under the addition of functions.

The set of all functions f from $\mathbb{R}$ into $\mathbb{R}$ such that $\lim_{x\to\infty} f(x) = 0$ is a group under the addition of functions.

7. Let I be any set and $(G, *, e)$ be a group. The set of all functions ${}^IG$ from I into G such that $\{i \in I : f(i) = e\}$ is cofinite in I is a group called **direct sum** of the family $(G_i)_i$. This group is denoted by $\oplus_I G$. Thus, with the notation introduced above,

$$\oplus_I G = \{(g_i)_{i\in I} : g_i = e \text{ except for finitely many } i \in I\}.$$

Clearly $\oplus_I G$ is a subset of $\prod_I G$ and they are equal only when I is finite.

8. Let I be any set and for each $i \in I$ let $(G_i, *_i, e_i)$ be a group. The set of all functions g from I into $\cup_{i\in I} G_i$ such that $g(i) \in G_i$ is a group under the following operation: If g and h are two such functions, define their product $g * h$ by the rule $(g * h)(i) = g(i) *_i h(i)$. This group is called the **direct product** of the family $(G_i)_i$. This group is denoted by $\prod_{i\in I} G_i$. As above we let $g_i = g(i)$ and set $g = (g_i)_i$. Clearly $(e_i)_{i\in I}$ is the identity element of this group.

   Also the subset $\{(g_i)_{i\in I} \in \prod_{i\in I} G_i : g_i = e_i \text{ for all } i \text{ except for finitely many}\}$ of $\prod_{i\in I} G_i$ is a group under the same operation. This group is called the **direct sum** of the family $(G_i)_i$ and is denoted by $\oplus_{i\in I} G_i$.

9. Let X be a set. Let $\phi : \mathbb{R}^n \longrightarrow X$ be a function. The set of bijections $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that $\phi(r_1, \ldots, r_n) = \phi(r_1, \ldots, r_n) = \phi(f(r_1), \ldots, f(r_n))$ for all $r_1, \ldots, r_n \in \mathbb{R}$ is a group under composition.

10. Let X and Y be two sets. Let $\phi : X \longrightarrow Y$ be a function. Consider the set of bijections $f : X \longrightarrow X$ such that $\phi \circ f\phi$. This set is a group under composition. In particular, the set of bijections of $\mathbb{R}^n$ that preserve the distance on $\mathbb{R}^n$ is a group, called the group of isometries of $\mathbb{R}^n$.

11. Let $(G, *, e)$ be a group. Let $X \subseteq G$ be a subset. Then the set

$$C_G(X) := \{g \in G : g * x = x * g \text{ for all } x \in X\}$$

is a group under $*$.

From now on $(G, *, e)$ stands for a group. We start by proving the most basic facts about groups.

Lemma 1.1.1 (Simplification) *For x, y, $z \in G$, if $x * z = y * z$ then $x = y$. Similarly, if $z * x = z * y$ then $x = y$.*

Proof: By G3 there is an element $t \in G$ such that $z * t = e$. Now, $x \stackrel{G2}{=} x * e = x * (z * t) \stackrel{G1}{=} (x * z) * t = (y * z) * t \stackrel{G1}{=} y * (z * t) = y * e \stackrel{G2}{=} y$. □

Lemma 1.1.2 *The element e satisfying G2 is unique. In fact if $f \in G$ is such that $x * f = x$ for some $x \in G$, then $f = e$.*

Proof: Since, $x * f = x \stackrel{G2}{=} x * e$, by Lemma 1.1.1, $f = e$. □

The unique element e is called the **identity element** of the group. Since the identity element is unique, a group may be written as $(G, *)$ instead of $(G, *, e)$.

Very often one writes xy instead of $x * y$. Also, one replaces the symbol e by 1. This is what we will do from now on. If there are several groups G, H etc., to distinguish, we will sometimes denote their identity elements by 1_G, 1_H etc.

Lemma 1.1.3 *Given $x \in G$, the element y that satisfies G3 is unique; in fact if $xz = 1$, then $y = z$.*

Proof: Since $xz = 1 = xy$, by Lemma 1.1.1, $z = y$. □

Given x the unique element y that satisfies G3 depends on x. We denote it by the symbol x^{-1}. Thus $xx^{-1} = x^{-1}x = 1$.

Note that for all x, $y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$. Be aware that we do not necessarily have $(xy)^{-1} = x^{-1}y^{-1}$. Note also that $(x^{-1})^{-1} = x$. (It is clear from G3 that if y is the inverse of x, then x is the inverse of y. Or: since $xx^{-1} = 1$ for all $x \in G$, applying this equality to x^{-1} instead of x we get $x^{-1}(x^{-1})^{-1} = 1 = x^{-1}x$, thus by Lemma 1.1.1 $x = (x^{-1})^{-1}$).

Property G1 says that when multiplying the elements of a group, the parentheses are unnecessary. From now on we will omit them.

For $x \in G$ and $n \in \mathbb{N}$ we denote the product of n many x's by x^n. Thus $x^1 = x$, $x^2 = xx$, $x^3 = xxx$ etc. We let $x^0 = 1$ and $x^{-n} = (x^n)^{-1}$. More formally, we should have defined x^n for $n \in \mathbb{N}$ by induction on n as follows: $x^0 = 1$ and $x^{n+1} = x^n x$. As usual, we call x^2 the square of x, x^3 the cube or the third power of x etc.

Lemma 1.1.4 *For any $x \in G$ and $n, m \in \mathbb{Z}$, $x^n x^m = x^m x^n = x^{m+n}$ and $(x^n)^m = x^{nm}$.*

Proof: Left as an exercise. (The formal proof using the inductive definition may not be so trivial). □

A group G is called **abelian** or **commutative** if $xy = yx$ for all x, $y \in G$.

Unless $|X| \leq 2$, the group $\mathrm{Sym}(X)$ is not abelian.

When the group is abelian, one sometimes uses the additive notation $x + y$ instead of xy. In this case the identity element is denoted as 0, the inverse of x is denoted as $-x$ and instead of x^n, one writes nx. Thus the lemma above becomes: $nx + mx = (n + m)x$ and $n(mx) = (nm)x$.

Exercise.

1. On $\mathbb{Z}$ which of the following binary operations is associative, i.e. satisfies G1?

   a) $x * y = x - y$.

   b) $x * y = x$.

   c) $x * y = xy$.

   d) $x * y = x^2$.

2. Let $G = \mathbb{R}$ and define the binary relation $*$ as $x * y = 0$. Show that $(G, *, 0)$ satisfies G1 and G3 but not G2.

3. Prove or disprove:

   a. $\{f \in \mathrm{Sym}(\mathbb{N}) : \{x \in \mathbb{N} : f(x) \neq x\}$ is finite $\}$ is a group under composition.

   b. $\{f \in \mathrm{Sym}(\mathbb{N}) : \{x \in \mathbb{N} : f(x) \neq x\}$ is an even integer $\}$ is a group under composition.

   c. $\{q \in \mathbb{Q}^{>0} : q = a/b$ and b is square-free$\}$ is a group under the usual multiplication.

4. Show that the set of functions $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ is a group under the usual product of functions: $(f \cdot g)(x) = f(x)g(x)$. What is the identity element and the inverse of an element?

5. a) Let $n \in \mathbb{N}$. Show that the set $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ is a group under addition.

   b) Show that any subset of $\mathbb{Z}$ which is a group under addition is of the form $n\mathbb{Z}$ for some unique $n \in \mathbb{N}$.

6. Show that any nonempty subset of $\mathbb{R}$ closed under substraction is a group under addition.

7. Show that the set $\{a/2^n : a \in \mathbb{Z}, n \in \mathbb{Z}\}$ is a group under addition.

8. Let $r \in \mathbb{R}^*$. Show that the set $\{r^n : n \in \mathbb{Z}\}$ is a group under multiplication.

9. Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{2}]^* = \mathbb{Q}[\sqrt{2}] \setminus \{0\}$. Show that $(\mathbb{Q}[\sqrt{2}]^*, \cdot, 1)$ is a group.

10. Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ and let

    $$\mathbb{Z}[\sqrt{2}]^* := \{\alpha \in \mathbb{Z}[\sqrt{2}] : \text{ there is a } \beta \in \mathbb{Z}[\sqrt{2}] \text{ such that } \alpha\beta = 1\}.$$

    Show that $(\mathbb{Z}[\sqrt{2}]^*, \cdot, 1)$ is a group.

11. Let G be a group such that $g^2 = 1$ for all $g \in G$. Show that G is abelian.

12. Let G be a group. Show that the set

$$\mathrm{Aut}(G) := \{\phi \in \mathrm{Sym}(G) : \phi(xy) = \phi(x)\phi(y) \text{ for all } x,\, y \in G\}$$

is a group under composition.

13. Let G be a group. For $x,\, y \in G$, set $x^y = y^{-1}xy$. Show that $(xy)^z = x^z y^z$ and that $(x^y)^z = x^{yz}$.

14. Let G be a group. For $x,\, y \in G$, define $[x, y] = x^{-1}y^{-1}xy$. Show that for $x, y, z \in G$,

a) $[x, yz] = [x, z][x, y]^z$ and $[xy, z] = [x, z]^y[y, z]$.

b) (Philip Hall.) $[[x, y^{-1}], z]^y[[y, z^{-1}], x]^z[[z, x^{-1}], y]^x = 1$.

15. Let G be a group. Show that for $x, y \in G$ and n a positive integer,

$$[x^n, y] = [x, y]^{x^{n-1}}[x, y]^{x^{n-2}} \ldots [x, y]^x[x, y].$$

16. Let G be a group, X a set and $f : G \longrightarrow X$ a bijection. On X define the binary operation $xy = f(f^{-1}(x)f^{-1}(y))$. Show that X becomes a group under this operation.

17. Let G be a group. The **center** of G is defined to be the set

$$Z(G) := \{z \in G : zg = gz \text{ for all } g \in G\}.$$

Show that $Z(G)$ is a group under the multiplication of G.

18. Let G be a set together with a binary operation $*$ and an element $e \in G$ satisfying the properties G1, G3 and

$$\text{G2}'. \quad \text{For all } x \in G,\ x * e = x.$$

Show that $(G, *, e)$ is a group.

19. Let G be a set together with a binary operation $*$ and an element $e \in G$ satisfying the following properties G1, G2′ (see the above exercise) and

$$\text{G3}' \quad \text{For all } x \in G, \text{ there is a } y \in G \text{ such that } x * y = e.$$

Is $(G, *, e)$ a group?

20. Let G be a set together with a binary operation $*$ and a constant e satisfying the following properties G1, G2′ (the above exercise) and

$$\text{G3}'' \quad \text{For all } x \in G, \text{ there is a } y \in G \text{ such that } y * x = e.$$

Is $(G, *, e)$ a group?

21. Let G be a set together with an associative binary operation $(x, y) \mapsto xy$.

    a. Assume that for all $a, b \in G$ there are unique $x, y \in G$ such that $ax = ya = b$. Show that G is a group under this binary operation.

    b. Assume that for all $a, b \in G$ there is a unique $x \in G$ such that $ax = b$. Is G necessarily a group under this binary operation?

22. Let $(G, *, e)$ and $(H, \times, e')$ be two groups. Let $f : G \longrightarrow H$ be a map such that $f(x * y) = f(x) \times f(y)$ for all x, $y \in G$. Such a function is called a **group homomorphism** from the group G into the group H.

    a) Show that $f(e) = e'$.

    b) Show that $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$.

    c) Show that $f(x^n) = f(x)^n$ for all $x \in G$ and $n \in \mathbb{N}$.

    d) Show that $f^{-1}(e')$ is a group under $*$.

    e) Suppose f is a bijection. Show that $f^{-1}(u \times v) = f^{-1}(u) * f^{-1}(v)$ for all u, $v \in H$.

23. Let G be a group. Let

    $$\mathrm{Aut}(G) = \{f : G \longrightarrow G : f \text{ is a bijection and } f(xy) = f(x)f(y) \text{ for all } x, yinG\}.$$

    a. Show that $\mathrm{Aut}(G)$ is closed under composition.

    b. Show that $\mathrm{Id}_G \in \mathrm{Aut}(G)$.

    c. Show that if $f \in \mathrm{Aut}(G)$, then $f^{-1} \in \mathrm{Aut}(G)$.

    d. Conclude that $\mathrm{Aut}(G)$ is a group.

    Elements of $\mathrm{Aut}(G)$ are called **automorphisms** of the group G.

1.2 Example: $\mathrm{Sym}(X)$

We first study the group $\mathrm{Sym}(n)$ for $n \in \mathbb{N}$. Let us for example consider the following element g of $\mathrm{Sym}(7)$:

$$\begin{aligned} g(1) &= 2 \\ g(2) &= 5 \\ g(3) &= 3 \\ g(4) &= 7 \\ g(5) &= 1 \\ g(6) &= 6 \\ g(7) &= 4 \end{aligned}$$

We can represent this element as

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 7 & 1 & 6 & 4 \end{pmatrix}$$

or as $(1,2,5)(3)(4,7)(6)$ or as $(1,2,5)(4,7)$. We will prefer the last representation. The last representation can be read as follows: "1 goes to 2, 2 goes to 5, 5 goes back to 1; 4 goes to 7, 7 goes back to 4; the rest of the numbers (3 and 6) are fixed".

Written this way, the element $g = (1,2,5)(4,7)$ may be seen as an element of Sym(7) as well as an element of Sym(8). If one is careful enough when needed, this never causes a problem.

It is impossible to represent $\mathrm{Id}_{\mathrm{Sym}(6)}$ with the representation we adopted, so we will write simply $\mathrm{Id}_{\mathrm{Sym}(6)}$ or just 1 (with abuse of language).

Such a representation is called the **cyclic representation** of the element. The elements such as $(1,2,5)$, (3) and $(4,7)$ of the cyclic representation $(1,2,5)(4,7)$ are called **cycles**. The cycle $(1,2,3)$ is a 3-cycle. The cycle $(4,7)$ is a 2-cycle. The element $(1,2,5)(4,7)$ of Sym(7) has four cycles, namely $(1,2,5)$, (3), $(4,7)$ and (6). On the other hand, the element $(1,2,5)(4,7)$ of Sym(8) has five cycles, namely $(1,2,5)$, (3), $(4,7)$, (6) and (8). The element $\mathrm{Id}_{\mathrm{Sym}(6)}$ or 1 of Sym(6) has six cycles. But the element 1 of Sym(8) has eight cycles.

Clearly $(1,2,3) = (2,3,1) = (3,1,2) \neq (1,3,2)$.

Also $(1,2,5)(4,7) = (4,7)(1,2,5) = (7,4)(5,2,1)$.

The multiplication (more precisely, the composition) of disjoint cycles is very simple: One just juxtaposes them, e.g. the multiplication of $(1,2,5)$ and $(4,7)$ is just $(1,2,5)(4,7)$, or $(4,7)(1,2,5)$. Similarly, the product of the two elements $(1,5,7)(3,4)$ and $(2,6)(8,9)$ is just $(1,5,7)(2,6)(3,4)(8,9)$.

If the cycles are not disjoint, then the multiplication of elements is slightly more complicated. For example to compute $(1,2,3)(1,2,4,3,5)$ we start from the right and see where 1 goes to: 1 first goes to 2 (the right cycle) and the left cycle takes 2 to 3. Thus the product starts as $(1,3,\ldots$. Now we restart the same procedure with 3. As a result we obtain $(1,2,3)(1,2,4,3,5) = (1,3,5,2,4)$. As an exercise the reader should check that

$$(1,2,3,4)(3,5,4) = (1,2,3,5)$$
$$(1,3,2,4)(1,4)(3,5,4) = (2,4)(3,5)$$

The inverse of an element is easy to find. For example $(1,2,3,4,5)^{-1} = (1,5,4,3,2)$ and $((1,2,3,4)(5,6,7))^{-1} = (1,4,3,2)(5,7,6)$. On the other hand, $((1,2,3,5)(5,6,7))^{-1} = (5,6,7)^{-1}(1,2,3,5)^{-1} = (5,7,6)(1,5,3,2) = (1,7,6,5,3,2)$.

We can use the same notation for Sym($\mathbb{N}$). For example the element $g := (0,1)(2,3)(4,5)(6,7)\ldots$ is in Sym($\mathbb{N}$) and $g^2 = \mathrm{Id}_{\mathbb{N}}$. On the other hand the element $(0,1,2,3,4,5,\ldots)$ is not in Sym($\mathbb{N}$) because the number 0 is not in the image and this function is not onto, hence not a bijection. An infinite cycle in Sym($\mathbb{N}$) cannot have a beginning.

For example the element $(\ldots,7,5,3,1,2,4,6,8,\ldots)$ is in Sym($\mathbb{N}$).

The reader should not that, for the moment, we do not see the element $(0,1)(2,3)(4,5)(6,7)\ldots$ as the product of infinitely many elements $(0,1)$, $(2,3)$, $(4,5)$ etc. We can only multiply finitely many elements of a group[1].

[1] Unless there is a concept of limit in the group.

The **cycle type** of the element g of $\mathrm{Sym}(n)$ is a sequence of n natural numbers $a_1 - a_2 - \ldots - a_n$ where a_i is the number of i-cycles in the cyclic representation of g. For example the cycle type of $(1,2,5)(4,7) \in \mathrm{Sym}(8)$ is $3-1-1$, the cycle type of $(1,2,5)(4,7) \in \mathrm{Sym}(9)$ is $4-1-1$, the cycle type of $(1,2,3)(4,5,6) \in \mathrm{Sym}(6)$ is $0-0-2$. The following formalism is more convenient and expressive: We will say that $(1,2,5)(4,7) \in \mathrm{Sym}(8)$ is of cycle type $(1)(2)(3,4)(5,6,7)$, or even of type $(1,2)(3,4,5)$ if there is no possible confusion. For example the elements of $\mathrm{Sym}(5)$ of cycle type $(1,2,3)(4,5)$ are: $(1,2,3)(4,5)$, $(1,3,2)(4,5)$, $(1,2,4)(3,5)$, $(1,4,2)(3,5)$, $(1,2,5)(3,4)$, $(1,5,2)(3,4)$, $(1,3,4)(2,5)$, $(1,4,3)(2,5)$, $(1,3,5)(2,4)$, $(1,5,3)(2,4)$, $(1,4,5)(2,3)$, $(1,5,4)(2,3)$, $(2,3,4)(1,5)$, $(2,4,3)(1,5)$, $(2,3,5)(1,4)$, $(2,5,3)(1,4)$, $(2,4,5)(1,3)$, $(2,5,4)(1,3)$, $(3,4,5)(1,2)$, $(3,5,4)(1,2)$.

Exercises.

1. Write the elements of $\mathrm{Sym}(n)$ for $n = 1,\ 2,\ 3,\ 4$. Draw the multiplication table of these groups. Show that $\mathrm{Sym}(n)$ has $n!$ elements.

2. Find elements of each cycle type of $\mathrm{Sym}(n)$ for $n = 2, 3, 4, 5, 6$.

3. How many cycle types of elements are there in $\mathrm{Sym}(9)$ whose square is 1?

4. Find the number of elements of type $(1,2,3)(4,5,6)(7,8,9)(10,11,12,13)$ of $\mathrm{Sym}(15)$.

5. Let $g := (\ldots, 7, 5, 3, 1, 2, 4, 6, 8, \ldots) \in \mathrm{Sym}(\mathbb{N})$. Show that $g^n \neq 1$ for any $n \in \mathbb{Z} \setminus \{0\}$.

6. Let $a := (0,1) \in \mathrm{Sym}(\mathbb{N})$. Show that $C_{\mathrm{Sym}(\mathbb{N})}(a) := \{g \in \mathrm{Sym}(\mathbb{N}) : ga = ag\} = \{g \in \mathrm{Sym}(\mathbb{N}) : g(\{0,1\}) = \{0,1\}\}$.

7. Multiply the elements $(0,1)(1,2)(3,4)\ldots$ and $(1,2)(3,4)(5,6)\ldots$ of $\mathrm{Sym}(n)$. How many cycles does the product have?

8. For a group G and an element $g \in G$, define $o(g)$, the **order** of g, to be the least positive natural number m such that $g^m = 1$ if there is such an m, otherwise define $o(g) = \infty$. Thus $o(g) = 1$ if and only if $g = 1$.

   Let $G = \mathrm{Sym}(\mathbb{N})$. Show that $o(1,2,3) = 3$, $o(1,2,3,4) = 4$, $o((1,2,3)(4,5)) = 6$, $o(\ldots, 7, 5, 3, 1, 2, 4, 6, 8, \ldots) = \infty$.

   For each $n = 1, 2, \ldots, 12$, find $\max\{o(g) : g \in \mathrm{Sym}(n)\}$.

9. The **exponent** $\exp(G)$ of a group G is the minimum natural number $n > 0$ such that $g^n = 1$ for all $g \in G$ if there is such a natural number, otherwise the exponent of a group is said to be infinite. Show that $\exp(\mathrm{Sym}(3)) = 6$. Find $\exp(\mathrm{Sym}(n))$ for $n = 4, \ldots, 12$.

10. Show that if $\exp(G) = n$ and $\exp(H) = m$, then $\exp(G \times H) = \mathrm{lcm}(m, n)$.

11. ** Is it true that every element of $\mathrm{Sym}(\mathbb{N})$ is a product of finitely many squares?

12. ** Is it true that every element of $\mathrm{Sym}(\mathbb{N})$ is a product of finitely many p-th powers?

1.3 Example: Automorphism Groups of Graphs

1.3.1 Automorphisms of Binary Relational Structures

A **binary relation** on a set X is just a subset R of $X \times X$. Instead of $(x, y) \in R$, we prefer to write xRy. A **binary relational structure** Γ is a set X together with a binary relation R. Thus a binary relational structure Γ is a pair (X, R) where X is a set and R is a binary relation Γ.

An **isomorphism** of a binary relational structure (X, R) into another binary relational structure (Y, S) is a bijection $f : X \longrightarrow Y$ such that for any x_1, $x_2 \in X$, $x_1 R x_2$ if and only if $f(x_1)Rf(x_2)$. An isomorphism from a binary relational structure onto itself is called an **automorphism** of the binary relational structure. The set of all automorphisms of a binary relational structure Γ is a group and is called the **automorphism group** of Γ and is denoted by $\mathrm{Aut}(\Gamma)$.

Two relational structures Γ and Γ_1 among which there is an isomorphism are called **isomorphic**. We then write $\Gamma \simeq \Gamma_1$.

The **dual** of a binary relational structure (X, R) is the binary relational structure (X, S) defined as follows:

$$xSy \text{ if and only if } xRy \text{ does not hold.}$$

Exercises.

1. Show that the set $\mathrm{Aut}(\Gamma)$ of all automorphisms of a binary relational structure Γ is a group under composition.

2. Let Γ, Γ_1 and Γ_3 be binary relational structures. Show that

   a) $\Gamma \simeq \Gamma$.

   b) If $\Gamma \simeq \Gamma_1$ then $\Gamma_1 \simeq \Gamma$

   c) If $\Gamma \simeq \Gamma_1$ and $\Gamma_1 \simeq \Gamma_2$ then $\Gamma \simeq \Gamma_2$.

3. Show that the automorphism groups of a binary relational structure and its dual are equal.

4. Let (X, R) and (Y, S) be two binary relational structure. Let ϕ be an isomorphism from (X, R) onto (Y, S). Show that $\mathrm{Aut}(Y, S) = \phi\,\mathrm{Aut}(X, R)\phi^{-1}$.

5. Let X be a set. On the set $\wp(X)$ of all subsets of X consider the binary relation $\subseteq$.

   For any $f \in \mathrm{Sym}(X)$, define $\phi_f : \wp(X) \longrightarrow \wp(X)$ by $\phi_f(A) = f(A)$. Show that $\phi_f \in \mathrm{Aut}(\wp(X), \subseteq)$. Show that $\mathrm{Aut}(\wp(X), \subseteq) = \{\phi_f : f \in \mathrm{Sym}(X)\}$. Show that, for f, $g \in \mathrm{Sym}(X)$, $\phi_f \circ \phi_g = \phi_{f \circ g}$.

6. Let (X, R) be a relational structure. We will call a bijection $\phi : X \longrightarrow X$ a **soft automorphism** if for all x, $y \in X$, if xRy then $\phi(x)R\phi(y)$.

   Is the set of all soft automorphism necessarily a group?

   Let now X be any set. Find the set of soft automorphisms of $(\wp(X), \subseteq)$.

1.3.2 Graphs and Their Automorphisms

A binary relation R on a set X is called **symmetric** if xRy implies yRx for all x, $y \in X$; it is called **reflexive** if xRx for all $x \in X$; it is called **irreflexive** if xRx does not hold for any $x \in X$.

A **graph** Γ is a set X together with a symmetric and irreflexive binary relation X. Thus a graph Γ is a pair (X, R) where X is a set and R is a symmetric and irreflexive binary relation on X.

If (X, R) is a graph and x, $y \in X$ are such that xRy then we say that x and y are **connected** or that they are of **distance** 1. We often write $x - y$ instead of xRy. In that case, we also say that x and y are **related** and that $x - y$ is an **edge**. The elements of a graph are called **vertices**. A chain of the form $x = x_0 - x_1 - \ldots - x_{n-1} - x_n = y$ is called a **path**. If all the vertices x_i are distinct, the path is called a **reduced path**. If x and y are two vertices of a graph such that $x = x_0 - x_1 - \ldots - x_{n-1} - x_n = y$ for some $x_1, \ldots, x_{n-1}$ and if n is minimal such number, we say that n is the **distance** between x and y. In that case the path $x = x_0 - x_1 - \ldots - x_{n-1} - x_n = y$ is called a **minimal path**. Otherwise the distance is said to be infinite. A minimal path is necessarily reduced. A graph whose vertices are all connected to each other by a path is called a **connected graph**. The maximum of the distances of vertices of a graph is called **diameter** of the graph. A **cycle** in a graph is a closed reduced path, i.e. a reduced path of the form $x = x_0 - x_1 - \ldots - x_{n-1} - x_n = x$. A **triangle-free** graph is a graph without cycles of length three. A **square-free** graph is a graph without cycles of length four. In a cycle-free graph, all minimal paths are unique.

Exercises.

1. Let us find all graph structures on the set $X = \{1, 2, 3\}$. For any two distinct points x and y we know that if $x - y$ then $y - x$, so to shorten our writing, we will write only one of the two relations (or edges).

   $\Gamma_\emptyset$: no relations at all
   Γ_3 : only $1 - 2$ (and $2 - 1$ of course)
   Γ_2 : only $1 - 3$
   Γ_1 : only $2 - 3$
   Γ_{13} : only $1 - 2$ and $2 - 3$
   Γ_{12} : only $1 - 3$ and $2 - 3$
   Γ_{23} : only $1 - 2$ and $1 - 3$
   Γ_{123} : all possible relations $1 - 2$, $2 - 3$ and $1 - 3$

Show that Γ_1, Γ_2 and Γ_3 are isomorphic. Show that Γ_{13}, Γ_{12} and Γ_{23} are isomorphic. Show that G_1 and G_{23} are not isomorphic, but duals of each other.

Thus on X there are only fundamentally different (i.e. nonisomorphic) graph structures: $\Gamma_\emptyset$, Γ_1, Γ_{23} and Γ_{123}.

Show that $\mathrm{Aut}(\Gamma_\emptyset) = \mathrm{Aut}(\Gamma_{123}) = \mathrm{Sym}(3)$ and $\mathrm{Aut}(\Gamma_1) = \mathrm{Aut}(\Gamma_{23}) = \{1, (2,3)\}$.

2. The **complete graph** on a set X is the graph where any two distinct $x, y \in X$ are related. Show that the automorphism group of a complete graph on a set X is $\mathrm{Sym}(X)$.

3. Consider the following graphs on $X := \{1,2,3,4\}$:

$\Gamma_\emptyset$: no relations at all
Γ_{12} : only $1-2$ (and $2-1$ of course)
Γ_{123} : only $1-2$ and $2-3$
Γ_{12-34} : only $1-2$ and $3-4$
Γ_{1234} : only $1-2$, $2-3$ and $3-4$
Γ_* : only $1-2$, $1-3$ and $1-4$

Show that

$\mathrm{Aut}(\Gamma_\emptyset) = \mathrm{Sym}(4)$
$\mathrm{Aut}(\Gamma_{12}) = \mathrm{Aut}(\Gamma_{12-34}) = \{1, (1,2), (3,4), (1,2)(3,4)\}$
$\mathrm{Aut}(\Gamma_{123}) = \{1, (1,3)\}$
$\mathrm{Aut}(\Gamma_{12-34}) = \{1, (12), (34), (12)(34), (13)(24), (23)(14), (1324), (1223)\}$
$\mathrm{Aut}(\Gamma_{1234}) = \{1, (14)(23)\}$
$\mathrm{Aut}(\Gamma_*) = \{1, (12), (13), (23), (123), (132)\}$

Show that the automorphism group of a graph Γ on $X = \{1,2,3,4\}$ is the automorphism group of one of the above graphs.

Draw the multiplication table of $\mathrm{Aut}(\Gamma_{12-34})$

4. Find a graph Γ on six points such that $\mathrm{Aut}(\Gamma) = 1$.

5. Find a finite graph Γ such that $|\mathrm{Aut}(\Gamma)| = 3$. Find one with 10 vertices.

6. Let X be a set. Let Γ be the set of subsets of X with two elements. On Γ define the relation $\alpha R \beta$ if and only if $\alpha \cap \beta = \emptyset$. Then Γ becomes a graph with this relation.

a) Calculate $\mathrm{Aut}(\Gamma)$ when $|X| = 4$.

b) Draw the graph Γ when $X = \{1,2,3,4,5\}$.

c) Show that $\mathrm{Sym}(5)$ imbeds in $\mathrm{Aut}(\Gamma)$ naturally. (You have to show that each element σ of $\mathrm{Sym}(5)$ gives rise to an automorphism $\tilde{\sigma}$ of Γ in such

a way that the map $\sigma \mapsto \tilde{\sigma}$ is an injection from Sym(5) into Aut(Γ) and that $\widetilde{\sigma_1 \circ \sigma_2} = \widetilde{\sigma_1} \circ \widetilde{\sigma_2}$).

d) Show that Aut(Γ) $\simeq$ Sym(5).

Solution: (a) The graph Γ is just six vertices joined two by two. A group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ preserves the edges. And Sym(3) permutes the edges. Thus the group has $8 \times 3! = 48$ elements.

More formally, one can prove this as follows. Let the points be $\{1,2,3,4,5,6\}$ and the edges be $v_1 = (1,4)$, $v_2 = (2,5)$ and $v_3 = (3,6)$. We can embed Sym(3) in Aut(Γ) $\leq$ Sym(6) via

$$\begin{array}{lcl} \mathrm{Id}_3 & \mapsto & \mathrm{Id}_6 \\ (12) & \mapsto & (12)(45) \\ (13) & \mapsto & (13)(46) \\ (23) & \mapsto & (23)(56) \\ (123) & \mapsto & (123)(456) \\ (132) & \mapsto & (132)(465) \end{array}$$

For any $\phi \in$ Aut(Γ) there is an element α in the image of Sym(3) such that $\alpha^{-1}\phi$ preserves the three edges $v_1 = (1,4)$, $v_2 = (2,5)$ and $v_3 = (3,6)$. Thus $\alpha^{-1}\phi \in \mathrm{Sym}\{1,4\} \times \mathrm{Sym}\{2,5\} \times \mathrm{Sym}\{3,6\} \simeq (\mathbb{Z}/2\mathbb{Z})^3$. It follows that Aut($\Gamma$) $\simeq (\mathbb{Z}/2\mathbb{Z})^3 \rtimes$ Sym(3) (to be explained next year).

(b) There are ten points. Draw two pentagons one inside the other. Label the outside points as $\{1,2\}$, $\{3,4\}$, $\{5,1\}$, $\{2,3\}$, $\{4,5\}$. Complete the graph.

(c and d) Clearly any element of $\sigma \in$ Sym(5) gives rise to an automorphism $\tilde{\sigma}$ of Γ via $\tilde{\sigma}\{a,b\} = \{\sigma(a), \sigma(b)\}$. The fact that this map preserves the incidence relation is clear. This map is one to one because if $\tilde{\sigma} = \tilde{\tau}$, then for all distinct a, b, c, we have $\{\sigma(b)\} = \{\sigma(a), \sigma(b)\} \cap \{\sigma(b), \sigma(c)\} = \tilde{\sigma}\{a,b\} \cap \tilde{\sigma}\{b,c\} = \tilde{\tau}\{a,b\} \cap \tilde{\tau}\{b,c\} = \{\tau(a), \tau(b)\} \cap \{\tau(b), \tau(c)\} = \{\tau(b)\}$ and hence $\sigma(b) = \tau(b)$.

Let $\phi \in$ Aut(Γ). We will compose ϕ by elements of Sym(5) to obtain the identity map. There is an $\sigma \in$ Sym(5) such that $\phi\{1,2\} = \tilde{\sigma}\{1,2\}$ and $\phi\{3,4\} = \tilde{\sigma}\{3,4\}$. Thus, replacing ϕ by $\sigma^{-1}\phi$, we may assume that ϕ fixes the vertices $\{1,2\}$ and $\{3,4\}$. Now ϕ must preserve or exchange the vertices $\{3,5\}$ and $\{4,5\}$. By applying the element (34) of Sym(5) we may assume that these two vertices are fixed as well. Now ϕ must preserve or exchange the vertices $\{1,3\}$ and $\{2,3\}$. By applying the element (12) of Sym(5) we may assume that these two vertices are fixed as well. Now all the vertices must be fixed.

7. Let $n \geq 3$ and let Γ be the cyclic graph on $\{1,2,\ldots,n\}$, i.e. the only relations are $1-2-3-\ldots-(n-1)-n-1$. Show that $\rho := (1,2,\ldots,n) \in$ Aut(Γ). Show that $\tau = (2,n)(3,n-1)\ldots \in$ Aut(Γ). (For example if $n = 6$ then $\tau = (2,6)(3,5)$, if $n = 7$ then $\tau = (2,7)(3,6)(4,5)$). Show that

$$\mathrm{Aut}(\Gamma) = \{\rho^i \tau^j : i = 0, 1, \ldots, n-1 \text{ and } j = 0, 1\}$$

and that $|\operatorname{Aut}(\Gamma)| = 2n$.

1.3.3 Binary Trees and Their Automorphism Groups

A **regular binary tree** Γ_n **of height** n is the finite graph on the set $\{1, 2, \ldots, 2^{n-1}\}$ where two vertices a and b are connected if and only if 2^n divides either $(a-2b)$ or $(b-2a)$ and $b \neq a$.

Exercises **1.** Draw Γ_1, Γ_2, Γ_3 and Γ_4. (To visualize better this tree, start by putting 2^{n-1} to the bottom of the page and go upwards).

2. Find $\operatorname{Aut}(\Gamma_2)$ and draw its multiplication table.

3. Show that $(1,5)(3,7) \in Z(\operatorname{Aut}(\Gamma_2))$. (See Exercise 17, 14).

Lemma 1.3.1 *The following hold in the regular binary tree* Γ_n *(*$n > 1$*):*

a) The element 2^{n-1} *(called the root) is the only vertex connected to exactly two vertices, namely to* $a := 2^{n-2}$ *and* $b := 2^{n-2} + 2^{n-1}$.

b) The odd numbers (called extremities) are the only vertices connected to only one vertex.

c) Any automorphism of Γ_n *fixes* 2^{n-1}*, either fixes or swaps* a *and* b*, and stabilizes the extremities.*

d) Let $H := \{\gamma \in \operatorname{Aut}(\Gamma_n) : \gamma(a) = a\}$ *and* $H_1 := \operatorname{Aut}(\Gamma_n) \setminus H$*. Then for any* $\alpha \in H_1$*,* $\alpha H = H_1$*. Also* $H \simeq \operatorname{Aut}(\Gamma_{n-1}) \times \operatorname{Aut}(\Gamma_{n-1})$*. Hence* $|\operatorname{Aut}(\Gamma_n)| = 2|\operatorname{Aut}(\Gamma_{n-1})|^2 = 2^{2^n-1}$.

Proof: Easy. For part (d) note that $\Gamma_n \setminus \{2^{n-1}\}$ is the union of two disjoint isomorphic copies of Γ_{n-1}. □

Proposition 1.3.2 $\operatorname{Aut}(\Gamma_n)$ *has* 2^{2^n-1} *elements. Its center consists just of two elements* Id *and the automorphism that exchanges the extremities of distance 2.*

Proof: We will prove the first statement by induction on n. For $n = 0$ the statement is clear. An automorphism of Γ_{n+1} must fix the root 2^n because the root is the only vertex with two edges. Thus an automorphism of Γ_{n+1} must either fix or exchange the two vertices $a := 2^{n-2}$ and $b := 2^{n-2}+2^{n-1}$ of distance one from the root. Let $H = \{\phi \in \operatorname{Aut}(\Gamma_{n+1}) : \phi(a) = a \text{ and } \phi(b) = b\}$ and $H_1 = \{\phi \in \operatorname{Aut}(\Gamma_{n+1}) : \phi(a) = b \text{ and } \phi(b) = a\}$. Thus $\operatorname{Aut}(\Gamma_{n+1}) = H \sqcup H_1$. For $\gamma \in H_1$, $H_1 = \gamma H$, thus $|H| = |H_1|$ and so $|\operatorname{Aut}(\Gamma_{n+1})| = 2|H|$. But H acts on the trees on top of the vertices a and b and these subtrees are isomorphic to Γ_n. It follows easily that $H \simeq \operatorname{Aut}(\Gamma_{n-1}) \times \operatorname{Aut}(\Gamma_{n-1})$. Thus $|H| = |\operatorname{Aut}(\Gamma_n)|^2$. Hence $|\operatorname{Aut}(\Gamma_n)| = 2|\operatorname{Aut}(\Gamma_n)|^2$. Now it follows quite easily by induction that $|\operatorname{Aut}(\Gamma_n)| = 2^{2^n-1}$.

Consider the element ζ that swaps the extremities of Γ_n and fixes the rest. Let $\gamma \in \operatorname{Aut}(\Gamma_n)$. We want to show that $\gamma\zeta = \zeta\gamma$. Let x be a vertex in G_n. If x is not an extremity, then $\gamma\zeta(x) = \gamma(x)$ because $\zeta(x) = x$ and $\zeta\gamma(x) = \gamma(x)$ because $\gamma(x)$ cannot be an extremity. If x is an extremity, then $g(x)$ is also an extremity and so $\zeta\gamma(x) = \gamma(x)'$ and $\gamma\zeta(x) = \gamma(x')$. (Here x' and $\gamma(x)'$ denote

the unique extremities of distance two from x and $\gamma(x)$ respectively). Thus we have to show that $\gamma(x') = \gamma(x)'$. Since x and x' have distance two, $\gamma(x)$ and $\gamma(x')$ have distance two as well. Thus $\gamma(x)' = \gamma(x')$. Thus ζ is in the center of $\mathrm{Aut}(\Gamma_n)$.

Conversely let $\zeta \in Z(\mathrm{Aut}(\Gamma_n))$.

Assume first that ζ fixes a and b. Then ζ fixes the two trees above a and b. By induction we know how ζ acts on these subtrees. Assume it acts as swap on the left tree (the one above a) and as identity on the right one. Let $\gamma \in \mathrm{Aut}(\Gamma_n)$ swap these two subtrees in some way or other. Then $\zeta\gamma(x) = \gamma\zeta(x)$ for all extremities x. If x is on the right, then $\zeta\gamma(x) = \gamma(x)' \neq \gamma(x) = \gamma\zeta(x)$, a contradiction. Thus ζ swaps all extremities.

Assume now ζ exchanges a and b and hence the trees above them. Let γ be identity on the left tree and swap on the right tree. Then for an extremity x of the left tree, $\gamma\zeta(x) = \zeta(x)' \neq \zeta(x) = \zeta\gamma(x)$, a contradiction. □

Exercises. Show that Γ_{n-1} is isomorphic to the subtree $\Gamma_n \backslash \{\text{extremities of } \Gamma_n\}$ via the map $x \mapsto x/2$. From now on we identify them. Conclude that the map from $\mathrm{Aut}(\Gamma_n)$ into $\mathrm{Aut}(\Gamma_{n-1})$ that sends γ to the restriction of γ to the set of non-extremities of Γ_n ($\simeq \Gamma_{n-1}$) is a surjection. What is its kernel? (Not defined yet)

Chapter 2

Subgroups

2.1 Definition and Examples

Let G be a group and H a subset of G. If the set H together with the multiplication of G is a group, then we say that H is a **subgroup** of G.

Examples.

1. The subset $\{1, (123), (132)\}$ of Sym(3) is a subgroup of Sym(3).
2. The set $2\mathbb{Z}$ of even integers is a subgroup of $\mathbb{Z}$, .
3. The center $Z(G)$ of a group G is a subgroup of G. (See Exercise 17, page 14).

When H is a subgroup of G, we write $H \leq G$. If $H \leq G$ and $H \neq G$, then we write $H < G$ and we say that H is a **proper** subgroup of G.

For a subset H of G to be a subgroup of G we need the following conditions:
1. H must be closed under the multiplication of G, i.e. we must have $h_1 h_2 \in H$ for all h_1, $h_2 \in H$.
2. The identity element 1 of G must be in H.
3. For $h \in H$, h^{-1} must be in H.

The first condition says that the binary operation of G restricted to H is a binary operation on H. The second condition says that H has an identity element. The third condition says that the inverse of an element of H, which is in G, is in fact in H. The associativity of the multiplication in H holds automatically since it holds in G.

Lemma 2.1.1 *A subset H of a group G is a subgroup if and only if $H \neq \emptyset$ and $HH^{-1} \subseteq H$. (Here $HH^{-1} = \{h_1 h_2^{-1} : h_1, h_2 \in H\}$).*

Proof: From left to right it is clear. We prove the other direction.

a) Since $H \neq \emptyset$, we may choose an element $h \in H$. Then $1 = hh^{-1} \in HH^{-1} \subseteq H$, so $1 \in H$.

b) Let $h \in H$. Then by part (a), $h^{-1} = 1h^{-1} \in HH^{-1} \subseteq H$, so $h^{-1} \in H$.

c) Let $h_1, h_2 \in H$. Then by part (b), $h_1 h_2 = h_1(h_2^{-1})^{-1} \in HH^{-1} \subseteq H$, so $h_1 h_2 \in H$. □

Examples.

1. $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+$.

2. $\{1, -1\} \leq \mathbb{Q}^* \leq \mathbb{R}^*$.

3. $\mathbb{Q}^{>0} \leq \mathbb{R}^{>0}$. But $\mathbb{Q}^{>0}$ is not a subgroup of $\mathbb{Q}$ because these groups do not have the same operations.

4. $n\mathbb{Z} \leq \mathbb{Z}$. By Exercise 5, page 13 (see also Lemma 2.1.2), these are the only subgroups of $\mathbb{Z}$.

5. For any group G, $\{1\} \leq G$ and $G \leq G$. By abuse of language, the subgroup $\{1\}$ is denoted by 1. It is called the **trivial** subgroup of G. Any subgroup H of G which is not G is called a **proper** subgroup; in this case we write $H < G$.

6. For any group G and any $g \in G$, the set $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G.

7. Let I be a set and for each $i \in I$, let G_i be a group.Then the **direct sum**

$$\oplus_{i \in I} G_i := \{g \in \prod_{i \in I} G_i : g_i \neq 1 \text{ for only finitely many } i \in I\}$$

   is a subgroup of the direct product $\prod_{i \in I} G_i$. If I is infinite then $\oplus_I G_i < \prod_{i \in I} G_i$.

8. Properly speaking $\mathrm{Sym}(n-1)$ is not a subgroup of $\mathrm{Sym}(n)$, in fact $\mathrm{Sym}(n-1)$ is not even a subset of $\mathrm{Sym}(n)$, because the elements of the first group are the bijections of the set $\{1, \ldots, n-1\}$ and the elements of the second group are the bijections of the set $\{1, \ldots, n\}$. But we may regard the elements of $\mathrm{Sym}(n-1)$ as the elements of $\mathrm{Sym}(n)$ that fixe the point n. For example the elements

$$\begin{array}{c} (1)(2)(3) \\ (1,2)(3) \\ (1,3)(2) \\ (2,3)(1) \\ (1,2,3) \\ (1,3,2) \end{array}$$

of Sym(3) may be regarded as the elements

$$(1)(2)(3)(4)$$
$$(1,2)(3)(4)$$
$$(1,3)(2)(4)$$
$$(2,3)(1)(4)$$
$$(1,2,3)(4)$$
$$(1,3,2)(4)$$

of Sym(4). Viewing this way, we may regard Sym(3) as a subgroup of Sym(4). More generally, if $Y \subseteq X$, Sym(Y) can be regarded as a subgroup of Sym(X) by regarding the elements of Sym(Y) as the elements of Sym(X) that fix the set $X \setminus Y$ pointwise.

Lemma 2.1.2 (Subgroups of $\mathbb{Z}$) *Any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for a unique $n \in \mathbb{N}$.*

Proof: Let $H \leq \mathbb{Z}$. If $H = 0$, we choose $n = 0$. So assume $H \neq 0$. Then, since $-H = H$, the set $H \cap \mathbb{N} \setminus \{0\}$ is nonempty. Let n be the smallest element of $H \cap \mathbb{N} \setminus \{0\}$. We will show that $H = n\mathbb{Z}$. Since $n \in H$ and H is a group, $n\mathbb{Z} \leq H$. Conversely, let $h \in H$. Divide h by n: $h = nq + r$ for some q and $r = 0, 1, \ldots, n-1$. Now $r = h - nq \in H$ because $nq \in n\mathbb{Z} \leq H$ and $h \in H$. By the choice of n, this implies that $r = 0$. Thus $h = nq \in n\mathbb{Z}$. □

Lemma 2.1.3 *Let G be a group and $(H_i)_{i \in I}$ any family of subgroups of G. Then $\bigcap_{i \in I} H_i$ is a subgroup of G.*

Proof: Trivial. □

Exercises.

1. Check that $\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq \text{Sym}(4)$.

2. Let G be a group and $a \in G$. Show that $C_G(a) := \{g \in G : ga = ag\}$ is a subset of G closed under multiplication. Show that $C_G(a)$ is a subgroup of G. This subgroup is called the **centraliser** of a in G.

3. Let G be a group

   a) Show that if $A \subseteq B \subseteq G$, then $C_G(B) \leq C_G(A)$.

   b) Show that for any $A \subseteq G$, $A \subseteq C_G(C_G(A))$.

   c) Show that for any $A \subseteq G$, $C_G(A) = C_G(C_G(C_G(A)))$.

4. Let X be any set and $Y \subseteq X$. Show that $\{g \in \text{Sym}(X) : g(Y) = Y\}$ is a subgroup of Sym(X).

5. Let X be any set and $Y \subseteq X$. Show that $\{g \in \text{Sym}(X) : g(y) = y \text{ for all } y \in Y\}$ is a subgroup of Sym(X).

6. Let G be an abelian group and $n \in \mathbb{N}$. Show that $\{g^n : g \in G\}$ and $\{g \in G : g^n = 1\}$ are subgroups of G.

7. Let G be an abelian group. Show that $\{g \in G : g^n = 1 \text{ for some } n \in \mathbb{N} \setminus \{0\}\}$ is a subgroup of G.

8. Show that $\{g \in \mathrm{Sym}(X) : g^n = 1 \text{ for some } n \in \mathbb{N} \setminus \{0\}\}$ is not a subgroup of $\mathrm{Sym}(X)$ unless $|X| \leq 2$.

9. Let H be a nonempty finite subset of a group G closed under multiplication. Show that H is a subgroup of G. Does this hold for infinite subsets?

10. For $n, m \in \mathbb{N} \setminus \{0\}$, show that $n\mathbb{Z} \leq m\mathbb{Z}$ if and only if m divides n.

11. Find all subgroups of $\mathrm{Sym}(3)$.

12. Find all subgroups of $\mathrm{Sym}(3) \times \{1, -1\}$.

13. Let G be a group and A and B two subgroups. Show that if $G = A \cup B$ then either $G = A$ or $G = B$

14. Let G be a group and A, B and C three proper subgroups. Assume that $G = A \cup B \cup C$. What can you say about G?

15. Let $r \in \mathbb{R}$. Show that $\langle r \rangle = r\mathbb{Z}$.

16. Let $r, s \in \mathbb{R}$. Show that the set $r\mathbb{Z} + s\mathbb{Z} := \{ra + sb : a, b \in \mathbb{Z}\}$ is a subgroup of $\mathbb{R}$. More generally, let $X \subseteq \mathbb{R}$ be any subset of $\mathbb{R}$. Show that the set
$$\{\sum_{i=1}^{n} x_i a_i : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z}\}$$
is a subgroup of $\mathbb{R}$.

17. Let H and K be two subgroups of a group G. Show that $\{HxK : x \in G\}$ is a partition of G, i.e. show that for any $x, y \in G$, either $HxK \cap HyK = \emptyset$ or $HxK = HyK$. The set HxK is called a **double coset**. (See also Lemma 2.3.1).

    Proof: The relation $x \equiv y$ defined by "$HxK = HyK$" is certainly reflexive and symmetric. Let us prove the transitivity. It is clear that $HxK = HyK$ if and only if $x \in HyK$. Thus if $x \in HyK$ and $y \in HzK$, then $x \in HHzKK \subseteq HzK$. □

18. Let G be any group. Let $X \subseteq G$. Show that the set
$$\{x_1^{a_1} \dots x_n^{a_n} : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z}\}$$
is a subgroup of G.

19. Let G be a group and A and B be two subgroups of G. Let $AB = \{ab : a \in A,\, b \in B\}$.

    a) Show that there is a quite a natural one to one correspondence between AB and BA.

    b) Consider the map $f : A \times B \longrightarrow AB$ given by $f(a, b) = ab$. Show that $f^{-1}(ab) = \{ac, c^{-1}b : c \in A \cap C\}$.

    c) Conclude that if A and B are finite then $|AB| = |A||B|/|A \cap B|$.

    d) Show that AB is a subgroup of G if and only if $BA \subseteq AB$ if and only if $AB = BA$.

20. Show that any two nontrivial subgroups of $\mathbb{Q}$ intersect nontrivially. What is the intersection of all the nontrivial subgroups of $\mathbb{Q}$?

21. Let G be any group. Let $X \subseteq G$. Show that the set

$$\{x_1^{a_1} \dots x_n^{a_n} : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z}\}$$

    is a subgroup of G. (By convention, $\sum_{i=1}^{0} a_i = 0$).

22. Let G be any group. Let $X \subseteq G$. Show that the set

$$\{x_1^{a_1} \dots x_n^{a_n} : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z},\, \sum_{i=1}^{n} a_i \text{ is even}\}$$

    is a subgroup of G.

23. Let X be a set. For $\alpha \in \mathrm{Sym}(X)$, let $\mathrm{Stab}(\alpha) = \{x \in X. : \alpha(x) = x\}$. Let $\mathrm{Sym}^{<\omega}(X) = \{\alpha \in \mathrm{Sym}(\omega) : \mathrm{Stab}(\alpha) \text{ is cofinite } \} = \{g \in \mathrm{Sym}(\mathbb{N}) : g(x) \neq x \text{ for only finitely many elements of } \mathbb{N}\}$. Then $\mathrm{Sym}^{<\omega}(X) \leq \mathrm{Sym}(\omega)$.

24. Let X be a set and κ a cardinal number. Let $\mathrm{Sym}^{<\kappa}(X) = \{\alpha \in \mathrm{Sym}(\omega) : |X \setminus \mathrm{Stab}(\alpha)| < \kappa\}$. Then $\mathrm{Sym}^{<\kappa}(X) \leq \mathrm{Sym}(\omega)$.

2.2 Generators

Let $X \subseteq G$. Then by Lemma 2.1.3, the intersection $\bigcap_{X \subseteq H \leq G} H$ of all the subgroups of G that contain X is a subgroup of G. Since it also contains X, $\bigcap_{X \subseteq H \leq G} H$ is the smallest subgroup of G containing X. We let

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

and call it the **subgroup generated** by X.

The following clearly hold:

If $x \in X$ then $x \in \langle X \rangle$
If $x \in X$ and $\epsilon = \pm 1$ then $x^\epsilon \in \langle X \rangle$
If $x_1, \dots, x_n \in X$ and $\epsilon_1, \dots, \epsilon_n \in \{1, -1\}$ then $x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in \langle X \rangle$

It follows that the set $\{x_1^{\epsilon_1} \in x_n^{\epsilon_n} : n \in \mathbb{N}, x_i \in X, \epsilon_i = \pm 1\}$ is a subset of $\langle X \rangle$. On the other hand by Exercise 21, page 29, the set $\{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} : n \in \mathbb{N}, x_i \in X, \epsilon_i = \pm 1\}$ is a subgroup of G; since it also contains X, by the fact that $\langle X \rangle$ is the smallest subgroup of G containing X, we must have the equality. We have proved:

Lemma 2.2.1 *Let $X \subseteq G$. Then*

$$\{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} : n \in \mathbb{N}, x_i \in X, \epsilon_i = \pm 1\} = \langle X \rangle.$$

We say that the subgroup $\langle X \rangle$ is **generated** by X. The set X is called a **set of generators of** $\langle X \rangle$. For any $H \leq G$, clearly $\langle H \rangle = H$.

If $G = \langle X \rangle$ for some finite subset X of G, we say that G is finitely generated. It is not true in general that a subgroup of a finitely generated group is finitely generated (¶ For example, if $G = F_2$, the free group on two generators, then G' is not finitely generated).

If $G = \langle x \rangle$ for some $x \in G$, then the group G is called **cyclic**. Cyclic groups are of course abelian (Lemma 1.1.4).

Exercises.

1. Find the subgroup of
   a. $\mathbb{Q}^+$ generated by $2/3$.
   b. qq^+ generated by $2/3$ and $4/9$.
   c. $\mathbb{Q}*$ generated by $\{1/p : p \text{ a prime in } \mathbb{N}\}$.
   d. $\mathbb{Q}*$ generated by $\{1/p : p \text{ an odd prime in } \in \mathbb{N}\}$.
2. **Generators of** $\mathrm{Sym}(n)$**.** a) Show that $\langle (12), (13), \dots, (1,n) \rangle = \mathrm{Sym}(n)$.
   b) Show that $\langle (1,2), (2,3), \dots, (n-1,n) \rangle = \mathrm{Sym}(n)$.
   c) Show that $\langle (1,2,\dots,n), (1,2) \rangle = \mathrm{Sym}(n)$.
3. What is the subgroup of $\mathrm{Sym}(12)$ generated by the element $(12)(345)(6789)$?
4. **Finitely Generated Subgroups of** $\mathbb{Q}$**.** Let $G = \mathbb{Q}$. Let $q_1, \dots, q_n \in \mathbb{Q}$. Show that there is a $q \in \mathbb{Q}$ such that $\langle q_1, \dots, q_n \rangle = \langle q \rangle$.
5. Let $G = \mathbb{Q}$. For $i \in \mathbb{N}$, let $q_i = 1/2^i$. Show that $\langle q_i : i \in \mathbb{N} = \{a/2^i : a \in \mathbb{Z} \text{ and } i \in \mathbb{N}\}$ and that this subgroup of $\mathbb{Q}$ is not generated by finitely many elements of $\mathbb{Q}$.
6. Show that $\mathbb{Q}^+$ is not finitely generated.
7. Show that any two nontrivial subgroups of $\mathbb{Q}$ intersect nontrivially.
8. Find all subgroups of $\mathbb{Q}^+$.

9. **Greatest Common Divisor.** Let $G = \mathbb{Z}$ and $n, m \in \mathbb{Z}$. Show that $\langle n, m\rangle = n\mathbb{Z} + m\mathbb{Z}$. Conclude that $n\mathbb{Z} + m\mathbb{Z} = s\mathbb{Z}$ for some $s \in \mathbb{N}$ (Exercise 5, page 13). Show that $s = \gcd(n, m)$. Conclude that there are x, $y \in \mathbb{Z}$ such that $\gcd(n, m) = nx + my$.

10. **Least Common Multiple.** Let $G = \mathbb{Z}$ and $n, m \in \mathbb{Z}$. We know that $n\mathbb{Z} \cap m\mathbb{Z} \leq \mathbb{Z}$. Conclude that $n\mathbb{Z} + m\mathbb{Z} = r\mathbb{Z}$ for some $r \in \mathbb{N}$. Show that $r = \operatorname{lcm}(n, m)$.

11. Let $H \leq G$, $g \in G$ and n and m two integers. Show that if g^n, $g^m \in H$, then $g^{\gcd(n,m)} \in H$. (Hint: See Exercise 9). In particular if $g^n = g^m = 1$, then $g^{\gcd(n,m)} = 1$.

12. Show that subgroups of a cyclic group are cyclic.

13. Show that every ascending chain of subgroups of G is stationary if and only if every subgroup of G is finitely generated.

2.3 Cosets and Coset Spaces

Let G be a group and X and Y be two subsets of G. Let $g \in G$. We define the following sets:

$$gX = \{gx : x \in X\}$$
$$Xg = \{xg : x \in X\}$$
$$XY = \{xy : x \in X,\, y \in Y\}$$
$$X^{-1} = \{x^{-1} : x \in X\}$$

The meaning of the terms XYZ, $g^{-1}Xg$, $gXhY$, $X^{-1}X$ should be clear. Note that $X^{-1}X = \{y^{-1}x : x,\, y \in X\}$ is not necessarily the set $\{1\}$.

If $H \leq G$ and $g \in G$, the set gH is called a **left coset** of H in G, the set Hg is called the **right coset** of H in G.

Lemma 2.3.1 *For $H \leq G$ and x, $y \in G$, either $xH = yH$ or $xH \cap yH = \emptyset$. Furthermore the first case happens if and only if $y^{-1}x \in H$ if and only if $x^{-1}y \in H$ if and only if $x \in yH$ if and only if $y \in xH$.*

Proof: Although a special case of Exercise 17, page 28, (take $K = 1$) we prove the first statement anyway. Assume $xH \cap yH \neq \emptyset$. Let $a \in xH \cap yH$. Then $a = xh = yk$ for some h, $k \in H$. Now $xH = xhh^{-1}H = ykh^{-1}H \subseteq yH$. Similarly $yH \subseteq xH$. Thus $xH = yH$. The second part is now obvious. □

If $H \leq G$ the set $\{xH : x \in G\}$ is called the **left coset space** of H in G. The **right coset space** is defined similarly.

Lemma 2.3.2 *The left coset space is a partition of G.*

Proof: Since for any $x \in G$, $x = x1 \in xH$, the sets xH for $x \in G$ cover G. They are also disjoint by the previous lemma. □

Corollary 2.3.3 *If G is finite and $H \leq G$ then $|H|$ divides $|G|$.*

Proof: The map $x \mapsto ba^{-1}x$ is a one to one correspondence from aH onto bH. Thus all the cosets of H have the same number of elements. The corollary now follows from the previous lemma. □

If a group G is finite, its cardinality is called the **order** of G

Corollary 2.3.4 *A group of prime order is cyclic, in fact it is generated by any of its nontrivial elements. In particular such a group is abelian.*

Proof: Let G be a group of prime order. Let $g \in G^{\#}$. Then $1 < \langle g \rangle \leq G$ and by Corollary 2.3.3, $1 \neq |\langle g \rangle|$ divides $|G|$. Hence $|\langle g \rangle| = |G|$ and $\langle g \rangle = G$. □

Note that the left coset space and the right coset space in general are not equal. However there is a natural bijection between them (Exercise 11, page 33). We denote by G/H any one of the coset spaces. We will say which coset space we intend if that is relevant. In any event, we can speak of $|G/H| \in \mathbb{N} \cup \{\infty\}$ without problems[1]. One sometimes writes $[G : H]$ instead of $|G/H|$. This number is called the **index** of H in G.

Note that the sets G/H and G do not intersect, even if $H = 1$, because the elements of G/H are subsets of G, and not elements of G.

Corollary 2.3.5 *If G is finite and $H \leq G$ then $|G/H| = |G|/|H|$.*

Exercises.

1. Let $H \leq G$ and $g \in G$. Show that $g^{-1}Hg \leq G$.
2. Show that $[\mathbb{Z} : n\mathbb{Z}] = n$.
3. Show that $[\mathbb{Q} : \mathbb{Z}] = \infty$.
4. Show that $[\mathbb{R} : \mathbb{Q}] = \infty$.
5. Show that $[\mathbb{R}^* : \mathbb{Q}^*] = \infty$.
6. Show that $[\mathbb{R}^* : \mathbb{R}^{>0}] = 2$.
7. Show that if $k \leq n$ then $[\mathrm{Sym}(n) : \mathrm{Sym}(k)] = (k+1)(k+2)\ldots n$.
8. Find $[\mathbb{Q}[\sqrt{2}]^* : \mathbb{Q}^*]$.
9. Is the subgroup of $\mathbb{Q}^*$ generated by $2/5$ and $4/7$ cyclic?
10. Show the subgroup of $\mathbb{R}^*$ generated by $\sqrt{2}$ and $\sqrt{2}$ is isomorphic to the subgroup of $\mathbb{R}$ generated by $\sqrt{2}$ and $\sqrt{3}$.

[1] To be precise, $|G/H|$ is a cardinal number. But in group theory, most often what more is important is whether or not $|G/H|$ is finite.

11. Let $H \leq G$. Show that there is a natural bijection between the left coset space and the right coset space.

    Proof: Consider the map $xH \mapsto Hx^{-1}$. This is well defined and one to one because $xH = yH$ if and only if $y^{-1}x \in H$ if and only if $y^{-1} \in Hx^{-1}$ if and only if $Hy^{-1} = Hx^{-1}$. It is also onto.

12. Write the left and the right coset spaces of Sym(3) in Sym(4).

13. Show that $\mathrm{Sym}(n) = \sqcup_{i=1}^{n-1}(i,n)\,\mathrm{Sym}(n-1)$.

14. Let $H \leq G$. Let $N_G(H) := \{g \in G : gH = Hg\}$. Show that $H \leq N_G(H) \leq G$. The group $N_G(H)$ is called the **normalizer** of H in G.

15. Let H, K be two subgroups of G. Assume that for all $k \in K$, $kHk^{-1} \subseteq H$. Show that $K \subseteq N_G(H)$.

16. Let H and K be two subgroups of a group G. Show that for x and y in G, $xH \cap yK$ either is empty or a coset of $H \cap K$.

    Proof: Assume $xH \cap yK \neq \emptyset$. Let $z \in xH \cap yK$. Then $xH = zH$ and $yK = zK$. So $xH \cap yK = zH \cap zK = z(H \cap K)$. □

17. Let G be any group generated by a subset $X \subseteq G$ and let $k \in \mathbb{N}$. Show that the set

$$\{x_1^{a_1} \dots x_n^{a_n} : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z},\, \sum_{i=1}^{n} a_i \equiv 0 \bmod k\}$$

    is a subgroup of G of index at most k.

18. * Does $\mathrm{Sym}(\mathbb{N})$ has a proper subgroup of finite index?

19. * Show that $\mathrm{Sym}(\mathbb{N})/\mathrm{Sym}^{<\omega}(\mathbb{N})$ is uncountable.

20. Let G be a group. For $a \in G$, let $a^G := \{g^{-1}ag : g \in G\}$ (the **conjugacy class** of a in G.

    a) For a, $b \in G$, show that either $a^G \cap b^G = \emptyset$ or $a^G = b^G$.

    b) Show that the map $gC_G(a) \longrightarrow gag^{-1}$ defines a bijection between $G/C_G(a)$ and a^G. (See Exercise 2, page 27).

    Proof: By question 11, we may assume that $G/C_G(a)$ stands for the right coset space $\{C_G(a)g : g \in G\}$. It is easy to check that the map $C_G(a)g \mapsto a^g$ is a well-defined bijection between $G/C_G(a)$ and a^G. □

21. a) How many conjugacy classes are there in Sym(5)?

    b). Find the sizes of the centralizers of the elements of Sym(5).

22. Proceeding as above show that there is a bijection between the right coset space $G/N_G(H)$ and the set $\{g^{-1}Hg : g \in G\}$.

23. a) Show that the intersection of two subgroups of finite index is finite.

b) If $C \leq B \leq A$ then $[A : C] = [A : B][B : C]$.

c) If $[G : H] = n$ and $[G : K] = m$, what can you say about $[G : H \cap K]$?

Proof: (a) Let H and K be two subgroups of index n and m of a group G. Then for any $x \in G$, $x(H \cap K) = xH \cap xK$ and there are at most n choices for xH and m choices for xK. Hence $[G : H \cap K] \leq nm$.

(b) If $B = \sqcup_{i=1}^{r} b_i C$ and $A = \sqcup_{j=1}^{s} a_j B$, then $A = \sqcup_{i=1}^{r} \sqcup_{j=1}^{s} b_i a_j C$.

(c) Thus $[G : K \cap H] = [G : H][H : H \cap K] = [G : K][K : H \cap K]$. It follows that n and m both divide $[G : K \cap H]$, hence $\text{lcm}(n, m)$ divides $[G : K \cap H]$. Further in part (a) we have seen that $[G : K \cap H] \leq mn$. □

2.4 Order of an Element

Let $g \in G$. We let $o(g)$ to be the smallest positive natural number n such that $g^n = 1$ if there is such a number. Otherwise we let $o(g) = \infty$. The number $o(g)$ is called the **order** of g.

Lemma 2.4.1 *If g is in a group G and $g^n = 1$ then $o(g)$ divides n.*

Proof: Divide n by $o(g)$: $n = o(g)q + r$ for some $q \in \mathbb{Z}$ and $r = 0, 1, \ldots, o(g) - 1$. We have $1 = g^n = g^{o(g)q+r} = g^{o(g)q} g^r = (g^{o(g)})^q g^r = 1^q g^r = g^r$. Thus $g^r = 1$. Since $0 \leq r < o(g)$, from the definition of $o(g)$ we get $r = 0$. Thus $o(g)$ divides n. □

Lemma 2.4.2 *If g is in a group G, then $|\langle g \rangle| = o(g)$.*

Proof: Left as an exercise. □

Corollary 2.4.3 *If G is finite and $g \in G$ then $o(g)$ divides $|G|$.*

Lemma 2.4.4 *Let $H \leq G$, $g \in G$ and n and m two integers.*

a) If g^n, $g^m \in H$, then $g^{\gcd(n,m)} \in H$.

b) In particular if n and m are prime to each other then $g \in H$.

c) In particular if n and m are prime to each other and $g^n = g^m = 1$ then $g = 1$.

Proof: Everything follows from part (a) that we now prove: Let $x, y \in \mathbb{Z}$ be such that $xn + ym = \gcd(n, m)$ (Exercise 9, page 31). Then $g^{\gcd(n.m)} = g^{xn+ym} = (g^n)^x (g^m)^y \in H$. □

Exercises.

1. What is the order of $(12)(345)(6789) \in \mathrm{Sym}(9)$?
2. Find all elements of order 5, 6 and 7 of $\mathrm{Sym}(5)$.
3. Find all elements of finite order of $\mathbb{R}^*$.
4. Let $g \in G$ have finite order n. Let $m \in \mathbb{N}$. What is the order of g^m?
5. Let g, $h \in G$ be such that $g^n = h$ and $o(h) = m$. What can you say about the order of g?
6. Let $g \in G$ have order n. Let d divide n and $q = n/d$. Show that g^q has order d and that g^d has order q.
7. Does the set of elements of finite order of a group form a subgroup?
8. Show that if G is a finite group and has an element of order n, then n divides $|G|$. Is the converse true? I.e. if G is finite and divisible by n, is it true that G has an element of order n?

Chapter 3

Fundamental Concepts

3.1 Morphisms

Let G and H be two groups. A map $\phi : G \longrightarrow H$ is called a **homomorphism of groups** if $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. If $G = H$, we say that ϕ is an **endomorphism**. A homomorphism which is also a bijection, is called an **isomorphism**. If there is an isomorphism $\phi : G \longrightarrow H$, then we say that G and H are **isomorphic**. An isomorphism from a group onto itself is called an **automorphism**.

The set of homomorphisms from a group G into a group H is denoted by $\mathrm{Hom}(G, H)$. The set of endomorphisms and automorphisms of a group is denoted by $\mathrm{End}(G)$ and $\mathrm{Aut}(G)$ respectively.

Lemma 3.1.1 *If $\phi : G \longrightarrow H$ and $\psi : H \longrightarrow K$ are group homomorphisms, then the map $\psi \circ \phi : G \longrightarrow K$ is a group homomorphism.*

Proof: Trivial. □

Lemma 3.1.2 *If G is a group then $\mathrm{Aut}(G)$ is also a group under composition.*

Proof: By Lemma 3.1.1, $\mathrm{Aut}(G)$ is closed under composition. Clearly $\mathrm{Id}_G \in \mathrm{Aut}(G)$. It remains to show that if $\phi \in \mathrm{Aut}(G)$, then $\phi^{-1} \in \mathrm{Aut}(G)$. We leave this as an exercise. □

Lemma 3.1.3 *If G is any group and A an abelian group then $\mathrm{Hom}(G, A)$ is also a group under the multiplication (For ϕ, $\psi \in \mathrm{Hom}(G, A)$ and $g \in G$, $(\phi\psi)(g) = \phi(g)\psi(g)$).*

Proof: For ϕ, $\psi \in \mathrm{Hom}(G, A)$, the map $\phi\psi : G \longrightarrow A$ is defined by $(\phi\psi)(g) = \phi(g)\psi(g)$ for all $g \in G$. It is a matter of triviality (using the commutativity of A) to check that $\phi\psi$ is a homomorphism of groups, i.e. that $\phi\psi \in \mathrm{Hom}(G, A)$.

The map $1 : G \longrightarrow A$ defined by $1(g) = g$ for all $g \in G$ is of course in $\mathrm{Hom}(G, A)$. It is easy to check that the homomorphism 1 is the identity element of $\mathrm{Hom}(G, A)$.

If $\phi \in \mathrm{Hom}(G, A)$ define ϕ^{-1} by $\phi^{-1}(g) = \phi(g)^{-1}$. It is a matter of triviality (using the commutativity of A) to check that ϕ^{-1} is a homomorphism of groups, i.e. that $\phi^{-1} \in \mathrm{Hom}(G, A)$.

These prove the lemma. □

Examples.

1. For $n \in \mathbb{Z}$, the map $x \mapsto nx$is an endomorphism of $\mathbb{Z}$. In general if G is an abelian group, for each $n \in \mathbb{Z}$, the map $g \mapsto g^n$ is an endomorphism of G.

2. Let G be a group and $g \in G$. Define $\mathrm{Inn}_g : G \longrightarrow G$ via $\mathrm{Inn}_g(x) = gxg^{-1}$. Then $\mathrm{Inn}_g \in \mathrm{Aut}(G)$.

3. For $i \in I$, the map $\mathrm{pr}_i : \prod_I G_i \longrightarrow G_i$ given by $\mathrm{pr}_i((g_i)_{i\in I}) = g_i$ is a surjective homomorphism of groups. It is called the i-th **projection** map.

Lemma 3.1.4 *Let $\phi : G \longrightarrow H$ be a* **homomorphism of groups**. *Then*
i. $\phi(1_G) = 1_H$.
ii. $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.
iii. $\phi(g^n) = \phi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

Proof: i. $\phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G)$, so $\phi(1_G) = 1_H$.
ii. $1 = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, so $\phi(g^{-1}) = \phi(g)^{-1}$.
iii. Clear. □

Lemma 3.1.5 *Let $\phi : G \longrightarrow H$ be a group homomorphism. Then*
i.For every $K \leq G$, $\phi(K) \leq H$. In particular $\phi(G) \leq H$.
i.For every $K \leq H$, $\phi^{-1}(K) \leq G$. In particular $\mathrm{Ker}(\phi) := \phi^{-1}(1_H) \leq G$.

Proof: Easy. □

Let ϕ be a group homomorphism from G into H. We define the **kernel** of ϕ to be

$$\mathrm{Ker}(\phi) := \{g \in G : \phi(g) = 1\} = \phi^{-1}(1).$$

By Lemma 3.1.5.ii, $\mathrm{Ker}(\phi) \leq G$.

The following result is used very often.

Lemma 3.1.6 *A group homomorphism $\phi : G \longrightarrow H$ is one to one if and only if* $\mathrm{Ker}(\phi) = 1\}$.

Proof: Assume ϕ is one to one. Let $g \in \mathrm{Ker}(\phi)$. Then $\phi(g) = 1 = \phi(1)$. Since ϕ is one to one, we get $g = 1$.

Conversely, assume $\mathrm{Ker}(\phi) = 1$. Let g_1, $g_2 \in G$ be such that $\phi(g_1) = \phi(g_2)$. Then by Lemma 3.1.4, $\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = 1$. Hence $g_1 g_2^{-1} \in \mathrm{Ker}(\phi) = 1$ and so $g_1 = g_2$. □

Exercises.

1. Let $H \leq G$ and $g \in G$. Show that gHg^{-1} is a subgroup of G isomorphic to H.

2. Find a group G that has a proper subgroup isomorphic to itself.

3. Find the kernel and the image of the group homomorphism, $\phi : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ given by, $\phi(x, y) = x + y$.

4. Let $\phi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ given by, $\phi(x, y) = (x + y, x - y)$. Find ϕ^n for $n \in \mathbb{N}$. Show that each ϕ^n is an automorphism.

5. Show that the subgroups generated by $\sqrt{2}$ and $\sqrt{3}$ in $\mathbb{R}^+$ are isomorphic.

6. Show that the subgroup generated by $\sqrt{2}$ and $\sqrt{3}$ in R* is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. (4 pts.)

7. Show that the maps $\phi_n(x) = nx$ $(n \in \mathbb{Z})$ are the only endomorphisms of $\mathbb{Z}$. Show that $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}, \phi_{-1}\}$ and that $\mathrm{Aut}(\mathbb{Z})$ is isomorphic to the subgroup $\{1, -1\}$ of $\mathbb{R}^*$.

8. Show that the maps $\phi_q(x) = qx$ $(q \in \mathbb{Q})$ are the only endomorphisms of $\mathbb{Q}$. Show that $\mathrm{Aut}(\mathbb{Q}) = \{\phi_q : q \neq 0\}$ and that $\mathrm{Aut}(\mathbb{Q}) \simeq \mathbb{Q}^*$.

9. Let A be an abelian group written additively and let r an integer.

   a) Let $A[r] = \{a \in A : ra = 1\}$. Show that $A[r] \leq A$.

   b) Let $rA = \{ra : a \in A\}$. Show that $rA \leq A$. 4.

   c) Assume A has exponent nm where $(n, m) = 1$. Show that $nA = A[m]$, $mA = A[n]$ and $A \simeq A[n] \oplus A[m]$.

10. Let G be a group and $g \in G$. Define $\mathrm{Inn}_g : G \longrightarrow G$ via $\mathrm{Inn}_g(x) = gxg^{-1}$. Show that the map $g \mapsto Inn_g$ is a homomorphism from the group G into $\mathrm{Aut}(G)$. Thus $\mathrm{Inn}(G) := \{\mathrm{Inn}_g : g \in G\}$ is a subgroup of G. Show that $\mathrm{Ker}(\mathrm{Inn}) = Z(G)$.

11. Consider the situation of Exercise 16, page 14. Show that f is an isomorphism of groups.

12. Let G be a group. For each n and $\sigma \in \mathrm{Sym}(n)$ show that the map $\tilde{\sigma} : G^n \longrightarrow G^n$ given by $\tilde{\sigma}(g_1, \ldots, g_n) = (g_{\sigma(1)}, \ldots, g_{\sigma(n)})$ is an automorphism of G^n. Show that the map $\tilde{} : \mathrm{Sym}(n) \longrightarrow \mathrm{Aut}(G)$ that sends $\sigma \in \mathrm{Sym}(n)$ to $\tilde{\sigma} \in \mathrm{Aut}(G)$ is a one-to-one group homomorphism.

3.2 Quotient Group

Let G be a group and $H \leq G$. Let us consider the left coset space G/H. For xH, $yH \in G/H$, we may want to define a binary operation on G/H as follows: $(xH)(yH) = (xy)H$ for all xH, $yH \in G/H$. Assuming we can do this, then it is clear that G/H becomes a group under this binary operation. However, this binary operation may not be well defined, because, we may have $xH = x_1H$ and $yH = y_1H$, but $(xy)H \neq (x_1y_1)H$ for some x, x_1, y, $y_1 \in G$, and this will prevent the binary operation on the set G/H to be well-defined.

Lemma 3.2.1 *For $H \leq G$, the following conditions are equivalent:*

i. For all x, x_1, y, $y_1 \in G$, if $xH = x_1H$ and $yH = y_1H$, then $(xy)H = (x_1y_1)H$.

ii. For all $x \in G$, $xH = Hx$.

iii. For all $x \in G$, $xH \subseteq Hx$.

iv. For all $x \in G$, $Hx \subseteq xH$.

v. For all $x \in G$, $x^{-1}Hx = H$.

vi. For all $x \in G$, $x^{-1}Hx \subseteq H$.

Proof: (ii $\Rightarrow$ iii) is clear. Conversely, if $xH \subseteq Hx$ for all $x \in G$, then $x^{-1}H \subseteq Hx^{-1}$ for all $x \in G$, i.e. $Hx \subseteq xH$ for all $x \in G$. This show (ii). Thus (ii) and (iii) are equivalent. By symmetry (ii) and (iv) are equivalent. (ii $\Rightarrow$ v) is clear as well. Certainly (v $\Rightarrow$ vi). Conversely if (vi) holds then $xHx^{-1} \subseteq H$ for all $x \in G$, i.e. $H \subseteq x^{-1}Hx$ for all $x \in G$. Hence (v) holds. Thus, (ii), (iii), (iv), (v) and (vi) are equivalent.

(i $\Rightarrow$ v). Let $y \in G$ and $h \in H$. Take $y = y_1$ and $x = h$ and $x_1 = 1$ in (i). Thus $hyH = yH$, i.e. $y^{-1}hy \in H$. Thus $y^{-1}Hy \subseteq H$ for all $y \in H$.

(ii $\Rightarrow$ i). Let x, x_1, y, $y_1 \in G$ be such that $xH = x_1H$ and $yH = y_1H$. Thus . $xyH = xy_1H = xHy_1 = x_1Hy_1 = x_1y_1H$. □

A subgroup satisfying one of the above conditions is called a **normal** subgroup. If the subgroup H is normal in G, we write $H \lhd G$. Thus when $H \lhd G$, every left coset xH is equal to the right coset Hx. Hence the left coset space of H in G is equal to the right coset space of H in G.

Condition (vi) is most often the easiest to check. Writing H^x for $x^{-1}Hx$, this condition becomes: $H^x \subseteq H$ for all $x \in G$.

Problem 3.2.1 *Is it true that if the left coset space of H in G is equal to the right coset space of H in G then $H \lhd G$?*

One should be aware that if $xH = Hx$ (even for all $x \in G$), does not imply that $xh = hx$ for all $h \in H$. The condition $xH = Hx$ only means that for every $h \in H$, $xh = h_1x$ for some $h_1 \in H$.

It should be clear that when $H \lhd G$ then the left coset space (which is equal to the right coset space) G/H is a group.

For $x \in G$, very often we will write $\overline{x} = xH = yH$. Thus

$$\overline{x}\,\overline{y} = (xH)(yH) = (xy)H = \overline{xy}$$

and so the map - from G into G/H is a group homomorphism. This map is certainly onto. It is called the **canonical homomorphism** or the **canonical surjection** from G onto G/H. Clearly $\mathrm{Ker}(\text{-}) = \{x \in G : \overline{x} = \overline{1}\} = \{x \in G : xH = H\} = \{x \in G : x \in H\} = H$.

Examples.

1. For every group G, the trivial subgroup 1 and G itself are normal subgroups of G.

2. Every subgroup of an abelian group is normal.

3. The intersection of any collection of normal subgroups of a group is normal.

4. The subgroup $Z(G) := C_G(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$ is a normal subgroup of G. It is called the **center** of G. Every subgroup of $Z(G)$ is a normal subgroup of G.

5. $G/G = 1$ and $G \simeq G/1$ via the canonical surjection $g \longrightarrow \overline{g}$.

6. Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. If $n = 0$, then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}$ as above. Assume $n > 0$. Let $m \in \mathbb{Z}$. Divide m by n: $m = nq + r$ for some $q \in \mathbb{Z}$ and $r = 0, 1, \ldots, n-1$. Now we have $m + n\mathbb{Z} = nq + r + n\mathbb{Z} = r + n\mathbb{Z}$. Thus

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

   Writing $\overline{i}$ for $i + n\mathbb{Z}$, we have

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

   For example $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$, $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\mathbb{Z}\}$. In $\mathbb{Z}/6\mathbb{Z}$ we have

$$\overline{4} + \overline{5} = \overline{4+5} = \overline{9} = \overline{3+6} = \overline{3} + \overline{6} = \overline{3} + \overline{0} = \overline{3+0} = \overline{3}$$
$$\overline{4} + \overline{2} = \overline{0}$$

   Note that $\mathbb{Z}/2\mathbb{Z} \simeq \{\overline{0}, \overline{3}\} \leq \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \simeq \{\overline{0}, \overline{2}, \overline{4}\} \leq \mathbb{Z}/6\mathbb{Z}$.

Lemma 3.2.2 *Let $\phi : G \longrightarrow H$ be a group homomorphism. Then*
i. If ϕ is onto then for every $K \lhd G$, $\phi(K) \lhd H$.
ii.For every $K \lhd H$, $\phi^{-1}(K) \lhd G$. In particular $\mathrm{Ker}(\phi) := \phi^{-1}(1_H) \lhd G$.

Proof: Easy and is left as an exercise. □

Exercises.

1. Let G be a group and let $H \lhd G$ be a normal subgroup of G.

   a) Show that $C_G(H) := \{g \in G : gh = hg \text{ for all } h \in H\}$ is a normal subgroup of G.

   b) For $x \in G$, define $B(x) := \{g \in G : g^{-1}x^{-1}gx \in H\}$. Show that $B(x)$ is a subgroup of G that contains H.

2. Let H and K be two normal subgroups of G. Show that if $H \leq K = 1$ then $hk = kh$ for all $h \in H$ and $k \in K$.

3. Let $H \leq G$, show that $\cap_{g\in G} gHg^{-1}$ is a normal subgroup of G contained in H. Show that this subgroup contains all normal subgroup of G contained in H. (See Theorem 3.2.3).

4. Let $H = \{(x, 2x, x) : x \in \mathbb{R}\}$. Then $H \lhd \mathbb{R}^3$. Show that $R^3/H \simeq R^2$.

5. We consider $\mathbb{R}$ as a group under addition. Since $\mathbb{Z} \leq \mathbb{R}$, we can consider the group $G := \mathbb{R}/\mathbb{Z}$.

   a) Show that every element of G can be written as $r + \mathbb{Z}$ for some unique $r \in \mathbb{R}$ with $0 \leq r < 1$.

   b) Show that if $q \in \mathbb{Q}$, then $q + \mathbb{Z}$ is an element of finite order of G.

   c) Find all elements of order 2, 3 and 6 of G.

   d) For a fixed integer $n > 0$, find all elements of order n of G.

6. Show that a subgroup of index 2 is normal. Show that this is false for 3. (Hint: Look at Sym(3)).

7. Let $H \leq G$. Show that $\cap_{x\in G} H^x \lhd G$.

8. Find an example where $K \lhd H \lhd G$ but K is not normal in G.

9. Let A be an abelian group. Let

   $$B := \{a \in A : a \text{ has finite order}\}.$$

   Show that $B \leq A$ and that in the quotient group A/B, the order of every nonidentity element is infinite.

10. Let A be an abelian group. Let $n \in \mathbb{Z}$. Let $B := \{a^n : a \in A\}$. Then B is a subgroup of A. Show that $\exp(A/B)$ divides n.

11. Let n, m, $k \in \mathbb{Z}$. Show that in $\mathbb{Z}/n\mathbb{Z}$, $k\overline{m} = \overline{km}$.

12. A group is called **simple** if it has no nontrivial proper normal subgroup. Let A and B be two simple nonabelian groups. Find all normal subgroups of $A \times B$.

13. Let $G_1, \ldots, G_n$ be nonabelian simple groups. Find all normal subgroups of $G_1 \times \ldots \times G_n$.

14. Let G be a group, H, $K \leq G$. We say that K **normalizes** H if $H^k = H$ all $k \in K$. Suppose K normalizes H. Show that HK is a subgroup of G.

15. Let G be a group, H, $K \leq G$. Suppose that $H^k \subseteq H$ all $k \in K$. Show that K normalizes H.

16. Let G be a group, $H \leq G$. Define $N_G(H) = \{g \in G : H^g = H\}$.

    a) Show that $H \lhd N_G(H) \leq G$.

    b) Show that $N_G(H)$ contains all subgroups of G that normalize H.

We end this section with the following result:

Theorem 3.2.3 (Core) *Let G be a group and $H \leq G$ a subgroup of index n. Then $\mathrm{Core}_G(H) := \bigcap_{g \in G} H^g$ is a normal subgroup G contained in H and it is the largest such subgroup of G (called the* **core** *of H in G). Furthermore $G/\mathrm{Core}_G(H)$ is isomorphic to a subgroup of $\mathrm{Sym}(n)$. In fact, $\mathrm{Core}_G(H)$ is the kernel of the action of G on the coset space G/H.*

Proof: Let G be a group and $H \leq G$ a subgroup of index n. Let $X = G/H$ be the left coset space. For $g \in G$, define $\tilde{g} : G/H \longrightarrow G/H$ by $\tilde{g}(xH) = gxH$ for $x \in G$.

Claim 1. $\tilde{g} \in \mathrm{Sym}(X)$.

Proof: Nothing can be clearer.

Claim 2. $\tilde{} : G \longrightarrow \mathrm{Sym}(X)$ is a homomorphism of groups.

Proof: Nothing can be clearer.

Claim 3. $\mathrm{Ker}(\tilde{})$ is the largest normal subgroup of G contained in H.

Proof: $\mathrm{Ker}(\tilde{})$ is certainly a normal subgroup of G. Also $\mathrm{Ker}(\tilde{}) = \{g \in G : \tilde{g} = \mathrm{Id}\} = \{g \in G : gxH = xH \text{ for all } x \in G\} = \{g \in G : x^{-1}gx \in H \text{ for all } x \in G\} = \{g \in G : g \in xHx^{-1} \text{ for all } x \in G\} = \cap_{x \in G} H^x$. It is now clear that $\mathrm{Ker}(\tilde{})$ is the largest normal subgroup of G contained in H.

Claim 4. $[G : \mathrm{Ker}(\tilde{})]$ divides $n!$.

By above $G/\mathrm{Ker}(\tilde{})$ embeds in $\mathrm{Sym}(G/H) \simeq \mathrm{Sym}(n)$. □

3.3 Subgroups of G/H

Theorem 3.3.1 *Let G be a group and $H \lhd G$.*

a) Let K be such that $H \leq K \leq G$. Then $K/H \leq G/H$.

b) Let K be such that $H \leq K \lhd G$. Then $K/H \lhd G/H$.

c) Any subgroup X of G/H is of the form K/H for some unique subgroup K of G containing H. In fact

$$K = \{g \in G : \overline{g} \in X\}.$$

Thus there is a one to one correspondence between $\{$*Subgroups of* $G/H\}$ *and* $\{$*subgroups of* G *containing* $H\}$.

d) Any normal subgroup X *of* G/H *is of the form* K/H *for some unique normal subgroup* K *of* G *containing* H. *In fact*

$$K = \{g \in G : \overline{g} \in X\}.$$

Thus there is a one to one correspondence between $\{$*Subgroups of* $G/H\}$ *and* $\{$*subgroups of* G *containing* $H\}$.

Proof: Consider the canonical surjection $\phi : G \longrightarrow G/H$and apply lemmas 3.1.5 and 3.2.2 to this map. □

Exercises.

1. Let $H \lhd G$. Let $X \subseteq G$ be such that $G/H = \langle \overline{X} \rangle$. Show that $G = \langle H, X \rangle$.
2. Let G be such that $G/Z(G)$ is cyclic. Show that G is abelian. (Hint: See the exercise above).
3. Find all subgroups of $\mathbb{Z}/n\mathbb{Z}$. (Hint: See Exercise 10, page 28).
4. Let $H \lhd G$, $\overline{G} = G/H$ and $x \in G$. We know that $C_\Gamma(\overline{x}) = C/H$ for some unique subgroup C of G containing H. Define C in terms of x and H.

3.4 Induced Homomorphisms

Theorem 3.4.1 *Let* $\phi : G \longrightarrow H$ *be a group homomorphism. Let* $K \lhd G$ *be such that* $K \leq \mathrm{Ker}(\phi)$. *Then the induced map* $\overline{\phi} : G/K \longrightarrow H$ *given by* $\overline{\phi}(\overline{g}) = \phi(g)$ *is well-defined and is a homomorphism whose kernel is* $\mathrm{Ker}(\phi)/K$. *In particular (taking* $K = \mathrm{Ker}(\phi)$*) the map* $\overline{\phi} : G/\mathrm{Ker}(\phi) \longrightarrow H$ *given by* $\overline{\phi}(\overline{g}) = \phi(g)$ *is a one to one homomorphism. If* ϕ *is onto then* $G/\mathrm{Ker}(\phi) \simeq H$.

Proof: Assume $\overline{g} = \overline{g_1}$. Then $g_1^{-1}g \in K \leq \mathrm{Ker}(\phi)$, so $\phi(g_1)^{-1}\phi(g) = \phi(g_1^{-1}g) = 1$ and $\phi(g) = \phi(g_1)^{-1}$. Thus the map $\overline{\phi}$ is well defined.

We have $\overline{g} \in \mathrm{Ker}(\overline{\phi})$ iff $\overline{p}hi(\overline{g}) = 1$ iff $\phi(g) = 1$ iff $g \in \mathrm{Ker}(\phi)$ iff $\overline{g} \in \mathrm{Ker}(\phi)/K$.

The second and third parts are direct consequences of these. □

The homomorphism $\overline{\phi} : G/K \longrightarrow H$ is said to be **induced** from the homomorphism $\phi : G \longrightarrow H$.

Exercises.

1. Let $\phi : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ be given by $\phi(x, y, z) = (2x - 3y, 4x - 3z)$.
   a. Show that ϕ is a homomorphism of groups.
   b. Is ϕ onto?
   c. Show that $\mathrm{Ker}(\phi) = \{(3a, 2a, 4a) : a \in \mathbb{Z}\}$.
   d. Show that $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/\mathrm{Ker}(\phi) \simeq \mathbb{Z} \times \mathbb{Z}$.

3.5 Fundamental Theorem

Theorem 3.5.1 *Let G be a group, $K \leq G$, $H \leq G$. Suppose K normalizes H, i.e. suppose that $K \leq N_G(H)$. Then*
i. $\langle H, K\rangle = HK = KH$.
ii. $H \lhd HK$ and $K \cap H \lhd K$.
iii. $HK/H \simeq K/(K \cap H)$.

Proof: i. Certainly HK is a subset of $\langle H, K\rangle$ and it contains H and K. So it is enough to show that $HK \leq G$. Let $h, h_1 \in H$ and $k, k_1 \in H$. Then $(hk)(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1} = hkk_1^{-1}h_1^{-1}k_1k^{-1}kk_1^{-1} = hh_1^{-k_1k^{-1}}kk_1^{-1} \in HK$. Thus $HK \leq G$.

ii. Trivial.

iii. Look at the natural map $K \longrightarrow HK/H$ given by $k \mapsto \overline{k}$. This map is onto and its kernel is $\{k \in K : \overline{k} = \overline{1}\} = \{k \in K : k \in H\} = K \cap H$. By Theorem 3.4.1, $HK/H \simeq K/(K \cap H)$. □

Exercises.

1. Let G be a group. The set $\delta(G \times G) := \{(g, g) : g \in G\}$ is a subgroup of $G \times G$. Show that it is a normal subgroup of $G \times G$ if and only if G is abelian.

2. Let G be a group. Let $H \lhd G$. Show that $H \times H \lhd G \times G$. When is $\delta(H \times H) := \{(h, h) : h \in H\}$ is a normal subgroup of $G \times G$?

3. Show that $(\mathbb{Q} \times \mathbb{Q})/\delta(\mathbb{Z} \times \mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}$ where $\delta(\mathbb{Z} \times \mathbb{Z}) = \{(z, z) : z \in Z\}$.

4. a) Find all automorphisms of order 2 of $\mathbb{Z}/p\mathbb{Z}$ (p a prime).

   b) For what prime numbers p, does $\mathbb{Z}/p\mathbb{Z}$ has an automorphism of order 3?

   c) For what prime numbers p, does $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has an automorphism of order 3?

5. Let H and K be two normal subgroups of a group G such that $H \cap K = 1$. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

6. Let G, H be two groups, $\phi : G \longrightarrow H$ a homomorphism of groups and $g \in G$ an element of finite order. Show that $o(\phi(g))$ divides $o(g)$.

7. Let G be a group and define $Z_0(G) = 1$ and $Z_{n+1}(G) = \{z \in G : forall g \in G, gzg^{-1}z^{-1} \in Z_n(G)\}$. Show that $Z_n(G) \lhd G$ for all n.

8. A subgroup H of a group G is called **characteristic** if $\phi(H) = H$ for all $\phi \in \mathrm{Aut}(G)$.

   a. Show that a characteristic subgroup is a normal subgroup.

   b. Show that a subgroup $H \leq G$ is characteristic if $\phi(H) \subseteq H$ for all $\phi \in Aut(G)$.

c. Show that for all n, $Z_n(G)$ (see Exercise 7, page 45) is a characteristic subgroup of G.

d. Let $X \subseteq G$ be such that $\phi(X) \subseteq X$ for all $\phi \in \mathrm{Aut}(G)$. Show that $\langle X \rangle$ is a characteristic subgroup of G.

e. Conclude that for any $n \in \mathbb{Z}$ the subgroup generated by $\{g^n : g \in G\}$ is characteristic.

f. Conclude that the subgroup generated by $\{g^{-1}h^{-1}gh : g, h \in G\}$ is characteristic.

9. Let $(G_i)_{i \in I}$ be a family of groups. Let $J \subseteq I$. Show that $\{(g_i)_{i \in I} : g_j = 1 \text{ for all } j \in J\} \lhd \prod_{i \in I} G_i$.

10. Let $H \leq G$. Recall that the normalizer of H in G is the subgroup $N_G(H) = \{g \in G : gH = Hg\}$. Show that $H \lhd N_G(H)$ and that $N_G(H)$ is the largest subgroup of G that normalizes H, i.e. show that if $H \lhd K \leq G$ then $K \leq N_G(H)$.

11. a) Is there an element of infinite order in $\mathbb{Q}/\mathbb{Z}$?

    b) Is there an element of finite order in $\mathbb{R}/\mathbb{Q}$?

12. Let G be a group and let X be a subset of G satisfying $g^{-1}Xg \subseteq X$. Show that $\langle X \rangle \lhd G$.

13. Let G be any group generated by a subset $X \subseteq G$. Show that the set

$$\{x_1^{a_1} \dots x_n^{a_n} : n \in \mathbb{N},\, x_i \in X,\, a_i \in \mathbb{Z},\, \sum_{i=1}^{n} a_i \text{ is even}\}$$

    is normal subgroup of G of index at most n.

14. Let X be a set. Show that $\mathrm{Sym}^{<\omega}(X) \lhd \mathrm{Sym}(\omega)$.

15. Let X be a set and κ a cardinal number. Show that $\mathrm{Sym}^{<\kappa}(X) \lhd \mathrm{Sym}(\omega)$.

16. Suppose every subgroup of a group is normal. Is the group necessarily abelian?

17. Let $H \leq G$. Let G/H denote the left coset space. For $g \in G$ and $xH \in G/H$, let $g^*(xH) = gxH$.

    a) Show that $g^* \in \mathrm{Sym}(G/H)$.

    b) Show that the map $g \mapsto g^*$ is a homomorphism from G into $\mathrm{Sym}(G/H)$.

    c) What is the kernel of the homomorphism $*$?

    d. Assuming that $[G : H] = n < \infty$, show that $\cap_{g \in G} gHg^{-1}$ is a normal subgroup of G contained in H and that its index divides n!

and

Chapter 4

Cyclic Groups

In this section we will study cyclic groups that have been already partially studied.

4.1 Classification

Theorem 4.1.1 *A cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. In particular any infinite cyclic group is isomorphic to $\mathbb{Z}^+$ and any finite cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some natural number $n > 0$.*

Proof: Let G be a cyclic group. Let $g \in G$ be a generator of G. Consider the map $\phi : \mathbb{Z} \longrightarrow G$ given by $\phi(n) = g^n$. Clearly ϕ is a homomorphism (Lemma 1.1.4) and is onto. By Lemma 2.1.2, $\text{Ker}(\phi) = n\mathbb{Z}$ for some unique $n \in \mathbb{N}$. By Theorem 3.4.1, the map $\overline{\phi} : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ given by $\overline{\phi}(\overline{n}) = g^n$ is well-defined and is an isomorphism. □

Thus, to study cyclic groups, we only need to study the groups $\mathbb{Z}/n\mathbb{Z}$.
Note that if $n = 0$, then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}$ and if $n = 1$, then $\mathbb{Z}/n\mathbb{Z} \simeq \{0\}$

4.2 Subgroups and Quotients

We will find all subgroup of $\mathbb{Z}/n\mathbb{Z}$.

Lemma 4.2.1 *All subgroups of $\mathbb{Z}/n\mathbb{Z}$ are cyclic. If $A \leq \mathbb{Z}/n\mathbb{Z}$, then $A = \langle\overline{m}\rangle = m\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{m}\mathbb{Z}$, for natural number $m \in [1, n]$ that divides n.*

Proof: First note that if m divides n, then $n\mathbb{Z} \leq m\mathbb{Z} \leq \mathbb{Z}$, so that $m\mathbb{Z}/n\mathbb{Z}$ makes sense, and it is a subgroup of $\mathbb{Z}/n\mathbb{Z}$; also, $\langle\overline{m}\rangle = \mathbb{Z}\overline{m} = \{k\overline{m} : k \in \mathbb{Z}\} = \{\overline{km} : k \in \mathbb{Z}\} = \{\overline{x} : \overline{x} \in m\mathbb{Z}\} = m\mathbb{Z}/n\mathbb{Z}$.

Let $H \leq \mathbb{Z}/n\mathbb{Z}$. By Theorem 3.3.1, $H = K/n\mathbb{Z}$ for some unique subgroup K such that $n\mathbb{Z} \leq K \leq \mathbb{Z}$. By Lemma 2.1.2, $K = m\mathbb{Z}$ for some $m \in \mathbb{N}$. Since

$n \in n\mathbb{Z} \leq K = m\mathbb{Z}$, m divides n. Thus $H = m\mathbb{Z}/n\mathbb{Z}$ for some natural number that divides n.

Consider the map $\phi : \mathbb{Z} \longrightarrow m\mathbb{Z}/n\mathbb{Z}$ given by $\phi(x) = \overline{mx}$. This is a surjective homomorphism. Its kernel is $\{x \in \mathbb{Z} : mx \in n\mathbb{Z}\} = \frac{n}{m}\mathbb{Z}$. By Theorem 3.4.1, $m\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{m}\mathbb{Z}$. □

Exercises.

1. Let n and k be positive natural numbers. Find $m \in \mathbb{N}$ such that $m|n$ and $\{m\overline{x} : \overline{x} \in \mathbb{Z}/n\mathbb{Z}\} = k\mathbb{Z}/n\mathbb{Z}$.

2. Let n and k be positive natural numbers. Find $m \in \mathbb{N}$ such that $m|n$ and $\{\overline{x} \in \mathbb{Z}/n\mathbb{Z} : m\overline{x} = \overline{0}\} = k\mathbb{Z}/n\mathbb{Z}$.

4.3 Morphisms

It is clear that a homomorphism ϕ from the cyclic $\mathbb{Z}/n\mathbb{Z}$ into a (multiplicative) group G is given just by the image of a generator of $\mathbb{Z}/n\mathbb{Z}$, say of $\overline{1}$. In other words, if we know $\phi(\overline{1})$, then we know ϕ: $\phi(\overline{k}) = \phi(\overline{1}+\ldots+\overline{1}) = \phi(\overline{1})\ldots\phi(\overline{1})) = \phi(\overline{1})^k$. But we do not have the right to choose the element $\phi(\overline{1})$ of G arbitrarily, in other words, not all choices for the image of $\overline{1}$ give rise to a homomorphism; in fact this element $\phi(\overline{1})$ of G must satisfy the following equality: $1 = \phi(\overline{0}) = \phi(\overline{n}) = \phi(\overline{1})^n$. Thus the order $o(\phi(\overline{1}))$ must divide n. It so happens that this condition is enough.

Lemma 4.3.1 *Let G be a group. The map* $\mathrm{val}_1 : \mathrm{End}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \{g \in G : g^n = 1\}$ *given by* $\mathrm{val}_1(\phi) = \phi(\overline{1})$ *is a bijection. In particular there is one to one correspondence between* $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z})$ *and G.*

Proof: It remains to prove that val_1 is onto. Let $g \in G$ be an element such that $g^n = 1$. Define $\phi : \mathbb{Z} \longrightarrow G$ via $\phi(k) = g^k$. This is clearly a homomorphism. Since $n\mathbb{Z} \longrightarrow \mathrm{Ker}(\phi)$, by Theorem 3.4.1, the map $\overline{\phi} : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ given by $\overline{p}hi(\overline{k}) = \phi(k) = g^k$. is well-defined and is a homomorphism of groups. We have $\mathrm{val}_1(\overline{\phi}) = \overline{\phi}(\overline{1}) = \phi(1) = g$. □

If G is an abelian group, we know that $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)$ is a group under the multiplication of homomorphisms (Lemma 3.1.3).

Lemma 4.3.2 *Let G be an abelian group. Then* $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) \simeq G_n$ *where G_n is the subgroup $\{g \in G : g^n = 1\}$ of G.*

Exercises.

1. Let n and m be two integers > 0. Show that $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq m'\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$ where $m' = m/d$ and $d = \gcd(m, n)$.

4.4 Decomposition

Proposition 4.4.1 *If n and m are natural numbers coprime to each other, then $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.*

Proof: Consider the map $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ given by $\phi(x) = (\overline{x}, \tilde{x})$ where $\overline{x}$ and $\tilde{x}$ are the images of x in $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ respectively. ϕ is a homomorphism of groups.

We first show that ϕ is onto. Let $(\overline{a}, \tilde{b}) \in \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ be any element. Since n and m are prime to each other, there are x and y in $\mathbb{Z}$ such that $xn + ym = 1$ (Exercise 9, page 31). Then for $\phi(xn) = (\overline{xn}, \tilde{xn}) = (\overline{0}, \widetilde{xn}) = (\overline{0}, \widetilde{xn} + \tilde{0}) = (\overline{0}, \widetilde{xn} + \widetilde{ym}) = (\overline{0}, \widetilde{xn + ym}) = (\overline{0}, \tilde{1})$. Similarly $\phi(ym) = (\overline{1}, \tilde{0})$. Hence $\phi(bxn + aym) = (\overline{a}, \tilde{b})$.

Thus $\mathbb{Z}/\operatorname{Ker}(\phi) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. We now compute $\operatorname{Ker}(\phi)$: $\operatorname{Ker}(\phi) = \{x \in \mathbb{Z} : \overline{x} = \overline{0} \text{ and } \tilde{x} = \tilde{0}\} = \{x \in \mathbb{Z} : n \text{ and } m \text{ divide } x\} = \{x \in \mathbb{Z} : nm \text{ divide } x\} = nm\mathbb{Z}$. Thus by Theorem 3.4.1, $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

We can have a sharpening of this result:

Proposition 4.4.2 *If n and m are natural numbers coprime to each other, then $\mathbb{Z}/nm\mathbb{Z} = m\mathbb{Z}/nm\mathbb{Z} \oplus n\mathbb{Z}/nm\mathbb{Z}$.*

Proof: Note first that $m(\mathbb{Z}/nm\mathbb{Z})$ and $n(\mathbb{Z}/nm\mathbb{Z})$ are subgroups of $\mathbb{Z}/nm\mathbb{Z}$.

Since n and m are prime to each other, there are a and b in $\mathbb{Z}$ such that $an + bm = 1$. Thus for every $x \in \mathbb{Z}$, $\overline{x} = \overline{(an + bm)x} = m\overline{bx} + n\overline{ax} \in m(\mathbb{Z}/nm\mathbb{Z}) + n(\mathbb{Z}/nm\mathbb{Z})$.

Since $nm\mathbb{Z} \leq m\mathbb{Z}$, we have $m(\mathbb{Z}/nm\mathbb{Z}) = m\mathbb{Z}/nm\mathbb{Z}$. Similarly $n(\mathbb{Z}/nm\mathbb{Z}) = n\mathbb{Z}/nm\mathbb{Z}$. It follows that $m(\mathbb{Z}/nm\mathbb{Z}) \cap n(\mathbb{Z}/nm\mathbb{Z}) = \{\overline{0}\}$.

Hence $\mathbb{Z}/nm\mathbb{Z} == m(\mathbb{Z}/nm\mathbb{Z}) \oplus n(\mathbb{Z}/nm\mathbb{Z}) = m\mathbb{Z}/nm\mathbb{Z} \oplus n\mathbb{Z}/nm\mathbb{Z}$. □

One should note that $\mathbb{Z}/m\mathbb{Z} \simeq n\mathbb{Z}/nm\mathbb{Z}$ via $\tilde{x} \mapsto \overline{x}$.

Exercises.

1. Let G and H be two nontrivial groups. Show that $G \times H$ is cyclic if and only if G and H are finite, cyclic and of orders prime to each other.

2. Show that a group of prime order is cyclic.

3. Let p be a prime number and n a natural number. How many elements of order p^i does $\mathbb{Z}/p^n$ have?

4. Let $n \in \mathbb{N} \setminus \{0\}$. Find a finite graph Γ such that $\operatorname{Aut}(\Gamma) = \mathbb{Z}/n\mathbb{Z}$.

Chapter 5

Abelian Groups

5.1 Generalities

The **exponent** of a group G is the smallest positive integer n (if it exists) such that $g^n = 1$ for all $g \in \mathbb{N}$.

Theorem 5.1.1 (Abelian groups of exponent p) *Let p be a prime. An abelian group of exponent p is a vector space over $\mathbb{F}_p$, thus it is isomorphic to a direct sum of $\mathbb{Z}/p\mathbb{Z}$. In particular any two abelian group of exponent p and of the same cardinality are isomorphic.*

A group is called **torsion** if all its elements have finite order.

Theorem 5.1.2 (Torsion Abelian Groups) *Let G be a torsion abelian group. For p a prime, define $G(p) = \{g \in G : g^{p^n} = 1 \text{ for some } n \in \mathbb{N}\}$. Then $G(p)$ is a p-group and $G = \oplus_p G(p)$. (See also Exercise 11).*

Problem 5.1.1 *Classify all abelian groups with a unique maximal subgroup. (Note that given an element $a \in G$ there may be no maximal subgroup containing a). ¶ Show that the ring of endomorphisms of such a group is a local ring (see Chapter 12).*

5.2 Decomposition

5.3 Divisible Abelian Groups

Part II

Basic Ring Theory

Chapter 6

Definition and Examples

A **ring** is a structure of the form $(R, +, \cdot, 0)$ where R is a set, 0 is a constant, $+$ and $\cdot$ are two binary operations on R (called **addition** and **multiplication**) such that

R1. The structure $(R, +, 0)$ is a commutative group.

R2. For all x, y, $z \in R$, $x(y + z) = x(y + z)$ and $(x + y)z = xz + yz$.

Since $0x = (0 + 0)x = 0x + 0x$, by R1, in a ring, we always have $0x = 0$. Similarly $x0 = 0$. Also, since $0 = 0y = (x + (-x))y = xy + (-x)y$, we have $(-x)y = -(xy)$. Similarly $x(-y) = -(xy)$. From now on we let $-xy$ denote any of $(-x)y$, $x(-y)$, $-(xy)$.

If in a ring R,

R3. For all x, y, $z \in R$, $x(yz) = x(yz)$,

then we say that the ring is **associative**.

If in a ring R there is an element 1 such that $1 \neq 0$ and $x1 = 1x = x$ for all $x \in R$, we will say that R is a **ring with identity**, or **with 1**.

If in a ring R, $xy = yx$ for all x, $y \in R$, we will say that R is **commutative**. Otherwise the ring will be called **noncommutative**.

Examples.

1. Let R be any abelian group written additively. Set $xy = 0$ for all x, $y \in R$. Then R is a commutative and associative ring without 1.

2. $\mathbb{Z}$ is a commutative and associative ring together with the usual addition and multiplication. It has an identity.

3. If $r \in \mathbb{R}$, $r\mathbb{Z}$ is a ring. It has identity if and only if $r = 1$ or $r = -1$.

4. Let A be an abelian group (written additively). Then the set $\mathrm{End}(A)$ of endomorphisms of A is an associative ring with identity under addition and composition.

5. If X is a set and R is a ring, the set of functions $\mathrm{Func}(X, R)$ from X into R is a ring with **pointwise** addition and multiplication, i.e. for f, $g \in \mathrm{Func}(X, R)$, define $f + g$ and fg by the rules,

$$(f + g)(x) = f(x) + g(x)$$

and

$$(fg)(x) = f(x)g(x)$$

for all $x \in X$. As with groups, we denote this ring as $\prod_X R$, call it the **direct product** of the rings R, and denote its elements as $(f_x)_{x\in X}$. If all the rings have 1, then the ring $\prod_X R$ has also 1. The commutativity and the associativity of R are reflected on $\prod_X R$. The set

$$\oplus_X R := \{(f_x)_{x\in X} : f_x = 0 \text{ except for finitely many } x \in X\}$$

is called the **direct sum** of the ring R. If X is finite, then clearly $\oplus_X R = \prod_X R$. If R has identity, then $\prod_X R$ has also identity. On the other hand if X is infinite $\prod_X R$ does not have an identity even if R has. If X has n elements, it is customary to denote $\prod_X R$ as R^n.

6. More generally, if for $i \in I$, R_i is a ring, then

$$\prod_{i\in I} R_i := \{(r_i)_i : r_i \in R_i\}$$

and

$$\oplus_{i\in I} R_i := \{(r_i)_i : r_i \in R_i \text{ and } r_i = 0\text{except for finitely many } i \in I\}$$

are rings.

7. Let R be a ring. Define a new multiplication $[x, y]$ by $xy - yx$. Then $(R, +, [\ ,\ ], 0)$ is a ring satisfying $[x, x] = 0$ and $[x, y] = -[y, x]$. If the original ring R is also associative, then $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all x, y, $z \in R$. This is the so-called **Jacobi identity**. A ring that satisfies this kind of weak associativity is called a **Lie ring**.

An element r of a commutative ring R is called a **zero-divisor** if $rs = 0$ for some $s \neq 0$.

An element r of an associative ring R is called **nilpotent** if $r^n = 0$ for some $n \neq \mathbb{N}$.

An element r of a ring R is called **invertible** or a **unit** of R if there is an s such that $rs = sr = 1$. The set of its invertible of a ring R is denoted by R^*. It is easy to show that R^* is a multiplicative group.

If R is a ring, forgetting that R has a multiplication, we may consider R only as a group under addition. We let R^+ denote this group. We call it the **additive group** of R.

Exercises.

1. Let S be a set, $\wp(S)$ be the set of all subsets of S. For $A, B \in \wp P(S)$ define
$$A + B := (A - B) \cup (B - A) \text{ and } A \cdot B := A \cap B.$$
Show that $(\wp P(S), +, \cdot)$ is a commutative ring.

2. Find $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$. Show that $\mathbb{Z}^* \simeq \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Q}^* \simeq \mathbb{Z}/2\mathbb{Z} \oplus (\oplus_{\mathbb{N}}\mathbb{Z})$. Show that $\mathbb{R}^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}^{>0}$.

3. Show that $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a ring. ¶ Find $\mathbb{Z}[\sqrt{2}]^*$. Find its elements of finite order.

4. Show that $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a ring. Find $\mathbb{Q}[\sqrt{2}]^*$.

5. Let R be an associative and commutative ring with identity. On $R \times R$ define the addition componentwise and the multiplication by the rule $(x, y)(z, t) = (xz, xt + yz)$. Show that $R \times R$ is a commutative and associative ring with identity. Find its zero-divisors, its nilpotent elements, its idempotents and its invertible elements.

6. Let $n \in \mathbb{Z}$. Consider the abelian (additive) group $\mathbb{Z}/n\mathbb{Z}$.

   a)For a, b, c, $d \in \mathbb{Z}$, show that if $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$ then $\overline{ac} = \overline{bd}$.

   b) Conclude that $\mathbb{Z}/n\mathbb{Z}$ is a commutative and associative ring with identity with respect to the usual addition, and multiplication defined by $\overline{x}\,\overline{y} = \overline{xy}$.

   c) Find the zero-divisors, the nilpotent elements, the idempotents and the invertible elements of $\mathbb{Z}/24\mathbb{Z}$.

7. Let A be an abelian group (written additively). Show that the set $\mathrm{End}(A)$ of endomorphisms of A is an associative ring with identity under addition and composition. Is it always commutative?

8. Let R be a ring and $x \in \mathbb{R}$. Let $\ell_x : R \longrightarrow R$ be defined by $\ell_x(y) = xy$. Show that ℓ_x is an additive group homomorphism of R^+. What is its kernel?

9. Let R be a commutative and associative ring with identity and without zero-divisors (such a ring is called a **domain**). For x, $y \in R$, define the relation $x|y$ by $y \in xR$. In such is the case, we say that x divides y.

   a) Show that this is a transitive and reflexive relation.

   b) Show that the units of R divide all the elements of R.

   c) Define $x \equiv y$ by $x|y$ and $y|x$. Show that $x \equiv y$ if and only if $x \in yR^*$. Conclude that $\equiv$ is an equivalence relation.

   d) Show that if $x \equiv x_1$, $y \equiv y_1$ and $x|y$, then $x_1|y_1$. Conclude that for $\overline{x}$, $\overline{y} \in R/\equiv$, the relation $\overline{x}|\overline{y}$ defined by $x|y$ is well-defined and that it is a partial order on $R/\equiv$.

10. Let R be a commutative ring. Show that the set of zero-divisors of R form an additive subgroup of R^+. Show that if x is a zero-divisor and $y \in R$, then xy is a zero-divisor. In particular the set of zero-divisors is a ring (without identity) by itself.

11. Let R be an associative and commutative ring. Show that the set of nilpotent elements form an additive subgroup of R^+. Show that if x is a nilpotent element and $y \in R$, then xy is a nilpotent element. In particular the set of nilpotent elements is a ring (without identity) by itself.

12. Let R be a ring. A function $\partial : R \longrightarrow R$ is called a **derivation** if it is an additive group homomorphism and if $\partial(xy) = \partial(x)y + x\partial(y)$ for all $x, y \in R$.

    a) Show that if R has 1 and ∂ is any derivation, then $\partial(1) = 0$.

    b) Show that if ∂_1 and ∂_2 are derivations of R, then $\partial + \partial_1$ is a derivation of R.

    c) Show that if R is ∂_1 and ∂_2 are derivations of R, then $\partial_1 - \partial_2$ and $[\partial_1, \partial_2] := \partial_1 \circ \partial_2 - \partial_2 \circ \partial_1$ (bracket operation) a derivation of R.

    d) Show that the set $\mathrm{Der}(R)$ of derivations of R is a Lie ring under the addition and the bracket operations.

13. Let R be a finite associative ring without zero divisors. Show that R has identity. Show that every nonzero element of R is invertible. (It is known that such a ring must also be commutative, but this is a much much harder result).

Chapter 7

Fundamental Notions

7.1 Subring

Let R be a ring. A **subring** of R is a subset S of R that is a ring under the operations of R. Thus a subset S of a ring R is a subring if and only if it is an additive subgroup and it is closed under multiplication.

If R is a ring with identity, then we also request from a subring to contain the identity of R.

If S is a subring of R (with or without identity, the context will make it clear), then we write $S \leq R$.

The notation $S \leq R$ may be confusing because we use the same notation for subgroups. To avoid this confusion, if S is a subgroup of the additive group of a ring R, we will use the notation $S \leq R^+$.

A ring R with an identity element may be considered only as a ring (without speaking about the existence of an identity, just forgetting it). When considered as a ring without identity, a subring S of R may or may not contain the identity element of R.

Examples.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.

2. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ if the latter is considered as a ring without identity. If $n \neq 1, -1$, then $n\mathbb{Z}$ is not a subring of $\mathbb{Z}$, if the latter is considered as a ring with identity.

3. For $i \in I$, let R_i be a ring. Then $\oplus_{i\in I} R_i$ is a subring of $\prod_{i\in I} R_i$. If each R_i has identity, then as we know $\prod_{i\in I} R_i$ has identity and – if X is infinite – $\oplus_{i\in I} R_i$ does not have an identity. In this case, we cannot say that $\oplus_{i\in I} R_i$ is a subring of the ring $\prod_{i\in I} R_i$, when the latter is considered as a ring with identity. On the other hand, ignoring the existence of the identity, $\oplus_{i\in I} R_i$ is a subring of the ring $\prod_{i\in I} R_i$.

4. Let R be a ring. The set $R \times \{0\}$ is a subring of $R \times R$. If R has identity 1, then both rings $R \times \{0\}$ and $R \times R$ have identities, namely $(1,0)$ and $(1,1)$ respectively. But since $(1,0) \neq (1,1)$, we cannot say that $R \times \{0\}$ is a subring of $R \times R$ when the latter is considered as a ring with identity.

7.2 Ring Homomorphisms

Let R and S be two rings. A **ring homomorphism** is a map $f : R \longrightarrow S$ which is an additive group homomorphism and also a multiplicative map, i.e. $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 r_2) = f(r_1)f(r_2)$. If R and S both have identity elements (1_R and 1_S respectively) and we consider them both as rings with identity, then we also want from a homomorphism to satisfy the equality $f(1_R) = 1_S$.

For example, the map that sends all the elements of a ring to its zero element 0 is a ring homomorphism. But if we consider a ring R with identity, then the zero-map is not a ring homomorphism anymore.

Isomorphisms, **automorphisms** and **endomorphisms** of rings are defined in the expected way. If two rings R and S are isomorphic, we denote this fact by $R \simeq S$.

Exercises.

1. Let R be a ring (with or without identity). Show that the projection map $\pi_1 : R \oplus R \longrightarrow R$ given by $\pi_1(x, y) = x$ is a homomorphism of rings. What is its kernel?

2. Let R and S be two rings (with or without identity). Let $\phi : R \longrightarrow S$ be a ring homomorphism. Show that $\phi(R) \leq S$.

3. Let R and S be two rings. Let $\phi : R \longrightarrow S$ be a ring homomorphism. Show that $\phi^{-1}(0) \leq R$ (i.e. is a subring of R). Show that if R and S are rings with identity then $\phi^{-1}(0)$ is not a subring of R anymore.

4. Let R be any ring with identity. Let 1_R be the identity element of R. Show that the map from $\mathbb{Z} \longrightarrow R$ defined by $n \mapsto n1_R$ is a ring homomorphism.

7.3 Ideals

Since a ring homomorphism is an additive group homomorphism, we can consider its **kernel**. Thus if $f : R \longrightarrow S$ is a ring homomorphism, we have

$$\mathrm{Ker}(f) := \{r \in R : f(r) = 0\}.$$

We know that $\mathrm{Ker}(f)$ is an additive subgroup of R^+. It is also a subring of R (if R is considered as a ring without identity), in other words $\mathrm{Ker}(f)$ is also closed under multiplication. But $\mathrm{Ker}(f)$ satisfies an even stronger property: If $x \in R$

and $y \in \mathrm{Ker}(f)$, then xy and yx are also in $\mathrm{Ker}(f)$. This is trivial to check: $f(xy) = f(x)f(y) = f(x)0 = 0$ and $f(yx) = f(y)f(x) = 0f(x) = 0$.

An additive subset of R that satisfies this property is called an **ideal** of R. Thus an ideal of R is an additive subgroup I of R such that $RI \subseteq I$ and $IR \subseteq I$. If I is an ideal of R, symbolically we represent this fact as $I \lhd R$.

There is another way to introduce ideals. Let R be a ring. Let I be an additive subgroup of R. Since the additive group structure of R is commutative, the quotient R/I is a group, with the addition defined as

$$(r + I) + (s + I) = (r + s) + I,$$

or as

$$\overline{r} + \overline{s} = \overline{r + s}$$

where $\overline{r} = r + I$ etc. We attempt to define a multiplication on R/I by setting

$$(r + I)(s + I) = rs + I.$$

But this may not be a well-defined addition. In other words, it is very possible that for $r, r_1, s, s_1 \in R$, $r + I = r_1 + I$, $s + I = s_1 + I$, but $rr_1 + I \neq ss_1 + I$. This attempt to define multiplication on the additive group R/I succeeds only if $I \lhd R$.

Theorem 7.3.1 *Let R be a ring and I an additive subgroup of R. Then the following conditions are equivalent:*

i) For all $r, r_1, s, s_1 \in R$, if $r + I = r_1 + I$ and $s + I = s_1 + I$, then $rs + I = r_1s_1 + I$.

ii. $I \lhd R$.

Proof: ($\Rightarrow$). Let $r \in R$ and $i \in I$. Take $r = r_1$, $s = i$ and $s_1 = 0$. Then we have $r + I = r_1 + I$ and $s + I = s_1 + I$, so we must have $rs + I = r_1s_1 + I$, i.e. $ri + I = I$, i.e. $ri \in R$. Thus $RI \subseteq I$. Similarly $IR \subseteq I$. Hence $I \lhd R$.

($\Leftarrow$). Assume $r, r_1, s, s_1 \in R$ are such that $r + I = r_1 + I$ and $s + I = s_1 + I$ then $rs - r_1s_1 = rs - rs_1 + rs_1 - r_1s_1 = r(s - s_1) + (r - r_1)s_1 \in I$. □

If R is a ring, then R and $\{0\}$ are two ideals of R. By abuse of language, the ideal $\{0\}$ is denoted by 0; it is called the zero-ideal. An ideal I is called **proper** if $I \neq R$.

Exercises.

1. Let R be a ring with identity and $I \subseteq R$. Show that $I \lhd R$ if and only if $I + I \subseteq I$, $RI \subseteq I$ and $IR \subseteq I$.

2. Let R be a ring with identity and let $I \lhd R$. Show that $I = R$ if and only if $1 \in I$.

3. Let R be a ring with identity and let $I \lhd R$. Show that $I = R$ if and only if $I \cap R^* \neq \emptyset$.

4. Show that any ideal of $\mathbb{R}$ is equal to $\{0\}$ or to $\mathbb{R}$.

5. Find all ideals of $\mathbb{Z} \oplus \mathbb{Q}$.

6. Find all the ideals of $\mathbb{Z}[\sqrt{2}]$.

7. Let R be an associative and commutative ring.

   a) Let $x \in R$. Show that the set Rx is an ideal.

   b) Let $x_1, \ldots, x_n \in R$. Show that $\{r_1x_1 + \ldots r_nx_n : r_i \in R\} \lhd R$.

   c) Let $X \subseteq R$. Show that $\{r_1x_1 + \ldots r_nx_n : n \in \mathbb{N},\, x_i \in X,\, r_i \in R\} \lhd R$.

8. Let R be a commutative ring. An element $x \in R$ is called a **zero-divisor** if $xy = 0$ for some nonzero $y \in R$. Show that the set of zero divisors of a commutative ring is an ideal.

9. Let R be a commutative ring. Show that the set of nilpotent elements of R is an ideal.

10. Is an ideal of an ideal of a ring necessarily an ideal of the ring?

11. Let R be a commutative and associative ring and $I \lhd R$. Let

$$\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}.$$

    $\sqrt{I}$ is called the **radical** of I.

    a) Show that $I \subseteq \sqrt{I} \lhd R$.

    b) Show that $\sqrt{I} = \sqrt{\sqrt{I}}$.

    c) Note that an element is nilpotent if and only if it is in $\sqrt{0}$.

12. Show that any ideal of the ring $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for a unique $n \in \mathbb{N}$.

13. Find all the ideals of $\mathbb{Z} \oplus \mathbb{Z}$.

14. Find all the ideals of $\mathbb{Z}^n$ $(n \in \mathbb{N})$.

15. Let I and J be two ideals of a commutative and associative ring R. Show that the set

$$I + J := \{i + j : i \in I, j \in J\}$$

    is an ideal. Show that it is the smallest ideal containing $I \cup J$.

16. Let I and J be two ideals of a commutative and associative ring R. Show that the set

$$IJ := \{i_1j_1 + \ldots + i_nj_n : n \in \mathbb{N},\, i_k \in I,\, j_k \in J\}$$

    is an ideal contained in $I \cap J$.

7.4 Ideal Generated by a Set

Lemma 7.4.1 *Let R be a ring. Then the intersection of a set of ideals of R is an ideal of R.*

Proof: Trivial. □

Let R be an associative and commutative ring and let $X \subseteq R$. Consider the intersection $\cap_{X \subseteq I \lhd R} I$ of all the ideals of R that contains X. By Lemma 7.4.1, this is an ideal of R. If R has identity, then this ideal certainly contains the set X. It follows that if R is an associative and commutative ring with identity, then $\cap_{X \subseteq I \lhd R} I$ is the smallest ideal of R that contains X.

We let $\langle X \rangle = \cap_{X \subseteq I \lhd R} I$ and call it the **ideal generated** by the set X.

Clearly $\{r_1 x_1 + \ldots r_n x_n : n \in \mathbb{N},\, x_i \in X,\, r_i \in R\} \subseteq \langle X \rangle$. But the set on the left hand side is an ideal of R by Exercise 7, page 62, and, since R has identity, it contains X (take $n = 1$ and $r_1 = 1$). Hence it is equal to $\langle X \rangle$.

We summarize these:

Theorem 7.4.2 *Let R be an associative and commutative ring with 1. Let $X \subseteq R$. Then $\langle X \rangle := \cap_{X \subseteq I \lhd R} I$ is the smallest ideal of R that contains X. Furthermore, $\langle X \rangle = \{r_1 x_1 + \ldots r_n x_n : n \in \mathbb{N},\, x_i \in X,\, r_i \in R\}$.*

If $X = \{x_1, \ldots, x_n\}$ then we sometimes write $\langle x_1, \ldots, x_n \rangle$instead of $\langle X \rangle$.

Instead of $\langle X \cup Y \rangle$, we also write $\langle X, Y \rangle$.

Exercises. In this set of exercises R denotes an associative and commutative ring with 1, unless stated otherwise.

1. Show that $\langle R \rangle = \langle -X \rangle$.
2. Show that $\langle 1 \rangle = R$.
3. Show that $\langle (1,0), (0,1) \rangle = R \oplus R$.
4. Show that if $I \lhd R$, then $\langle I \rangle = I$.
5. Let $R = \mathbb{Z}$. Find $\langle 2, 3 \rangle$.
6. Let $R = \mathbb{Z}$. Find $\langle 24, 36, 30 \rangle$.
7. Let $R = \mathbb{Z} \oplus \mathbb{Z}$. Find $\langle (24, -15), (7, 36) \rangle$.
8. If I and J are ideals of R, show that $\langle I,\, J \rangle = I + J$.
9. Do not assume that R has identity. Let $x \in R$. Show that $Rx + \mathbb{Z}x$ is the smallest ideal of R containing x. Generalize this result to an arbitrary subset of R.

7.5 Quotient of a Ring and Fundamental Theorems

Let R be a ring and $I \lhd R$. As we have seen above, we can define addition and multiplication on the coset space

$$R/I := \{r + I : r \in R\}$$

by

$$(r + I) + (s + I) = (r + s) + I$$

and

$$(r + I)(s + I) = rs + I.$$

Letting $\overline{r} = r + I$, we get

$$\overline{r} + \overline{s} = \overline{r + s}$$

and

$$\overline{r}\,\overline{s} = \overline{rs}.$$

Theorem 7.5.1 *If R is a ring and $I \lhd R$, then R/I is a ring with the operations defined as above. The map $r \mapsto \overline{r}$ is a homomorphism of rings from R onto R/I. The* **quotient ring** *R/I inherits the commutativity and the associativity of R. Furthermore if R has identity and I is a proper ideal of R, then $\overline{1}$ is the identity element of R/I.*

Proof: Easy. □

We can also describe the ideals of the quotient R/I:

Theorem 7.5.2 *Let R be a ring and $I \lhd R$. If $I \subseteq J \lhd R$, then J/I is an ideal of R/I. Conversely, any ideal α of R/I is of the form J/I for some unique ideal J or R containing I. Indeed,*

$$\alpha = \{r \in R : \overline{r} \in \alpha\}.$$

Proof: Easy. □

Sometimes we can "**factor out**" a homomorphism:

Theorem 7.5.3 *Let R and S be two rings (with r without identity) and $\phi : R \longrightarrow S$ be a ring homomorphism. Let $I \lhd R$ be such that $I \leq \mathrm{Ker}(\phi)$. Then the map $\overline{\phi} : R/I \longrightarrow S$ given by $\overline{p}hi(\overline{r}) = \phi(r)$ is well-defined and is a homomorphism of rings. We have $\mathrm{Ker}(\overline{\phi}) = \mathrm{Ker}(\phi)/I$. In particular, the map $\overline{\phi} : R/\mathrm{Ker}(\phi) \longrightarrow S$ is a one-to-one homomorphism of rings.*

Proof: Assume $r \equiv r_1 (\mathrm{mod}\, I)$. Then $r - r_1 \in I \leq \mathrm{Ker}(\phi)$, so that $\phi(r - r_1) = 0$ and $\phi(r) = \phi(r_1)$. Thus $\overline{\phi}$ is well-defined. Also, $\mathrm{Ker}(\overline{\phi}) = \{\overline{r} : \overline{\phi}(\overline{r}) = 0\} = \{\overline{r} : \phi(r) = 0\} = \{\overline{r} : r \in \mathrm{Ker}(\phi)\} = \mathrm{Ker}(\phi)/I$. The rest is easy. □

The quotient of R/I by some ideal J/I is as expected:

Theorem 7.5.4 *Let R be a ring and $I \lhd R$. Let $I \subseteq J \lhd R$. Then $R/J \simeq (R/I)/(J/I)$ naturally, via the map $\tilde{r} \mapsto \hat{\overline{r}}$ where $\tilde{r}$ is the class of $r \in R$ in R/J, $\overline{r}$ is the class of $r \in R$ in R/I, and $\hat{\overline{r}}$ is the class of $\overline{r} \in R/I$ in $(R/I)(J/I)$.*

Proof: Consider the composition of the canonical surjections $R \longrightarrow R/I \longrightarrow (R/I)/(J/I)$ given by $r \mapsto \overline{r} \mapsto \widehat{\overline{r}}$. The kernel of this composition is $\{r \in R : \hat{\overline{r}} = \hat{\overline{0}}\} = \{r \in R : \overline{r} = J/I\} = \{r \in R : r \in J\} = J$. Now apply Theorem 7.5.3. □

Exercises.

1. Find $\mathrm{End}(\mathbb{Z}/12\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{Z}/12\mathbb{Z})$. Find nilpotent elements and idempotents of the ring $\mathrm{End}(\mathbb{Z}/12\mathbb{Z})$.
2. Show that $\mathrm{Aut}(R \oplus R)$ has an element of order 2.
3. Does $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z})$ have an element of order 3?
4. Does $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z})$ have an element of order 3?
5. Find all ideals of $\mathbb{Z}/12\mathbb{Z}$.
6. Find all ideals of $\mathbb{Z}/n\mathbb{Z}$. How many of them are there?
7. Find all ideals I of $\mathbb{Z}$ for which $\mathbb{Z}/I$ has no nonzero nilpotent element.
8. Find all ideals I of $\mathbb{Z}$ for which $\mathbb{Z}/I$ has no nonzero zero-divisor.
9. Find all ideals I of $\mathbb{Z}$ for which $\mathbb{Z}/I$ has no idempotent element.
10. Let R be a ring and $I \lhd R$. Show that the ring R/I is associative if and only if for all x, y, $z \in R$ if $(xy)z - x(yz) \in I$.
11. Let R be a ring and $I \lhd R$.

    a) Show that the ring R/I is ring if and only if $xy - yx \in I$ for all x, $y \in R$.

    b) Show that the ideal $\langle xy - yx : x, y \in I \rangle$ is the smallest ideal I for which the ring R/I is commutative.
12. Let R be a ring and $I \lhd R$. Show that the ring R/I has no nonzero zero-divisors if and only if for all x, $y \in R$ if $xy \in I$ then either x or y is in I. Such an ideal is called a **prime ideal**.

Chapter 8

Domains, Division Rings and Fields

8.1 Some Facts About Ideals

A commutative, associative ring identity and without zero divisors is called a **domain**. An associative ring identity in which every nonzero element is invertible is called a **division ring**. A commutative division ring is called a **field**. Thus a field is a division ring and a division ring is a domain. But the converses are false. For example $\mathbb{Z}$ is a domain, but not a field. The rings $\mathbb{Q}$ and $\mathbb{R}$ are fields. Later we will give example of domains which are not fields.

An ideal M of a ring R is called **maximal** if it is a proper ideal and $M < I \lhd R$ implies $I = R$. We need Zorn's Lemma to prove the next lemma.

Lemma 8.1.1 *Let R be a ring with identity and $I \lhd R$ a proper ideal of R. Then there is a maximal ideal of R containing I.*

Proof: We will apply Zorn's Lemma to the set $Z = \{J \lhd R : I \subseteq J < R\}$ ordered by inclusion. Since $I \in Z$, $Z \neq \emptyset$. Let us show that Z is an inductive set. If $(J_\lambda)_{\lambda\in\Lambda}$ is a chain from Z, then clearly $\cup_{\lambda\in\Lambda} J_\lambda \neq R$ because 1 is not in $\cup_{\lambda\in\Lambda} J_\lambda$. We now show that $\cup_{\lambda\in\Lambda} J_\lambda$ is an ideal. Let x, $y \in \cup_{\lambda\in\Lambda} J_\lambda$. Let λ_1, $\lambda_2 \in \Lambda$ be such that $x \in J_{\lambda_1}$ and $y \in J_{\lambda_2}$. If $\lambda = \max(\lambda_1, \lambda_2)$, then x, $y \in J_\lambda$ and so $x + y \in J_\lambda \subseteq \cup_{\lambda\in\Lambda} J_\lambda$. Similarly, one can show that zx, $xz \in \cup_{\lambda\in\Lambda} J_\lambda$ for all $z \in R$. Thus Z is an inductive set. It follows that Z has a maximal element M. This maximal element M is a maximal ideal of R containing I. □

Note that in the lemma above we can take $I = 0$ to show that every ring with 1 has maximal ideals. This is false for rings without 1, see Question 2, 89.

Proposition 8.1.2 *Let R be a commutative ring with identity. Then R is a field if and only if R has only two ideals, 0 and R.*

Proof: Suppose R is a field. Let $0 < I \lhd R$. Let $x \in I \setminus \{0\}$. Since x has a multiplicative inverse y, $1 = xy \in I$. So for every $r \in R$, $r = r1 \in I$. Therefore $I = R$.

Conversely suppose that R has only two ideals 0 and R. Let $x \in R \setminus \{0\}$. Then $0 \neq x = 1x \in Rx \lhd R$. Thus $Rx = R$ and so $1 \in R = Rx$. Thus $1 = yx$ for some $y \in R$. This shows that x is invertible and that R is a field. □

In fact this theorem almost holds even if we do not assume that R has an identity.

Theorem 8.1.3 *Let R be a commutative ring without nontrivial proper ideals. Then*

i. Either R is a field, or

ii. $R = \mathbb{Z}/p\mathbb{Z}$ with p a prime and with the usual addition but trivial (zero) multiplication, or

iii. $R = 0$.

Proof: Let R be such a ring. Assume first R has zero multiplication, i.e. $xy = 0$ for all $x, y \in R$. Then ideals of R are just the subgroups of the additive group R^+. Thus R^+ has no proper, nontrivial subgroups. It follows from the Claim of Question 2, page 88 that either ii or iii holds. Assume from now on that the multiplication is not trivial.

For $x \in R$, xR is either 0 or R. The set $\mathrm{ann}_R(R) := \{x \in R : xR = 0\}$ is clearly an ideal of R. Thus either $\mathrm{ann}_R(R) = 0$ or R. The second case gives the zero multiplication. So $\mathrm{ann}_R(R) = 0$, i.e., if $x \neq 0$, then $xR \neq 0$.

Also for $x \in R \setminus \{0\}$, $0 \neq xR \lhd R$, so $xR = R$. Thus there is a $y \in R$ such that $xy = x$. Let now $z \in R$. Then since $Rx = R$, $z = rx$ for some $y \in R$. Hence $zy = rxy = rx = z$ and y is the identity element of R. Now the theorem follows from Theorem 8.1.2. □

Corollary 8.1.4 *Let R be a commutative ring with identity and $I \lhd R$. Then R/I is a field if and only if I is a maximal ideal of R.*

Proof: Follows from above and Theorem 7.5.2. □

Proposition 8.1.5 *Let $n \in \mathbb{N} \setminus \{0\}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is a prime if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field.*

Proof: The equivalence of the last two assertions follows from Corollary 8.1.4, but we will give a direct proof.

Note that each one of the three conditions implies that $n \neq 1$. So we assume $n \neq 1$.

Assume $\mathbb{Z}/n\mathbb{Z}$ is a domain. If $n = ab$ for $a\, b \in \mathbb{N}$, then $\overline{a}\,\overline{b} = \overline{n} = \overline{0}$, so that either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, i.e. n divides either a or b. If n divides a, then $a = na_1$ for some $a_1 \in \mathbb{N}$. Now we have $n = ab = na_1b$ and $a_1b = 1$, implying $b = 1$. Similarly if n divides b, then $a = 1$. Thus n is a prime. (See also Exercise 4, page 69).

Assume n is a prime. Let $\overline{x} \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$. Then x is prime to n and so there are a, $b \in \mathbb{N}$ such that $ax + bn = 1$. Now $\overline{a}\,\overline{x} = \overline{1}$ and so $\overline{x}$ is invertible.

If $\mathbb{Z}/n\mathbb{Z}$ is a field, it is clear that it is a domain. □

Let R be a ring with identity. As we know the map $\mathbb{Z} \longrightarrow R$ given by $n \mapsto n1_R$ is a homomorphism of rings. (Exercise 4, page 60). Let $n\mathbb{Z}$ be the kernel of this map ($n \in \mathbb{N} \setminus \{1\}$). Then $\mathbb{Z}/n\mathbb{Z}$ imbeds in R (Theorem 7.5.3). We call n the **characteristic** of the ring R and we write $n = \mathrm{char}(R)$. If $n = \mathrm{char}(R)$, then we have for any $x \in R$, $nx = (n1_R)x = 0x = 0$. In fact, if $\mathrm{char}(R) > 0$, then $\mathrm{char}(R)$ is the smallest positive natural number n for which $nx = 0$ for all $x \in R$. And if $\mathrm{char}(R) = 0$, then there is no smallest such $n > 0$.

If D is a domain of characteristic n, then, since $\mathbb{Z}/n\mathbb{Z}$ imbeds in D (Theorem 7.5.3), $\mathbb{Z}/n\mathbb{Z}$ is a domain and it follows from Proposition 8.1.5 that either $n = 0$ or n is a prime. In fact, in a domain D, if $nx = 0$ for some $x \in D \setminus \{0\}$ and $n \in \mathbb{N} \setminus \{0\}$, then $\mathrm{char}(D)$ divides n.

Now we ask the following question: Given a ring R and an ideal $I \lhd R$, what should be the conditions on I for R/I not to have zero-divisors? This is easy to answer: R/I does not have a nonzero divisor if and only if for all r, $s \in R$, if $rs \in I$, then either r or s is in I. We leave the formal proof to the reader. Such an ideal is called a **prime ideal**.

Now a harder question: Given a ring R and an ideal $I \lhd R$, what should be the conditions on I for R/I to be a division ring?

Exercises.

1. Show that a subring of a domain is a domain.
2. Show that the ring $R \oplus R$ is never a domain.
3. Show that in a domain D, if $nx = 0$ for some $x \in D \setminus \{0\}$ and $n \in \mathbb{N} \setminus \{0\}$, then $\mathrm{char}(D)$ divides n.
4. Show that a finite domain is a field. (See Exercise 13, page 58).
5. Does the ring $X\mathbb{R}[X]$ have a maximal ideal?

8.2 Field of Fractions of a Domain

Chapter 9

Ring of Polynomials

9.1 Definition

We start by giving a mathematical definition of the polynomials. Towards the end of this section, the polynomials will take the form that we believe the reader is most accustomed.

Let R be a ring. Consider the set $\oplus_{\mathbb{N}} R$. We know that $\oplus_{\mathbb{N}} R$ is an additive abelian group with the componentwise addition. We define another binary operation called multiplication as follows:

$$(r_n)_n (s_n)_n = (\sum_{i+j=n} r_i s_j)_n.$$

Theorem 9.1.1 *The set $\oplus_{\mathbb{N}} R$ together with the componentwise addition and the multiplication defined as above is a ring. If R is a commutative ring, then so is the ring $\oplus_{\mathbb{N}} R$. If R is an associative ring, then so is the ring $\oplus_{\mathbb{N}} R$. If R has identity, then so does the ring $\oplus_{\mathbb{N}} R$.*

Proof: Everything is trivial. Note that $(1, 0, 0, \ldots)$ is the identity of $\oplus_{\mathbb{N}} R$ if 1 is the identity of R. □

We may view the ring R as a subring of $\oplus_{\mathbb{N}} R$ by identifying $r \in R$ with the element $(r, 0, 0, \ldots)$ of $\oplus_{\mathbb{N}} R$ (even if R has identity). With this identification, we may multiply an element of R and an element of $\oplus_{\mathbb{N}} R$:

$$r \cdot (r_n)_n = (r r_n)_n.$$

Assume now R has identity. Let

$$X = (0, 1, 0, 0, \ldots).$$

Then it is easy to check that

$$\begin{aligned} X^2 &= (0, 0, 1, 0, 0, \ldots) \\ X^3 &= (0, 0, 0, 1, 0, \ldots) \\ X^4 &= (0, 0, 0, 0, 1, \ldots) \end{aligned}$$

Thus every element of $f = (f_i)_i \in \oplus_{\mathbb{N}} R$ can be written as $f = \sum_i f_i X^i$. With this notation, the addition and the multiplication become:

$$\begin{array}{rcl} (\sum_i f_i X^i) + (\sum_i g_i X^i) & = & \sum_i (f_i + g_i) X^i \\ (\sum_i f_i X^i)(\sum_i g_i X^i) & = & \sum_n (\sum_{i+j=n} f_i g_j) X^n. \end{array}$$

From now on, we will denote this ring as $R[X]$. The ring $R[X]$ is called the **ring of polynomials** over R and its elements are called **polynomials** over R. Because the notation suggests, an element f of $R[X]$ is often denoted as $f(X)$.

If $f(X) = \sum_i f_i X^i \neq 0$, then there is a largest n for which $f_n \neq 0$. This natural number n is called the **degree** of $f(X)$. We let the degree of the zero-polynomial to be $-\infty$. We denote the degree of $f(X)$ as $\deg(f(X))$. Note that

$$\deg(f + g) \leq \max(\deg(f), \deg(g))$$

and if $\deg(f) \neq \deg(g)$, then

$$\deg(f + g) = \max(\deg(f), \deg(g)).$$

Also

$$\deg(fg) \leq \deg(f) + \deg(g)).$$

On the other hand, if R has no zero-divisors, then

$$\deg(fg) = \deg(f) + \deg(g)).$$

If $f(X) = f_0 + f_1 X + \ldots + f_n X^n$ and $f_n \neq 0$ (i.e. $\deg(f) = n$), them f_n is called the **leading coefficient** and f_0 is called the **constant term** of the polynomial $f(X)$. A polynomial whose leading coefficient is 1 is called a **monic** polynomial. Polynomials of degree < 1 (i.e. the elements of R as they imbed in $R[X]$) are called **constant polynomials**.

Exercises.

1. Let $R = \mathbb{Z}/2\mathbb{Z}$ and $f(X) = X^2 + X \in R[X]$. Note that $f(X)$ is not a zero polynomial but that $x^2 + x = 0$ for all $x \in R$.
2. Show that if $S \leq R$, then $S[X] \leq R[X]$.
3. Show that the product of two monic polynomials is a monic polynomial.
4. Let R be a commutative ring with no nonzero nilpotent elements. If the polynomial $f(X) = a_0 + a_1 X + \ldots + a_m X^m$ in $R[X]$ is a zero-divisor (that is $g(X)f(X) = 0$ for some nonzero polynomial $g(X) \in R[X]$), prove that there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \ldots = ba_m = 0$.
5. Show that $(R[X])[Y] \simeq (R[Y])[X]$ (as rings).
6. Let $I \lhd R$.
   a) Show that $I[X] \lhd R[X]$.
   b) Show that $R[X]/I[X] \simeq (R/I)[X]$.

7. Let $I \lhd R$ and $n \in \mathbb{N}$. Show that the set of polynomials over R whose first n coefficients are in I is an ideal of $R[X]$.

8. Let I be the set of polynomials over $\mathbb{Z}$ whose constant term is in $2\mathbb{Z}$. Then $I \lhd \mathbb{Z}[X]$. Find $\mathbb{Z}[X]/I$.

9. Let I be the set of polynomials over $\mathbb{Z}$ whose first two coefficients are in $2\mathbb{Z}$. Then $I \lhd \mathbb{Z}[X]$. Find $\mathbb{Z}[X]/I$.

10. Let $n \in \mathbb{N} \setminus \{0\}$. Let I be the set of polynomials over $\mathbb{Z}$ whose first n coefficients are in $2\mathbb{Z}$. Then $I \lhd \mathbb{Z}[X]$. Find $\mathbb{Z}[X]/I$.

11. Let $n \in \mathbb{N}$. Show that $\mathbb{Z}[X]/n\mathbb{Z}[X] \simeq (\mathbb{Z}/n\mathbb{Z})[X]$.

12. Find the idempotents, the zero-divisors, the invertible elements, the nilpotent elements of $\mathbb{Z}[X]/\langle 3X - 2\rangle$.

13. Show that $\mathbb{Z}[X]/\langle X - 2\rangle \simeq \mathbb{Z}$.

14. Find the idempotents, the zero-divisors, the invertible elements, the nilpotent elements of $\mathbb{R}[X]/\langle X^2\rangle$.

15. Find the idempotents, the zero-divisors, the invertible elements, the nilpotent elements of $\mathbb{R}[X]/\langle X^2 - 1\rangle$.

16. Find the idempotents, the zero-divisors, the invertible elements, the nilpotent elements of $\mathbb{R}[X]/\langle X^2 + 1\rangle$.

17. Show that $\mathbb{R}[X]/\langle X^2 + 1\rangle \simeq \mathbb{R}[X]/\langle X^2 + X + 1\rangle$.

18. Find the idempotents, the zero-divisors, the invertible elements, the nilpotent elements of $\mathbb{R}[X]/\langle X^3\rangle$.

19. Find the nilpotent elements of $(\mathbb{Z}/4\mathbb{Z})[X]$.

20. Show that the ideal $\langle 2, X\rangle$ of $\mathbb{Z}[X]$ is not generated by a single element of $\mathbb{Z}[X]$.

9.2 Euclidean Division

Theorem 9.2.1 (Euclidean Division) *Let R be a ring. Let $f(X), g(X) \in R[X]$. Assume the leading coefficient of $g(X)$ is invertible. Then there are unique $q(X), r(X) \in R[X]$ such that $f(X) = g(X)q(X)+r(X)$ and $\deg(r(X)) < \deg(g(X))$.*

Proof: We first show the existence of $q(X)$ and $r(X)$ by induction on the degree of $f(X)$. Assume first that $\deg(f(X)) < \deg(g(X))$. Then we can take $q(X) = 0$ and $r(X) = f(X)$. Assume now $\deg(f(X)) \geq \deg(g(X))$. Let f_n and g_m be the leading coefficients of $f(X)$ and $g(X)$ respectively. Consider the

polynomial $f(X) - g(X)g_m^{-1}f_nX^{n-m}$. The degree of this polynomial is strictly less than the degree of $g(X)$. By induction, there are q_1, $r \in R[X]$ such that $f(X) - g(X)g_m^{-1}f_nX^{n-m} = g(X)q_1(X) + r(X)$ and $\deg(q(X)) < \deg(g(X))$. Thus we have, $f(X) = g(X)(g_m^{-1}f_nX^{n-m}+q_1(X))+r(X)$. We can take $q(X) = g_m^{-1}f_nX^{n-m} + q_1(X)$.

We now prove the uniqueness of $q(X)$ and $r(X)$. Assume $g(X)q(X)+r(X) = g(X)q_1(X) + r_1(X)$ and $\deg(r(X)) < \deg(g(X))$ and $\deg(r_1(X)) < \deg(g(X))$ for some $q(X)$, $q_1(X)$, $r(X)$, $r_1(X) \in R[X]$. Then $g(X)(q(X) - q_1(X)) = r_1(X) - r(X)$ and so $\deg(g(X)) + \deg(q(X) - q_1(X)) = \deg(g(X)(q(X) - q_1(X))) = \deg(r_1(X) - r(X)) < \deg(g(X))$. Thus $\deg(q(X) - q_1(X)) = -\infty$ and $q(X) = q_1(X)$. It follows that $r(X) = r_1(X)$ as well. □

9.3 Ideals of $K[X]$

9.3.1 Irreducible Polynomials

9.4 Ideals of $K[[X]]$

9.5 Ideals of $K[X_1, \ldots, X_n]$

Chapter 10

Euclidean Domains and Principal Ideal Domains

Chapter 11

Modules and Vector Spaces

Chapter 12

Local Rings

12.1 Introduction

A commutative ring R with identity is called **local** M if it has a unique maximal (proper of course) ideal. Thus R/M is a field, called the **residue field** of R. In this section all our rings are commutative and have identity.

Note the trivial fact that if R is a local ring with M its unique maximal ideal and if $I \lhd R$, then R/I is a local ring with M/I its unique maximal ideal.

Lemma 12.1.1 *A ring is local if and only if its noninvertible elements form an ideal.*

Proof: Let R be the ring. Assume it is local. Let M be its unique maximal ideal. Clearly $M \subseteq R \setminus R^*$. Conversely let r be a noninvertible element of R. Assume $r \notin M$. Then there is a maximal ideal N containing r. Since $N \neq M$, this contradicts the fact that M is the unique maximal ideal of R. □

From now on, R denotes a local ring. We let M denote its maximal ideal. By the lemma above we have $M = R \setminus R^*$.

Lemma 12.1.2 *For M^n/M^{n+1} is an R/M-vector space in a natural way.*

Proof: Suppose $m, m' \in M^n$ are such that $m \equiv m' \bmod M^{n+1}$ and $r, r' \in R$ such that $r \equiv r' \bmod M$. Then $rm - r'm' = r(m - m') + (r - r')m' \in M^{n+1}$. Thus we can multiply an element $\overline{r} \in R/M$ and an element $\overline{m} \in M^n/M^{n+1}$ by $\overline{r} \cdot \overline{m} = \overline{rm}$. To check that M^n/M^{n+1} is an R/M-vector space is easy. □

We will see in Section 12.3.1 that if $\cap_n M^n = 0$ then the local ring R is also a metric space compatible with the ring structure (Proposition 12.3.1).

Exercises.

1. Let K be a field. Show that $K[X]/\langle X^n \rangle$ is a local ring.

2. Show that $K[[X]]$ is a local ring.
3. Let R be any local ring and $k \in \mathbb{N}^{>0}$. Show that the ring $S = R[X]/\langle X^k \rangle$ is also a local ring. Show that $N = M + Rx + \ldots + Rx^{k-1}$ is the unique maximal ideal of S. Find N^n for $n \in \mathbb{N}^{>0}$. Show that if $\cap_n M^n = 0$ then $\cap_n N^n = 0$.
4. Find a local ring R whose maximal ideal M satisfies $\cap_n M^n \neq 0$.

12.2 Completion of a Ring

Let R be a commutative ring with 1 which is also a metric space compatible with the operations of R, i.e. the maps $(x, y) \mapsto x - y$ and $(x, y) \mapsto xy$ from $R \times R$ into R are continuous. Let d denote the metric. Let $\tilde{R}$ be the completion of R. Recall that $\tilde{R}$ is the set of Cauchy sequences of R divided out by the equivalence relation

$$(r_n)_n \equiv (s_n)_n \iff \lim_{n\to\infty} r_n - s_n = 0.$$

We embed R into $\tilde{R}$ by sending an element $r \in R$ to the class of the constant sequence $(r)_n$. Recall also that $\tilde{R}$ is a metric space with

$$d(\overline{(r_n)_n}, \overline{(s_n)_n}) = \lim_{n\to\infty} d(r_n, s_n).$$

Lemma 12.2.1 *The maps $(x, y) \mapsto x - y$ and $(x, y) \mapsto xy$ from $\tilde{R} \times \tilde{R}$ into $\tilde{R}$ are continuous.*

Proof:

Exercises. Let (R, d) be as in this subsection.

1. Show that any polynomial map from R into R is continuous.

12.3 Discrete Valuation Rings

12.3.1 Introduction

Let R be a commutative ring with identity and $I \lhd R$ an ideal. Set $I^0 = R$ and $I^{n+1} = I^n I = \langle xy : x \in I^n, y \in I \rangle$. Clearly $I^{n+1} \leq I^n$ and $I^n I^m \leq I^{n+m}$. If $x \in I^n \setminus I^{n+1}$, we set $\mathrm{val}_I(x)$ to be n. If $x \in \cap_n I^n$, set $\mathrm{val}_I(x) = \infty$. In particular $\mathrm{val}_I(0) = \infty$. Thus val_I is a function from R into $\mathbb{N} \sqcup \{\infty\}$. We order $\mathbb{N} \sqcup \{\infty\}$ naturally and define addition on it in a natural way. Clearly $\mathrm{val}_I(x) \geq n$ if and only if $x \in I^n$. Also,

$$\begin{array}{lcl} \mathrm{val}(x) = \infty & \iff & x \in \cap_n I^n \\ \mathrm{val}_I(xy) & \geq & \mathrm{val}_I(x) + \mathrm{val}_I(y), \\ \mathrm{val}(-x) & = & \mathrm{val}(x), \\ \mathrm{val}_I(x+y) & \geq & \min\{\mathrm{val}_I(x), \mathrm{val}_I(y)\}, \\ \mathrm{val}_I(x+y) & = & \min\{\mathrm{val}_I(x), \mathrm{val}_I(y)\} \text{ if } \mathrm{val}_I(x) \neq \mathrm{val}_I(y). \end{array}$$

Exercises.

1. Give an example of a ring R with an ideal I such that $I^{n+1} < I^n$ and $\cap_n I^n \neq 0$. (Example: $R = \mathbb{R}[X,Y]/\langle XY - Y\rangle$ and $I = \langle X, Y\rangle$).
2. Let K be a field, $R = K[X,Y]/\langle X^2 - Y^3\rangle$, $I = \langle X, Y\rangle$. Show that I^n is generated by two elements. Show that $\mathrm{val}_I(x) = 1$ and $\mathrm{val}_I(x^2) = 3$. More generally find $\mathrm{val}_I(x^n)$.

For $\lambda \in (0,1)$, a fixed real number, define $d_I(x,y) = \lambda^{\mathrm{val}(x-y)} \in \mathbb{R}$. (We let $\lambda^\infty = 0$). Then, for all x, y, $z \in R$ we have,

$$\begin{aligned}
&d_I(x,y) \geq 0,\\
&d_I(x,y) = 0 \text{ if and only if } x - y \in \cap_n I^n,\\
&d_I(x,y) = d_I(y,x),\\
&d_I(x,y) \leq \max(d_I(x,z), d_I(z,y)) \leq d_I(x,z) + d_I(z,y).
\end{aligned}$$

We even have a sharper relation than the last one, namely,

$$d_I(x,y) = \max(d_I(x,z), d_I(z,y))$$

if $d_I(x,z) \neq d_I(z,y)$.

As one notices, d_I looks like a distance function. For d_I to be a distance function, we need sharper relations:

$$d_I(x,y) = 0 \text{ if and only if } x = y.$$

In other words we need $\cap_n I^n = 0$.

Proposition 12.3.1 *Let R be a commutative ring with 1. Let $I \lhd R$ be such that $\cap_n I^n = 0$. Let $\lambda \in (0,1)$ be any real number. Define*

$$\mathrm{val}_I(x) = \begin{cases} \max(n \in \mathbb{N} : x \in I^n) & \text{if } x \neq 0\\ \infty & \text{otherwise.}\end{cases}$$

Then val_I is a map from R into $\mathbb{N} \cup \{\infty\}$ with the following properties:

$$\begin{aligned}
&\mathrm{val}_I(x) = \infty \text{ if and only if } x = 0,\\
&\mathrm{val}_I(x) = \mathrm{val}_I(-x),\\
&\mathrm{val}_I(xy) \geq \mathrm{val}_I(x) + \mathrm{val}_I(y),\\
&\mathrm{val}_I(x+y) \leq \min(\mathrm{val}_I(x), \mathrm{val}_I(y)).
\end{aligned}$$

If λ is any real number strictly between 0 and 1, defining

$$d(x,y) = \lambda^{\mathrm{val}_I(x-y)},$$

we get a metric space (R,d) where the ring operations subtraction and multiplication are continuous maps from $R \times R$ into R. The ideal I^n are clopen subsets of R.

Proof: We already have shown that the four properties of val_I hold. We also have shown that d is a metric on R.

Let us show that substraction is continuous. We have to show that the inverse image of an open subset of R under the map $- : R \times R \longrightarrow R$, $(x, y) \mapsto x - y$, is open in $R \times R$. It is enough to show this for the open balls $B(a, r)$ of R. We will show that if $b - c \in B(a, r)$ then the image $B(b, r) - B(c, r)$ of $B(b, r) \times B(c, r)$ is a subset of $B(a, r)$, this will show that (b, c) is in the interior of the inverse image of $B(a, r)$, proving that the inverse image of $B(a, r)$ is open.

Let n be such that $\lambda^n \geq r > \lambda^{n+1}$. Let $x \in B(b, r)$ and $y \in B(c, r)$. Then $\lambda^{\mathrm{val}_I(x-b)} = d_I(x, b) < r \leq \lambda^n$, so that $\mathrm{val}_I(x-b) > n$, i.e. $x-b \in I^{n+1}$. Similarly $y-c \in I^{n+1}$ and $b-c-a \in I^{n+1}$. Thus $x-y-a = (x-b)-(y-c)+(b-c-a) \in I^{n+1}$, $\mathrm{val}_I(x - y - a) > n + 1$ and $d_I(x - y, a) = \lambda^{\mathrm{val}_I(x-y-a)} < \lambda^{n+1} < r$.

Assume now that $bc \in B(a, r)$. We will know show that $B(b, r)B(c, r) \subseteq B(a, r)$. Let $x \in B(b, r)$ and $y \in B(c, r)$. As before, $x - b$, $y - c$, $bc - a \in I^{n+1}$. Thus $xy - a = xy - by + by - bc + bc - a = (x - b)y + b(y - c) + (bc - a) \in I^{n+1}$.

Since $I^n = \{x \in R : \mathrm{val}(x) \geq n\} = \{x \in R : d(x, 0) \leq \lambda^n\} = \overline{B}(0, \lambda^n) = B(0, \lambda^{n-1/2})$, I^n is both open and closed subset of R. □

The metric space (R, d_I) satisfies an inequality sharper than the triangular inequality, namely,

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}.$$

Metric spaces satisfying this sharper inequality are called **ultrametric spaces**

Exercise.

1. Let R and I be as in the proposition above. Show that if $I^n = 0$ for some n, then (R, d_I) is a complete metric space. (Hint: Cauchy sequences are eventually constant).

12.3.2 Discrete Valuation Rings

Let R be a commutative ring with identity. To the properties of the function val_I defined above we will add a new one to get the concept of discrete valuation ring.

A map $\mathrm{val} : R \longrightarrow \mathbb{Z} \cup \{\infty\}$ is called a **valuation** if

$$\begin{array}{lcl} \mathrm{val}(x) = \infty & \iff & x = 0 \\ \mathrm{val}_I(xy) & = & \mathrm{val}_I(x) + \mathrm{val}_I(y), \\ \mathrm{val}_I(x + y) & \geq & \min\{\mathrm{val}_I(x), \mathrm{val}_I(y)\}, \end{array}$$

A commutative ring with identity together with a valuation above is called a **discrete valuation ring**. Note that we have not used the multiplication on $\mathbb{Z}$ in the definition, we have only used the ordered abelian group structure $(\mathbb{Z}, +, 0, \leq)$. Replacing $\mathbb{Z}$ with any other ordered abelian group, we get a more general concept of valuation.

From now on (R, val) stands for a discrete valuation ring. We start listing the properties of such a ring.

Properties of (R, val)**.**

1. $\mathrm{val}(1) = \mathrm{val}(-1) = 0$.

   Proof: Since $\mathrm{val}(1) = \mathrm{val}(1 \cdot 1) = \mathrm{val}(1) + \mathrm{val}(1)$, we have $\mathrm{val}(1) = 0$. Also, since $0 = \mathrm{val}(1) = \mathrm{val}((-1)\cdot(-1)) = \mathrm{val}(-1) + \mathrm{val}(-1)$, $\mathrm{val}(-1) = 0$.

2. *For all* $x \in R$, $\mathrm{val}(x) = \mathrm{val}(-x)$.

   Proof: Since $\mathrm{val}(-1) = 1$, $\mathrm{val}(-x) = \mathrm{val}((-1)x) = \mathrm{val}(-1)\,\mathrm{val}(x) = \mathrm{val}(x)$.

3. R *is a domain.*

   Proof: Assume $xy = 0$. Then $\infty = \mathrm{val}(0) = \mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$. Therefore either $\mathrm{val}(x)$ or $\mathrm{val}(y)$ is ∞, i.e. either x or y is 0.

4. val *extends to the field of fractions* K *of* R *and* (K, val) *is also a discrete ring (field!) of valuation.*

   Proof: Let x, y, z, $t \in R$ with $y \neq 0$ and $t \neq 0$. Assume $x/y = z/t$ in K. Then $xt = yz$ and so $\mathrm{val}(x) - \mathrm{val}(y) = \mathrm{val}(z) - \mathrm{val}(t)$. Therefore we may define $\mathrm{val}(x/y)$ to be $\mathrm{val}(x) - \mathrm{val}(y)$. The fact that (K, val) is a discrete ring (field!) of valuation is easy to check and we leave it to the reader.

From now on we forget about R, and we work with the field K, the field of fractions of R.

Since val is a homomorphism from the multiplicative group $(K^*, \cdot)$ into the additive group $(\mathbb{Z}, +)$, $\mathrm{val}(K^*) \leq \mathbb{Z}^+$. Thus $\mathrm{val}(K^*) = n\mathbb{Z}$ for some unique $n \in \mathbb{N}^{>0}$. Replacing val by $\mathrm{val}(n)$, we may assume that $\mathrm{val} : K^* \longrightarrow \mathbb{Z}$ is onto. In particular there is a $\pi \in K$ such that $\mathrm{val}(\pi) = 1$. From now on we fix such a π.

We let

$$\mathcal{O} = \{x \in K : \mathrm{val}(x) \geq 0\}$$

and

$$\mathcal{M} = \{x \in K : \mathrm{val}(x) > 0\} = \{x \in K : \mathrm{val}(x) > 0\} = \{x \in K : \mathrm{val}(x) \geq 1\}.$$

We continue listing the properties of (K, val).

Properties of (K, val)**.**

1. *For* $x \in K^*$, $\mathrm{val}(x^{-1}) = -\,\mathrm{val}(x)$.

   Proof: Since $0 = \mathrm{val}(1) = \mathrm{val}(xx^{-1}) = \mathrm{val}(x) + \mathrm{val}(x^{-1})$, $\mathrm{val}(x^{-1}) = -\,\mathrm{val}(x)$.

2. $\mathcal{O}$ *is a ring with 1 and* $\mathcal{M} \lhd \mathcal{O}$.

   Proof: This follows from the fact that $\mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$.

3. *$\mathcal{O}$ is a local ring with $\mathcal{M}$ as its unique maximal ideal. In other words $\mathcal{O}^* = \mathcal{O} \setminus \mathcal{M}$.*

   Proof: Let $x \in \mathcal{O}^*$. Then $\mathrm{val}(x) \geq 0$ and $-\mathrm{val}(x) = \mathrm{val}(x^{-1}) \geq 0$. Thus $\mathrm{val}(x) = 0$. It follows that $x \in (O) \setminus (M)$.

   Conversely, if $x \in (O) \setminus (M)$, then $\mathrm{val}(x) = 0$ and so $\mathrm{val}(x^{-1}) = -\mathrm{val}(x) = 0 \geq 0$, i.e. $x^{-1} \in \mathcal{O}$. Thus $x \in \mathcal{O}^*$.

4. *$\mathcal{M} = \pi\mathcal{O}$.*

   Proof: Since $\mathrm{val}(\pi) = 1$, $\pi \in \mathcal{M}$. So $\pi\mathcal{O} \leq \mathcal{M}$. Conversely, if $x \in \mathcal{M}$, then $x = \pi(x\pi^{-1}) \in \pi\mathcal{O}$ because $\mathrm{val}(x\pi^{-1}) = \mathrm{val}(x) + \mathrm{val}(\pi^{-1}) = \mathrm{val}(x) - \mathrm{val}(\pi) = \mathrm{val}(x) - 1 \geq 0$.

5. *For $n \in \mathbb{Z}$, $\{x : \mathrm{val}(x) \geq n\} = \pi^n\mathcal{O}$ and $\{x : \mathrm{val}(x) = n\} = \pi^n\mathcal{O}^*$.*

   Proof: Let $x \in K$ have valuation n. Then $x = \pi^n(x\pi^{-n})$ and since $\mathrm{val}(x\pi^{-n}) = \mathrm{val}(x) + \mathrm{val}(\pi^{-n}) = 0$, $x\pi^{-n} \in \mathcal{O}^*$.

Example. $R = \mathbb{Z}$ and $M = p\mathbb{Z}$ (p a prime). We get the so-called **p-adic valuation**. Its completion is denoted $\mathbb{Z}_p$ and is called the **p-adic integers**.

Exercises.

1. What is the field of fractions of $\mathbb{Z}_p$?
2. **(Conway and Sloan)** Let

   $$a_1 = 4,\ a_2 = 34,\ a_3 = 334,\ a_4 = 3334, \ldots$$

   Show that $3a_n = 5^n + 2$. Conclude that in $\mathbb{Z}_5$, $\lim_{n\to\infty} a_n = 2/3$.
3. Show that there is a sequence $(a_n)_n$ of integers such that

   $$\begin{aligned} a_n^2 + 1 &\equiv 0 \bmod 5^n \\ a_{n+1} &\equiv a_n \bmod 5^{n+1} \end{aligned}$$

   for all $n \geq 1$ Conclude that $x^2 + 1 = 0$ is solvable in $\mathbb{Z}_5$.
4. Show that $x^2 + 1 = 0$ has a solution in $\mathbb{Z}_p$ if and only if $p \equiv 1 \bmod 4$. (Needs some finite field theory).

12.3.3 p-adic Integers

Theorem 12.3.2 (Hensel's Lemma) *Let $f(X) \in \mathbb{Z}_p[X]$. Assume that there is an $\alpha \in \mathbb{Z}_p$ (equivalently in $\mathbb{Z}$) such that $f(a) \equiv 0 \bmod p$ and $f'(a) \not\equiv 0 \bmod p$. Then there is a unique $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$ and $\beta \equiv \alpha \bmod p$.*

Chapter 13

Exams

13.1 Basic Algebra I, Midterm, November 2003 and Its Correction

1. *How many abelian groups are there up to isomorphism of order* 67500? (5 pts.)

Answer: Since $67500 = 675 \times 10^2 = 25 \times 27 \times 10^2 = 2^2 \times 3^2 \times 5^4$, the answer is $2 \times 2 \times 5 = 20$.

For the 2-part of the group we have two choices: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

For the 3-part of the group we have two choices: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$.

For the 5-part of the group we have five choices:

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,

$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$,

$\mathbb{Z}/625\mathbb{Z}$,

$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

2. *Let* $\mathbb{Z}(p^\infty)$ *be the Prüfer p-group. Prove or disprove*: $\mathbb{Z}(p^\infty) \simeq \mathbb{Z}(p^\infty) \oplus \mathbb{Z}(p^\infty)$. (5 pts.)

Disproof: The first one has $p-1$ elements of order p, the second one has $p^2 - 1$ elements of order p, so that these two groups cannot be isomorphic.

3. *Show that a subgroup of index* 2 *of a group is necessarily normal.* (5 pts.)

Proof: Let H be a subgroup of index 2 of G. Let $a \in G/H$. Then $G = H \sqcup Ha = H \sqcup aH$, so that $aH = G/H = Ha$, hence $aH = Ha$. If $a \in H$, $aH = Ha$ as well. So $aH = Ha$ all $a \in G$ and $H \triangleright G$.

4. *Show that* $\mathbb{Q}^* \approx (\mathbb{Z}/2\mathbb{Z}) \oplus (\oplus_\omega \mathbb{Z})$. (5 pts.)

Proof: Let $q \in \mathbb{Q}^*$. Then $q = a/b$ for some $a, b \in \mathbb{Z}/\{0\}$. Decomposing a and b into their prime factorization, we can write q as a $\pm$product of (negative or

positive) powers of prime numbers. Set,

$$q = \varepsilon(q) \prod_{p \text{ prime}} p^{\text{val}_p(q)}$$

where $\text{val}_p(q) \in \mathbb{Z}$ and $\varepsilon(q) = \pm 1$ depending on the sign of q. Note that all the $\text{val}_p(q)$ are 0 except for a finite number of them. Let $\phi : \mathbb{Q}^* \to (\mathbb{Z}/2\mathbb{Z}) \oplus (\oplus_\omega \mathbb{Z})$ be defined by

ϕ(q) = ($\varepsilon(q)$, $\text{val}_2(q)$, $\text{val}_3(q)$, $\text{val}_5(q)$, ...)

It is clear that ϕ is an isomorphism of groups. (Here we view $\mathbb{Z}/2\mathbb{Z}$ as the multiplicative group {1, -1}).

5. *Find* $|\text{Aut}(\mathbb{Z}/p^n\mathbb{Z})|$. (10 pts.)

Solution. The group $\mathbb{Z}/p^n\mathbb{Z}$ being cyclic (generated by $\underline{1}$, the image of 1), any endomorphism ϕ of $\mathbb{Z}/p^n\mathbb{Z}$ is determined by $\phi(\ \underline{1}\ )$. Then $\phi(\ \underline{x}\ ) = x\phi(\ \underline{1}\ )$ for all $x \in \mathbb{Z}$. Conversely any $\underline{a} \in \mathbb{Z}/p^n\mathbb{Z}$ gives rise to a homomorphism ϕ_a via $\phi_a(\ \underline{x}\ ) = x\underline{a}$. In other words $\text{End}(\mathbb{Z}/p^n\mathbb{Z}) \approx \mathbb{Z}/p^n\mathbb{Z}$ via $\phi \mapsto \phi(1)$ as rings with identity. Thus $\text{Aut}(\mathbb{Z}/p^n\mathbb{Z}) = \text{End}(\mathbb{Z}/p^n\mathbb{Z})^* \approx (\mathbb{Z}/p^n\mathbb{Z})^* = \{\underline{a} : a \text{ prime to } p\}$ $= \{\underline{a} : a \text{ not divisible by } p\} = \mathbb{Z}/p^n\mathbb{Z}/p\mathbb{Z}/p^n\mathbb{Z}$ and has $p^n - p^{n-1}$ elements.

6. *What is* $\text{Hom}(\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z})$? *More generally, what is* $\text{Hom}(\mathbb{Z}/n\mathbb{Z},\ \mathbb{Z}/m\mathbb{Z})$? *How many elements does it have*? (15 pts.)

Answer: Since $\mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by $\underline{1}$ (the image of 1 in $\mathbb{Z}/n\mathbb{Z}$), any element ϕ of $\text{Hom}(\mathbb{Z}/n\mathbb{Z},\ \mathbb{Z}/m\mathbb{Z})$ is determined $\phi(\ \underline{1}\ ) \in \mathbb{Z}/m\mathbb{Z}$. Let

$$\text{val}_1 : \text{Hom}(\mathbb{Z}/n\mathbb{Z},\ \mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z}$$

be the map determined by $\text{val}_1(\phi) = \phi(\ \underline{1}\ )$. This is a homomorphism of (additive) groups. Furthermore it is one to one. However val_1 is not onto as in Question 5, because not all $\underline{a} \in \mathbb{Z}/m\mathbb{Z}$ gives rise to a well-defined function $\underline{x} \mapsto x\underline{a}$.

Claim: *An element* $\underline{a} \in \mathbb{Z}/m\mathbb{Z}$ *gives rise to a well-defined function* $\underline{x} \mapsto x\underline{a}$ *if and only if* m/d *divides* a *where* $d = \gcd(m,\ n)$.

Proof of the Claim: Assume m/d divides $a$where $d = \gcd(m,\ n)$. We want to show that the map $\underline{x} \mapsto x\underline{a}$ from $\mathbb{Z}/n\mathbb{Z}$ into $\mathbb{Z}/m\mathbb{Z}$ is well-defined. Indeed assume $\underline{x} = \underline{y}$. Then n divides $x - y$. So na divides xa - ya. By hypothesis, it follows that nm/d divides xa - ya. Since $nm/d = \text{lcm}(m,\ n)$, we get that $\text{lcm}(m,\ n)$ divides xa - ya. Hence m divides xa - ya. It follows that $x\underline{a} = y\underline{a}$.

Conversely, assume that the function $\underline{x} \mapsto x\underline{a}$ from $\mathbb{Z}/n\mathbb{Z}$ into $\mathbb{Z}/m\mathbb{Z}$ is well-defined. Then $n\underline{a} = 0\underline{a} = \underline{0}$ and m divides na. Hence m/d divides $(n/d)a$. Since n/d and m/d are prime to each other we get that m/d divides a. This proves the claim.

Now we continue with the solution of our problem. The claim shows that the homomorphism

$$\text{val}_1 : \text{Hom}(\mathbb{Z}/n\mathbb{Z},\ \mathbb{Z}/m\mathbb{Z}) \to (m/d)\mathbb{Z}/m\mathbb{Z}$$

is an isomorphism. We can go further and prove that $(m/d)\mathbb{Z}/m\mathbb{Z} \approx \mathbb{Z}/d\mathbb{Z}$

Claim: *If $n = mp$ then $m\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}/p\mathbb{Z}$.*

Proof of the Claim: Let $\phi : \mathbb{Z} \to m\mathbb{Z}/n\mathbb{Z}$ be defined by $\phi(x) = \underline{mx}$. Clearly ϕ is a homomorphism and onto. Its kernel is $\{x \in \mathbb{Z} : n \text{ divides } mx\} = \{x \in \mathbb{Z} : mp \text{ divides } mx\} = \{x \in \mathbb{Z} : p \text{ divides } x\} = p\mathbb{Z}$. So $\mathbb{Z}/p\mathbb{Z} \approx m\mathbb{Z}/m\mathbb{Z}$.

Thus $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \approx \mathbb{Z}/d\mathbb{Z}$ where $d = \gcd(m, n)$.

7. *Let p be a prime, A a finite p-group and $\phi \in \mathrm{Aut}(A)$ an automorphism of order p^n for some n. Show that $\phi(a) = a$ for some $a \in A^{\#}$.* (10 pts.)

Proof: Let $G = \langle \phi \rangle$. Then $|G| = p^n$ and G acts on $A^{\#}$. For $a \in A^{\#}$, there is a bijection between the G-orbit Ga of a and the coset space G/G_a where $G_a = \{g \in G : g(a) = a\}$ given by $gG_a \mapsto ga$. Thus $|Ga| = |G/G_a|$ and

$|A^{\#}| = |\sqcup_a\ Ga| = \Sigma_a\ |Ga| = \Sigma_a |G/G_a|$.

If $G_a \neq G$ for all a, then $|G/G_a| = p^i$ for some $i \geq 1$ so that p divides $\Sigma_a |G/G_a| = |A^{\#}| = p^n - 1$, a contradiction. Thus $G_a \neq G$ for some a and for this a, $|Ga| = 1$, i.e. $Ga = \{a\}$ and $\phi(a) = a$.

8. *Let G be a group and $g \in G^{\#}$. Show that there is a subgroup H of G maximal with respect to the property that $g \notin H$.* (10 pts.)

Proof: Let $Z = \{H \leq G : g \notin H\}$. Order Z by inclusion. Since the trivial group $1 \in Z$, $Z \neq \emptyset$. It is easy to show that if $(H_i)_I$ is an increasing chain from Z then $\cup_I H_i \in Z$. Thus Z is an inductive set. By Zorn's Lemma it has a maximal element, say H. Then H is a maximal subgroup of G not containing g.

9. *A group G is called divisible if for every $g \in G$ and $n \in \mathbb{N}/\ \{0\}$ there is an $h \in G$ such that $h^n = g$.*

9a. *Show that a divisible group cannot have a proper subgroup of finite index.* (10 pts.)

Proof: Assume G is divisible. Let $H \leq G$ be a subgroup of finite index, say n. We first prove that G has a normal subgroup K of finite index contained in H.

Claim: *A group G that has a subgroup of index n has a normal subgroup of index dividing $n!$ and contained in H.*

Proof of the Claim. Let G act on the left coset space G/H via $g.(xH) = gxH$. This gives rise to a homomorphism ϕ from G into $\mathrm{Sym}(G/H)$, and the latter is isomorphic to $\mathrm{Sym}(n)$. Thus $\mathrm{Ker}(\phi)$ is a normal subgroup and ϕ gives rise to an embedding of $G/\mathrm{Ker}(\phi)$ into $\mathrm{Sym}(n)$. Thus $|G/\mathrm{Ker}(\phi)|$ dives $n!$ and $\mathrm{Ker}(\phi)$ is a normal subgroup of index dividing $n!$

An easy calculation shows that $\mathrm{Ker}(\phi) = \{g \in G : g(xH) = xH \text{ all } g \in G\} = \cap_{x \in G} H^x \leq H$. This proves the claim.

Let K be the normal subgroup of index m of G. Let $a \in G$. Let $b \in G$ be such that $a = b^m$. Then $a = b^m \in K$ (because the group G/K has order m) and so $G = K$.

9b. *Conclude that a divisible abelian group cannot have a proper subgroup which is maximal with respect to being proper.* (10 pts.)

Proof: Let G be a divisible abelian group. Let $H < G$ be a maximal subgroup

of G. Then G/H has no nontrivial proper subgroups. Thus G/H is generated by any of its nontrivial elements. In particular G/H is cyclic. Since G/H cannot be isomorphic to $\mathbb{Z}$ (because $\mathbb{Z}$ has proper nontrivial subgroups, like $2\mathbb{Z}$), G/H is finite. By the question above $H = G$.

10. *Let G be a group. Let $H \triangleright G$.*

10a. *Assume $\mathbb{Z} \approx H$. Show that $C_G(H)$ has index 1 or 2 in G.* (10 pts.)
Proof: Any element of G gives rise to an automorphism of H (hence of $\mathbb{Z}$) by conjugation. In other words, there is a homomorphism of groups $\phi : G \to \mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z})$ given by $\phi(g)(h) = h^g$ for all $h \in G$. The kernel of ϕ is clearly $C_G(H)$. Thus $G/C_G(H)$ embeds in $\mathrm{Aut}(\mathbb{Z})$. But $\mathbb{Z}$ has only two generators, 1 and -1 and any automorphism of $\mathbb{Z}$ is determined by its impact on 1, which must be 1 or -1. Thus $|\mathrm{Aut}(\mathbb{Z})| = 2$. This proves it.

10b. *Assume H is finite. Show that $\mathrm{C}_G(H)$ has finite index in G.* (5 pts.)
Proof: As above. ϕ is a homomorphism from G into the finite group $\mathrm{Aut}(H)$ and the kernel of this automorphism is $C_G(H)$.

13.2 Basic Algebra I, Final, January 2004 and Its Correction

1. *Let R be a ring with 1. Show that R has a maximal (and proper) ideal.* (5 pts.)

   Proof: Let Z be the set of proper ideals of R. Since the trivial ideal 0 is in Z, Z is nonempty. Order Z by inclusion. If $(I_i)_i$ is an increasing chain from Z, then $\cup_i I_i$ is also in Z since 1 cannot be in $\cup_i I_i$ (this is the important point: 1 exists! Otherwise the statement does ot hold as we will see. Also if $(I_i)_i$ were not a chain, it wouldn't be an ideal), not being in any of the I_i's. Thus Z is an inductive set and by Zorn's Lemma Z has a maximal element. Any maximal element of Z is a maximal ideal of R.

2. **a.** *Let G be an abelian group. Let $H < G$ be a proper maximal subgroup. Show that $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p.* (7 pts.) *Conclude that a divisible abelian group cannot have a maximal proper subgroup.* (7 pts.)

   Proof: Since H is a maximal subgroup, the quotient group G/H does not have a proper nontrivial subgroup. Now the first part of the question follows from the following:

   Claim: *Any group (abelian or not) that does not have a proper nontrivial subgroup is either the trivial group or isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.*

   Proof of the Claim: Let G be such a group. Then for any $g \in G$, $C_G(g) = G$, thus G is abelian. Since $G = \langle g \rangle$ for any $g \in G \setminus \{1\}$, G is cyclic. We cannot have $G \simeq \mathbb{Z}$, since otherwise G would have many

subgroups corresponding to the subgroups $n\mathbb{Z}$, $n > 1$. Thus $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 0$. Assume $n \neq 0$. If p were a proper divisor of n, then $0 < p\mathbb{Z}/n\mathbb{Z} < \mathbb{Z}/n\mathbb{Z}$, a contradiction. Thus n is a prime. This proves the claim and the first part.

Let now G be a divisible abelian group. Let $H < G$ be a maximal subgroup. Then, by the first part, $G/H \simeq \mathbb{Z}/p\mathbb{Z}$ for some (prime) integer p. Let $g \in G$. Let $k \in G$ be such that $k^p = g$. Then in the quotient group G/H, $\overline{g} = \overline{k}^p = 1$, so that $g \in H$. Thus $G = H$.

b. *Conclude from part a that there are rings (necessarily without 1) without maximal ideals.* (5 pts.)

Proof: Let G be any divisible group, e.g. $G = \mathbb{Q}^+$, $\mathbb{R}^+$ or $\mathbb{Z}_{p^\infty}$. Denote G additively. Define multiplication on I by decreeing $gh = 0$ all g, $h \in G$. Then G becomes a ring. An ideal of the ring G corresponds to a subgroup of the group G. Thus G – not having maximal subgroups – does not have maximal ideals.

c. *Let G be a group and $1 \neq a \in G$. Show that G has a subgroup which is maximal with respect to not containing a.* (4 pts.)

Proof: Exactly as in Question 1.

d. *Find a subgroup of $\mathbb{Q}^+$ which is maximal with respect to not containing 1.* (7 pts.)

Solution. Let p be any prime. Consider

$$H := \{a/b : a, b \in \mathbb{Z} \text{ such that } p \text{ divides } a \text{ but not } b\}.$$

Then H is a subgroup of $\mathbb{Q}^+$. Clearly $1 \notin H$ and $p \in H$. We claim that if $H < K \leq G$ then $1 \in K$. This will show that H is a maximal subgroup of $\mathbb{Q}$ not containing 1. Let $\gamma \in K \setminus H$. We can write $\gamma = c/d$ for some c, $d \in \mathbb{Z}$ with $(c, p) = 1$. There are x, $y \in \mathbb{Z}$ such that $cx + yp = 1$. Thus $1 = (dx)\gamma + yp \in \langle \gamma, H \rangle \leq K$.

3. *Let $R = X\mathbb{R}[X]$ considered as a ring (without 1). Let $I = X^2\mathbb{R}[X] \lhd X\mathbb{R}[X]$.*

a. *Show that R/I as an additive group is isomorphic to $\mathbb{R}^+$ and that the multiplication of R/I is the zero-multiplication (i.e. the product of any two elements of R/I is zero).* (3 pts.)

Proof: Consider the map $\phi : \mathbb{R} \longrightarrow R/I$ given by $\phi(a) = \overline{aX}$. This is certainly a homomorphism of additive groups.

ϕ is onto because for any $f(X) = f_0 + f_1X + ... + f_nX^n$, $\phi(f_0) = \overline{Xf(X)}$.

ϕ is one-to-one because if $a \in \ker(\phi)$, i.e. if $\phi(a) = \overline{0}$ then $\overline{aX} = \overline{0}$ and the second degree polynomial X^2 divides the first degree polynomial aX, which implies that $aX = 0$ and $a = 0$.

For the multiplication in R/I: Given any $\overline{Xf(X)}$, $\overline{Xg(X)} \in R/I$, we have $\overline{Xf(X)Xg(X)} = \overline{X^2 f(X)g(X)} = \overline{0}$.

b. *Conclude that R/I has no maximal ideals.* (4 pts.)

By part a, instead of R/I we may just consider the ring $\mathbb{R}$ with the usual addition and the zero multiplication. By the solution of part b of Question 2, $\mathbb{R}$ has no maximal ideals.

c. *Conclude that R has no maximal ideals.* (8 pts.)

Proof: Note first that I is not a maximal ideal of R (because otherwise $\overline{0}$ would be a maximal ideal of R/I, contradicting part b.

Let J be a maximal ideal of R. Since $(I+J)/I \lhd R/I$, either $I+J=I$ or $I+J=R$. In the first case $J \leq I$, making I a maximal ideal, a contradiction. Assume $I+J=R$.

I do not know how to continue... The question seems to be open for the moment. Does R have a maximal ideal? Is a maximal ideal of R that does not contain X a maximal ideal of R?

4. *Let $R = \mathbb{Z}[\sqrt{d}]$ where $d \neq 0, 1$ is a square-free element of $\mathbb{Z}$.*

a. *Show that the map $- : R \longrightarrow R$ defined by $\overline{a+b\sqrt{d}} = a - b\sqrt{d}$ for all $a, b \in \mathbb{Z}$ is a ring automorphism.* (2 pts.)

Proof: This is easy to show. We need to compute to check that $\overline{\alpha}+\overline{\beta} = \overline{\alpha+\beta}$, $\overline{\alpha}\,\overline{\beta} = \overline{\alpha\beta}$ for all $\alpha, \beta \in R$. The facts that the map $-$ is onto and one-to-one is trivial.

b. *For $\alpha \in R$, let $N(\alpha) = \alpha\overline{\alpha}$. Show that $N(\alpha) \in \mathbb{Z}$ and that $N : R \longrightarrow \mathbb{Z}$ is multiplicative.* (2 pts.)

Proof: Since, for $a, b \in \mathbb{Z}$ and $\alpha = a + b\sqrt{d}$, $N(\alpha) = (a+b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$, $N(\alpha) \in \mathbb{Z}$. Also, for any $\alpha\beta \in R$, $N(\alpha\beta) = (\alpha\beta)\overline{\alpha\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$.

c. *For $\alpha \in R$, show that $\alpha \in R^*$ if and only if $N(\alpha) = \pm 1$.* (5 pts.)

Proof: If $\alpha \in R^*$, then there is a $\beta \in R$ such that $\alpha\beta = 1$. Thus $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $N(\alpha)$, $N(\beta) \in \mathbb{Z}$, this implies that $N(\alpha) = N(\beta) = \pm 1$.

Conversely, assume $N(\alpha) = \pm 1$. Then $(N(\alpha)\overline{\alpha})\alpha = N(\alpha)^2 = 1$ so that $N(\alpha)\overline{\alpha}$ is the inverse of α.

d. *For $\alpha \in R$, show that if $N(\alpha)$ is prime then α is irreducible.* (3 pts.)

Proof: Assume $N(\alpha)$ is prime. Let $\alpha = \beta\gamma$ where $\beta, \gamma \in R$. Then $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Since $N(\alpha)$ is prime, this implies that either $N(\beta)$ or $N(\gamma)$ is ± 1, i.e. either β or γ is invertible. Hence α is irreducible.

e. *Assume $d < -1$. Find R^*.* (3 pts.)

By part c, $R^* = \{\alpha \in R : N(\alpha) = \pm 1\}$. But $N(\alpha) = a^2 - db^2 = a^2 + |d|b^2$ for $\alpha = a + b\sqrt{d}$ and $a, b \in \mathbb{Z}$. So $N(\alpha) \geq |d| > 1$ if $b \neq 0$. Thus $R^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

f. *Assume $d = -1$. Find R^* and its group structure.* (5 pts.)

Proof: By part c, $R^* = \{a+b\sqrt{-1} : a, b \in \mathbb{Z}\ a^2+b^2 = 1\} = \{1, -1, i, -i\}$ where $i^2 = -1$. Since i has order 4, $R^* \simeq \mathbb{Z}/4\mathbb{Z}$.

e. *Show that the map $\_ : R \longrightarrow R$ defined above is the only nontrivial ring automorphism of R.* (5 pts.)

Proof: Any automorphism must be trivial on $\mathbb{Z}$, as usual. Thus it is enough to find the image of $\sqrt{d}$. Let $x = \sqrt{d}$. Then $x^2 = d$ and so $\phi(x)^2 = \phi(x^2) = \phi(d) = d$, hence $\phi(x) = \pm\sqrt{d}$.

5. *Let G be a finite abelian group. Show that if any p-subgroup of G is cyclic for any prime p then G is cyclic itself.* (5 pts.)

   Proof: G is the direct sum of its primary parts, which are all cyclic. We know that the product of finitely many cyclic groups of order two by two prime to each other is a cyclic group. (For this, it is enough to prove that if $(n, m) = 1$, then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/nm\mathbb{Z}$).

6. *Show that if $r \leq s$ then $X^{p^r} - 1$ divides $X^{p^s} - 1$.* (3 pts.)

   Proof: Let $s = r + t$ and $Y = X^{p^r}$. Then $X^{p^s} = X^{p^{r+t}} = X^{p^r p^s} = (X^{p^r})^{p^t} = Y^{p^t}$. Thus we need to show that $Y - 1$ divides $Y^{p^t} - 1$, but $Y - 1$ always divides $Y^n - 1$.

7. *Show that if F_1 and F_2 are two finite subfields of a field K of the same cardinality then $F_1 = F_2$.* (5 pts.)

   Proof: Say $|F_1| = |F_2| = n$. Then F_1^* and F_2^* are groups of order $n - 1$. Hence, for any $x \in F_1^* \cup F_2^*$, $x^{n-1} = 1$. It follows that for any $x \in F_1 \cup F_2$, $x^n = x$. Hence the elements of $F_1 \cup F_2$ are the roots of the polynomial $X^n - X$. But this polynomial has at most n roots. So $F_1 = F_2 = \{x \in K : x^n = x\}$. (In reality n is a prime power).

8. *Show that a finite subgroup of a field is cyclic.* (15 pts.)

   Proof: Let F be a field and G be a finite group of F^*. By decomposing G into its primary parts, we may assume that G is a p-group for some prime p. (Direct sum of finitely many cyclic groups whose orders are two by two relatively prime to each other is cyclic). Since any finite abelian p-group, for p prime, is a direct sum of cyclic p-subgroups, it is enough to show that G cannot be of the form $\mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}$ for some m, $n \geq 1$. Assume not. Then $\{x \in F : x^p = 1\}$ has at least $p^2 - 1$ elements, so the polynomial $X^p - 1$ has at least $p^2 - 1$ roots in the field F, more than p, a contradiction.

9. *Conclude from Question 8 that if $F \leq K$ are finite fields then $K = F[\alpha]$ for some $\alpha \in K$.* (3 pts.)

   Proof: Since K^* is a cyclic group, there is an $a \in K^*$ such that $K^* = \langle \alpha \rangle$. Then $K = F[\alpha]$ of course.

13.3 Basic Algebra II First Midterm May 2003

K stands for a field.

1. Let K be a finite field. Show that K has p^n elements for some prime p and some natural number n. (5 pts.)

2. Find all ideals of $K \times \ldots \times K$. (5 pts.)

3. Let R be a commutative ring with 1 and $I \lhd R$. Show that I is a maximal ideal if and only if R/I is a field. (5 pts.)

4. Let K be a field with a valuation v. Recall that this means that v is a map from K into $\mathbb{Z} \cup \{\infty\}$ such that for all $x, y \in K$,

   $v(x) = \infty$ if and only if $x = 0$,

   $v(x + y) \geq \min(v(x), v(y))$,

   $v(xy) = v(x) + v(y)$.

5. Show that if $v(x) \neq v(y)$, then $v(x + y) = \min(v(x), v(y))$. (10 pts.)

6. Let R be a domain containing a field K. Then R is a vector space over K. Assume that $\dim_K(R) < \infty$.

   a) Show that R is a field.

   b) Show that for every $r \in R$ there is an irreducible polynomial $p(X) \in K[X]$ such that $p(r) = 0$. (20 pts.)

   After that I classified all finite dimensional central $\mathbb{R}$-algebras, not as difficult as it seems: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.

7. Let K be a field and X a set. Let R be the ring of all functions from X into K. Find a maximal ideal of R. (5 pts.)

8. Show that, except for $p = 2$, $\mathbb{Z}_p$ has no elements satisfying $x^p = 1$. (10 pts.)

9. Let R be a commutative ring. Let I be a maximal ideal of $R[X]$. Is $R \cap I$ necessarily a prime ideal of R? (10 pts.)

10. Find all two-sided ideals of $\mathrm{Mat}_{2\times 2}(K)$. (10 pts.)

11. Find all the ring automorphisms of $K[X]$. (20 pts.)

13.4 Basic Algebra II Final, May 2003

1. Find all ring homomorphisms from $\mathbb{C}^n$ onto $\mathbb{C}$. (The ring structure on $\mathbb{C}^n$ is componentwise).

2. Show that the additive group of a commutative ring with identity cannot be isomorphic to the additive group $\mathbb{Q}/\mathbb{Z}$.

3. Let R be a principal ideal domain. And let I and J be nonzero ideals of R. Show that $IJ = I \cap J$ if and only if $I + J = R$.

4. Is the ideal of $\mathbb{Z}[X]$ generated by $X^3 + X + 1$ prime?

5. Let I be an ideal and S be a subring of the ring R. Prove that $I \cap S$ is an ideal of S. Give an example to show that every ideal of S need not be of the form $I \cap S$ for some ideal I of R.

6. Let R be a commutative ring and P be a maximal ideal of R. Let $I = P[X]$ be the ideal of the polynomial ring $R[X]$ consisting of the polynomials in $R[X]$ with coefficients in P. Show that I is a nonmaximal prime ideal.

7. Let R be a commutative ring with identity. Let $f(X) = a_0 + a_1X + \ldots + a_nX^n \in R[X]$. Prove that $f(X)$ is unit if and only if a_0 is a unit in R and a_i is nilpotent for all $i > 0$.

8. Suppose A and B are finitely generated R-modules where R is a principal ideal domain. Show that if $A \oplus A \simeq B \oplus B$, then $A \simeq B$.

9. Suppose A is a finitely generated R-module where R is a principal ideal domain. If $A \oplus A \simeq A$, show that $A = 0$.

Chapter 14

Rings of Matrices

Let R be a ring with 1. We consider the additive abelian group R^n (with the componentwise addition). For $r \in R$ and $v = (r_1, \ldots, r_n) \in R^n$, we let

$$r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n).$$

We call this last multiplication, **multiplication by a scalar**. In this section, we will forget the ring structure on R^n defined in the previous section and we will only care about the addition on R^n and the multiplication by a scalar as defined just above.

Now we consider the additive group homomorphisms $\phi : R^n \longrightarrow R^m$ such that $\phi(rv) = r\phi(v)$ for all $r \in R$ and $v \in R^n$. We denote the set of such homomorphisms by $\mathrm{Hom}_R(R^n, R^m)$. It is clear that $\mathrm{Hom}_R(R^n, R^m)$. It can also be checked that if $\phi \in \mathrm{Hom}_R(R^n, R^m)$ and $\psi \in \mathrm{Hom}_R(R^m, R^p)$, then $\psi \circ \phi \in \mathrm{Hom}_R(R^n, R^p)$.

Lemma 14.0.1 *The set* $\mathrm{End}_R(R^n) := \mathrm{Hom}_R(R^n, R^n)$ *is an associative ring with identity.*

Proof: Left as an exercise. □

Now we will describe the elements of $\mathrm{Hom}_R(R^n, R^m)$ in terms of the elements of R.

Consider the n elements

$$\begin{array}{c}(1, 0, 0 \ldots, 0, 0)\\(0, 1, 0, \ldots, 0, 0)\\ \ldots\\(0, 0, 0, \ldots, 0, 1)\end{array}$$

of R^n. This set of elements of R^n is called the **canonical basis** of R^n. Denote them by $e_1, \ldots, e_n$. The canonical basis $e_1, \ldots, e_n$ has the following property,

for any $v \in R^n$, there are unique $r_1, \ldots, r_n \in R$ such that $v = r_1e_1 + \ldots + r_ne_n$.

Indeed, if $v = (r_1, \ldots, r_n)$, then $v = r_1 e_1 + \ldots + r_n e_n$.

Note that there may be other sets of elements that have the same property. But the canonical basis is considered to be a special one. Let $f_1, \ldots, f_m$ be the canonical basis of R^m.

Now let $\phi \in \mathrm{Hom}_R(R^n, R^m)$. Let $v = (r_1, \ldots, r_n) \in R^n$. Then $\phi(v) = \phi(r_1 e_1 + \ldots + r_n e_n) = r_1\phi(e_1) + \ldots + r_n\phi(e_n)$. Thus if we know $\phi(e_1), \ldots, \phi(e_n)$, then we know ϕ. In other words ϕ is determined by the n elements $\phi(e_1), \ldots, \phi(e_n)$ of R^m. And each element of R^m is given by an m-tuple of elements of R. Write,

$$\begin{array}{rcl} \phi(e_1) & = & (\phi_{11}, \ldots, \phi_{m1}) \\ \phi(e_2) & = & (\phi_{12}, \ldots, \phi_{m2}) \\ & & \ldots \\ \phi(e_j) & = & (\phi_{1j}, \ldots, \phi_{mj}) \\ & & \ldots \\ \phi(e_n) & = & (\phi_{1n}, \ldots, \phi_{mn}) \end{array}$$

Thus any $\phi \in \mathrm{Hom}_R(R^n, R^m)$ gives rise to an nm-tuple

$$(\phi_{ij})_{i=1,\ldots,m;\ j=1,\ldots,n} \in R^{nm}.$$

Conversely, any mn-tuple $(\phi_{ij})_{i=1,\ldots,m;\ j=1,\ldots,n} \in R^{nm}$ determines a homomorphism $\phi \in \mathrm{Hom}_R(R^n, R^m)$. We write the mn-tuple $(\phi_{ij})_{i=1,\ldots,m;\ j=1,\ldots,n}$ in the following way:

$$\begin{pmatrix} \phi_{11} & \phi_{12} & \ldots & \phi_{1j} & \ldots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \ldots & \phi_{2j} & \ldots & \phi_{2n} \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \phi_{i1} & \phi_{i2} & \ldots & \phi_{ij} & \ldots & \phi_{in} \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ \phi_{m1} & \phi_{m2} & \ldots & \phi_{mj} & \ldots & \phi_{mn} \end{pmatrix}$$

Such an object is called an $(m \times n)$**-matrix**. The set of $(m \times n)$-matrices with coefficients in R is denoted by $\mathrm{Mat}_{m\times n}(R)$.

Note that, as a set, $\mathrm{Mat}_{m\times n}(R)$ is just R^{mn}.

Thus there is a bijection, let us call it M, from $\mathrm{Hom}(R^n, R^m)$ into $\mathrm{Mat}_{m\times n}(R)$.

Note that, for $\phi \in \mathrm{Hom}(R^n, R^m)$, the j-th column of the matrix $\Theta(\phi)$ is the entries of $\phi(e_j)$.

Now we carry the addition, the scalar multiplication and the composition when possible. of

Part III

Basic Field Theory

Let $F \supseteq K$ be an algebraic extension of fields and let R be a subring of F with $R \supseteq K$. Show that R is a field.

Part IV

Basic Module Theory

Chapter 15

Finitely Generated Torsion Modules over PIDs

Part V

Basic Linear Algebra

Part VI

Intermediate Group Theory

Chapter 16

Commutator Subgroups

Exercises.

1. Show that if $H, K \leq G$, then H and K normalize the subgroup $[H, K]$. (Hint: See Exercise 14, page 14).

2. Show that if $A \leq G$ is an abelian subgroup and if $g \in N_G(A)$, then the map $\mathrm{ad}(g) : A \longrightarrow A$ given by $\mathrm{ad}(g)(a) = [g, a] := g^{-1}a^{-1}ga$ is a group homomorphism whose kernel is $C_A(g)$. (Hint: See Exercise 1, page 109).

Chapter 17

Cauchy's Theorem

Theorem 17.0.2 (Cauchy's Theorem) *Let G be a finite group whose order is divisible by the prime p. Then G has an element of order p.*

Chapter 18

Sylow Theory

Theorem 18.0.3 (Sylow Theory) *Let G be a finite group and p a prime. Assume $|G| = p^n m$ where m and p are prime to each other. Then G has subgroups of order p^n (called* **Sylow p-subgroups** *of G). Furthermore*

i. The Sylow p-subgroups are conjugate to each other.

ii. Any p-subgroup of G is in some Sylow p-subgroup of G.

iii. The number of Sylow p-subgroups divides m and is 1 modulo p.

Proof: (See Lemma 28.0.13 for groups acting on sets). Let $\wp$ be the set of maximal p-subgroups. The group G acts on the set $\wp$ by conjugation. For $P, Q \in \wp$, $|P^Q| = |Q/N_Q(P)|$. Hence $|P^Q| = 1$ if and only if $P = Q$, and if $P \neq Q$ then p divides $|P^Q|$. Let $\emptyset \neq \wp_1 \subset \wp$ be a G-stable subset, and let $P \in \wp_1$, $Q \in \wp \setminus \wp_1$. By counting the P-orbits in $\wp_1$ we see that $|\wp_1| \equiv 1$ modulo p. By counting the Q-orbits in $\wp_1$ we see that p divides $|\wp_1|$, a contradiction. Thus there is only one G-conjugacy class in $\wp$. This proves that the maximal p-subgroups of G are conjugate to each other. Thus $\wp = P^G$ some $P \in \wp$ (so $|\wp| \equiv 1$ modulo p) and $|\wp| = |G/N_G(P)|$ (thus p^n divides $|N_G(P)|$ and $|\wp|$ divides m). Since $N_G(P)/P$ is a $p^\perp$-group, p^n divides $|P|$ and so $|P| = p^n$.

If H is a p-subgroup, by letting H act on $\wp$ and counting the H-orbits, we see that H must fix (i.e. normalize) a $P \in \wp$. Then $H \leq P$. □

Exercises.

1. Find the number of Sylow 3-subgroups and the number of Sylow 5-subgroups of the symmetric group Sym(5).

2. Let G be a group of order $165 = 3 \cdot 5 \cdot 11$. Show that

   a) G has a normal Sylow 11-subgroup, say C.

   b) G/C is cyclic. (HINT: Show that every group of order 15 is cyclic.)

   c) G has normal subgroups of orders 33 and 55.

3. Let $H \leq G$ and P a Sylow p-subgroup of G. Show that for some $g \in G$, $P^g \cap H$ is a Sylow p-subgroup of H. By considering Sym(4), show that we may not be able to choose $g \in H$.

4. Let G be a finite group and $H \lhd G$. If $P \leq G$ is a Sylow p-subgroup of G, then $P \cap H$ is a Sylow p-subgroup of H and all Sylow p-subgroup of H arise in this way.

Chapter 19

Semidirect Products

Let U and T be two groups and let $\phi : T \longrightarrow \mathrm{Aut}(U)$, $t \longmapsto \phi_t$ be a group homomorphism. We will construct a new group denoted by $U \rtimes_\phi T$, or just by $U \rtimes T$ for short. The set on which the group operation is defined is the Cartesian product $U \times T$, and the operation is defined as follows:

$$(u,t)(u',t') = (u \cdot \phi_t(u'),\, tt').$$

The reader will have no difficulty in checking that this is a group with $(1,1)$ as the identity element. The inverse is given by the rule:

$$(u,t)^{-1} = (\phi_{t^{-1}}(u^{-1}),\, t^{-1}).$$

Let G denote this group. G is called the *semidirect product* of U and T (in this order; we also omit to mention ϕ). U can be identified with $U \times \{1\}$ and hence can be regarded as a normal subgroup of G. T can be identified with $\{1\} \times T$ and can be regarded as a subgroup of G. Then the subgroups U and T of G have the following properties: $U \lhd G$, $T \leq G$, $U \cap T = 1$ and $G = \mathrm{UT}$.

Conversely, whenever a group G has subgroups U and T satisfying these properties, G is isomorphic to a semidirect product $U \rtimes_\phi T$ where $\phi : T \longrightarrow \mathrm{Aut}(U)$ is given by $\phi_t(u) = tut^{-1}$.

When $G = U \rtimes T$, one says that the group G is *split*[1]; then the subgroups U and T are called each other's **complements**. We also say that T (or U) splits in G. Note that T is not the only complement of U in G: for example, any conjugate of T is still a complement of U.

When the subgroup U is abelian, it is customary to denote the group operation of U additively. In this case, it is suggestive to let $tu = \phi_t(u)$. Then the group operation can be written as:

$$(u,t)(u',t') = (tu' + u,\, tt').$$

[1]This is an abuse of language: every group G is split, for example as $G = G \rtimes \{1\}$. When we use the term "split", we have either U or T around.

¶ One should compare this with the following formal matrix multiplication:

$$\begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t' & u' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} tt' & tu'+u \\ 0 & 1 \end{pmatrix}.$$

Examples.

1. ¶ Let V be a vector space and $\mathrm{GL}(V)$ be the group of all vector space automorphisms of V. The group $V \rtimes \mathrm{GL}(V)$ (where $\phi = \mathrm{Id}$) is a subgroup of $Sym(V)$ as follows: $(v, g)(w) = gw + v$.
2. ¶ The subgroup $B_n(K)$ that consists of all the invertible $n \times n$ upper triangular matrices over a field K is the semidirect product of $\mathrm{UT}_n(K)$ (upper-triangular matrices with ones on the diagonal) and $T_n(K)$ (invertible diagonal matrices).

Exercises.

1. ¶ Let K be any field. Show that the group
$$G = \left\{ \begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix} : t \in K^*, u \in K \right\}$$
is a semidirect product of the form $G' \rtimes T$ for some subgroup T. This group is called the **affine group**.
2. Let $G = U \rtimes T$.
   a. Let $U \leq H \leq G$. Show that $H = U \rtimes (H \cap T)$.
   b. Let $T \leq H \leq G$. Show that $H = (U \cap H) \rtimes T$.
   c. Show that if T is abelian then $G' \leq U$.
   d. Show that if $T_1 \leq T$, then $N_U(T_1) = C_U(T_1)$.
3. Let $G = U \rtimes T$. Let $t \in T$ and $x \in U$. Show that xt is G-conjugate to an element of T if and only if xt is conjugate to t if and only $(xt)^u = t$ for some $u \in U$ if and only if $x \in [U, t^{-1}]$.
4. Let $G = U \rtimes T$ and let $V \leq U$ be a G- normal subgroup of U. Show that $G/V \simeq U/V \rtimes T$ in a natural way.
5. Let $G = U \rtimes T$ and let $V \leq U$ be a G- normal subgroup of U. By Exercise 4, $G/V \simeq U/V \rtimes T$. Let $t \in T$ be such that $V = \mathrm{ad}(t)(V)$ and $U/V = \mathrm{ad}(t)(U/V)$. Show that $U = \mathrm{ad}(t)(U)$. (Here $\mathrm{ad}(t)(v) = [t, v]$).
6. ¶ Let K be a field and let n be a positive integer. For $t \in K^*$ and $x \in K$, let $\phi_t(x) = t^n x$. Set $G = K^+ \rtimes_\phi K^*$. What is the center of G? Show that $Z_2(G) = Z(G)$. What is the condition on K that insures $G' \simeq K^+$? Show that G is isomorphic to a subgroup of $\mathrm{GL}_2(K)$.

Lemma 19.0.4 *Let G be a group and A a normal subgroup of G. Assume G/A is cyclic of order n and A is torsion without elements of order p for any divisor p of n. Then $G = A \rtimes H$ for some subgroup H of G.*

Chapter 20

Solvable Groups

Throughout this subsection G denotes a group. If $x, y \in G$ and n any integer (even a negative one), we let $x^{ny} = y^{-1}x^n y$ and $[x,\, y] = x^{-1}y^{-1}xy$. In particular $x^{-y} = y^{-1}x^{-1}y$. An element of the form $[x, y]$ is called a **commutator**. If $X, Y \leq G$ are two subsets of G, $[X, Y]$ denotes the subgroup generated by the set $\{[x, y] : x \in X,\, y \in Y\}$. Since $[x, y] = [y, x]^{-1}$, $[X, Y] = [Y, X]$.

Clearly, if H and K are normal subgroups of G, then $[H, K]$ is also a normal subgroup of G. Exercise 2.a below will show that the subgroup $[H, K]$ is normalized by H and K, and therefore by $\langle H, K\rangle$. However it is not always true that if $H,\, K \leq G$ and $H \lhd G$, then $[H, K] \lhd G$. As an example, let $G = \mathrm{GL}_2(K) \rtimes K^2$ with the natural action. Let $H = K^2 \lhd G$ and K be the set of strictly lower triangular matrices of $\mathrm{GL}_2(K)$. Then one can check easily that $[H, K]$ is (one dimensional and) not normal in G.

The subgroups G^n and $G^{(n)}$ are defined inductively:

$$G^0 = G^{(0)} = G, \quad G^1 = G^{(1)} = [G,\, G],$$
$$G^{n+1} = [G^n,\, G], \quad G^{(n+1)} = [G^{(n)},\, G^{(n)}].$$

Lemma 20.0.5 *G^n and $G^{(n)}$ are* **characteristic** *subgroups of G, i.e. they are invariant under the automorphisms of G.*

The subgroup G^1 is denoted by G' and is called the **derived subgroup** or the **commutator subgroup** of G.

Lemma 20.0.6 *$G' \leq H \leq G$ if and only if $H \lhd G$ and G/H is abelian. In other words, G' is the smallest normal subgroup H of G such that G/H is abelian.*

The subgroup G^2 is also denoted by G'' sometimes. A group G is called **solvable** if $G^{(n)} = 1$ for some n. The smallest such n is called the **solvability class** of G. A group G is said to be **nilpotent** if $G^n = 1$ for some n. Again, the smallest such n is called the **nilpotency class** of G.

For an integer n, we define $Z_n(G)$ inductively. The subgroup $Z_\circ(G)$ is defined to be $\{1\}$ and $Z_{n+1}(G) = \{g \in G :\ [g, G] \leq Z_n(G)\}$. The subgroup $Z_1(G)$ is

also denoted by $Z(G)$; it is the set of elements that commute with every element of G and is called the **center** of G. An element or a subgroup is called **central** if it is in the center of G. It immediately follows (by induction) from the definition that $Z_n(G) \lhd Z_{n+1}(G) \lhd G$ and that $Z_{n+1}(G)/Z_n(G)$ is the center of $G/Z_n(G)$.

Exercises. Throughout the exercises G is a group. We let $Z_i = Z_i(G)$ and $Z = Z(G)$.

1. Show that for x, $y \in G$ and n a positive integer,

$$[x^n, y] = [x, y]^{x^{n-1}} [x, y]^{x^{n-2}} \cdots [x, y].$$

2. **a.** Show that for $x, y, z \in G$, $[x, yz] = [x, z][x, y]^z$ and $[xy, z] = [x, z]^y[y, z]$. Conclude that if $H, K \leq G$, then H and K normalize the subgroup $[H, K]$. Conclude also that if $A \leq G$ is an abelian subgroup and if $g \in N_G(A)$, then $\mathrm{ad}(g) : A \longrightarrow A$ is a group homomorphism whose kernel is $C_A(g)$. (Here $\mathrm{ad}(t)(v) = [t, v]$).

   b. Let $x, y, z \in G$. Show that

$$[[x, y^{-1}], z]^y [[y, z^{-1}], x]^z [[z, x^{-1}], y]^x = 1.$$

   Conclude that if H and K are two subgroups of a group G and if $[[H, K], K] = 1$, then $[H, K'] = 1$.

   c. Three Subgroup Lemma of P. Hall. Let H, K, L be three normal subgroups of G. Using part b, show that

$$[[H, K], L] \leq [[K, L], H][[L, H], K].$$

   d. Conclude from part (c) that $[G^i, G^j] \leq G^{i+j+1}$, $G^{(i)} \leq G^{2^i-1}$, $[G^i, Z_j] \leq Z_{j-i-1}$, $[Z_{i+1}, G^i] = 1$.

   e. Show that a nilpotent group is solvable. Show that the converse of this statement is false.

3. **a.** Let G be nilpotent of class n. Show that $G^{n-i} \leq Z_i$. Conclude that $G = Z_n$.

   b. Conversely, assume that $G = Z_n$. Show that $G^i \leq Z_{n-i}$. Conclude that G is nilpotent of class $\leq n$.

   c. Show that G is nilpotent of class n if and only if $Z_n = G$ and $Z_{n-1} \neq G$.

4. Let $H \lhd G$ and K, $L \leq G$.

   a. Show that $[KH/H,\ LH/H] = [K, L]H/H$.

   b. Conclude that if G is solvable (resp. nilpotent), then so are H and G/H.

   c. Show that if G/H and H are solvable, then so is G.

d. Find an example where the previous result fails if we replace the word "solvable" by "nilpotent".

e. Deduce from part c that if A and B are solvable subgroups of G and if one of them normalizes the other, then $\langle A, B\rangle = AB$ is also solvable.

5. Let $X \leq Z_n(G)$ be a normal subgroup of G. Show that G is nilpotent if and only if G/X is. Let i be fixed integer. Show that G is nilpotent of class n if and only if G/Z_i is nilpotent of class $n-i$. Show that Z_i is nilpotent of class $\leq i$. Find a (nilpotent) group where $Z_2 \neq Z$ and Z_2 is abelian.

6. **a.** Show that the subgroup G^n is generated by the elements of the form $[x_1, [x_2, \ldots, [x_n, x_{n+1}]\ldots]]$, where $x_i \in G$. Find a similar statement for $G^{(n)}$.

7. ¶ Let K be a field. By Exercise 20.0.6, $\mathrm{GL}_n(K)' \leq \mathrm{SL}_n(K)$. Show that if $K \neq \mathbb{F}_2, \mathbb{F}_3$, $\mathrm{GL}_2(K)' = \mathrm{SL}_2(K)$. Find $\mathrm{GL}_2(\mathbb{F}_2)'$ and $\mathrm{GL}_2(\mathbb{F}_3)'$.

8. ¶ The prototype of solvable groups is the group $B_n(K)$ of $n \times n$ invertible upper-triangular matrices over some fixed field $K \neq \mathbb{F}_2$. Show that $B_n(K)$ is solvable of class $\leq n$. (But not necessarily of class n, for example $B_4(K)$ is solvable of class 3).

9. ¶ Find the solvability class of $B_n(K)$.

10. ¶ Consider the group $\mathrm{UT}_n(K)$ of **strictly upper-triangular** (or **unitriangular**) $n \times n$ matrices (i.e. with ones on the diagonal). Show that it is a nilpotent group of class $n-1$.

Chapter 21

Nilpotent Groups

21.1 p-Groups

Let p be a prime. A **p-element** of a group is an element whose order is a p-th power. A group is called a **p-group** if all its elements are p-elements.

Lemma 21.1.1 *If H, $K \leq G$ are p-subgroups such that $K \leq N_G(H)$, then HK is a p-group.*

Lemma 21.1.2 *A finite p-group has nontrivial center. (Corollary 28.0.14)*

Corollary 21.1.3 *A finite p-group is nilpotent.*

Proposition 21.1.4 *A finite p-group is nilpotent.*

Proposition 21.1.5 *A group of order p^k is nilpotent of class $\leq k$.*

Proposition 21.1.6 *Let A be a locally finite p-group and G a finite p-group of automorphisms of A. Then $C_A(G) \neq 1$, thus $Z(A \rtimes G) \neq 1$.*

Exercises.

1. ¶ Let V be a vector space over a field of characteristic p. Let $\sigma \in \mathrm{GL}(V)$ be a p-element of order p^k say. Then $V \rtimes \langle\sigma\rangle$ is a nilpotent group of class $\leq p^k + 1$.

2. Let $A = \mathbb{Z}_{2^\infty}$ and $\sigma \in \mathrm{Aut}(\mathbb{Z}_{2^\infty})$ be the inversion. Then $G := \mathbb{Z}_{2^\infty} \rtimes \langle\sigma\rangle$ is solvable of class 2 and nonnilpotent. Furthermore $\mathbb{Z}/2^n\mathbb{Z} \simeq Z_n(G) \leq \mathbb{Z}_{2^\infty}$.

3. Let $A = (\mathbb{Z}/p\mathbb{Z})^n$. Find all involutions $\sigma \in \mathrm{Aut}(A)$ such that $A \rtimes \langle\sigma\rangle$ is nilpotent of class 2 (and p). How many of them are nonisomorphic?

4. **(Normalizer Condition)** Show that a nilpotent group G satisfies the *normalizer condition* (i.e. if $H < G$ then $H < N_G(H)$).

5. Let G be a nilpotent group. Show that if $1 \neq H \lhd G$, then $H \cap Z \neq 1$.

6. Let A and B be two normal nilpotent subgroups of G. Show that the subgroup $\langle A, B\rangle = AB$ is also normal and nilpotent.

7. **a.** Let $g \in G$ and $H \leq G$ be such that $[g, H] \subseteq Z$. Show that the map $\mathrm{ad}(g) : H \longrightarrow Z$ given by $\mathrm{ad}(g)(x) = [g, x]$ is a group homomorphism. (Here $\mathrm{ad}(t)(v) = [t, v]$). Show that for all $h \in H$, $n \in Z$, $[g, h]^n = [g^n, h] = [g, h^n]$.

   b. Using Exercise 1, show that if $z \in Z_2$ and $z^n \in Z$, then $[z, G]$ is a central subgroup of finite exponent and that $\exp([z, G])$ divides n.

   c. Use part b to prove, by induction on the nilpotency class, that if a nilpotent group has an element of order p where p is a prime, then it has central elements of order p.

   d. Let G be a nilpotent group and D a p-divisible subgroup of G. Show that D commutes with all the p-elements of G. Deduce that in a divisible nilpotent group, elements of finite order form a central subgroup.

8. **(p-Divisible Nilpotent Groups.)** Let p be a prime and let G be a p-divisible nilpotent group.

   a. Show that if $g^p \in Z$, then $g \in Z$.

   b. Conclude that Z is p-divisible, contains all the p-elements and that G/Z is p-torsion-free and p-divisible.

   c. Show that G/Z_i is p-torsion-free for all $i \geq 1$.

   d. Conclude that Z_{i+1}/Z_i is p-torsion-free and p-divisible for $i \geq 1$.

9. **(p-Divisible Nilpotent Groups)** Let G be a nilpotent group.

   a. Let $i \geq 1$ be an integer. Show that G/G^i is p-divisible if and only if G/G^{i+1} is p-divisible.

   b. Conclude that G is p-divisible if and only if G/G' is p-divisible.

   c. Show that G has a unique maximal p-divisible subgroup D.

   d. Assume that for some $D \lhd G$, D and G/D are p-divisible. Show that G is p-divisible.

10. **(Nilpotent Groups of Bounded Exponent)** Let G be nilpotent and assume that $\exp(G/G') = n$.

    a. Show that $\exp(G^i/G^{i+1})|n$ for all i.

    b. Conclude that $\exp(G)|n^c$ where c is the nilpotency class of G.

11. **(Sylow p-Subgroup of Nilpotent Groups)** Let P be a Sylow p-subgroup of a nilpotent group G. Show that P is characteristic in $N_G(P)$. Conclude that $N_G(N_G(P)) = N_G(P)$. By Exercise 4, if G is nilpotent, $N_G(P) = G$, i.e. $P \lhd G$.

Conclude that, for a given prime p, a nilpotent group G has a unique Sylow p-subgroup, and that if G is torsion, then G is the direct sum of its Sylow p-subgroups.

Chapter 22

Sym(X) Revisited

22.1 Alt(n)

Odd and even permutations...

Exercises.

1. If a subgroup G of the symmetric group S_n contains an odd permutation, then $|G|$ is even and exactly half the elements of G are odd permutations.

22.2 Conjugacy Classes

Proposition 22.2.1 *Let G be a group, $a \in G$, $G/C_G(a)$ the right coset space. Then the map $C_G(a)g \longrightarrow a^g$ is a bijection between $G/C_G(a)$ and a^G.*

Proof: By question 3, we may assume that $G/C_G(a)$ stands for the right coset space $\{C_G(a)g : g \in G\}$. It is easy to check that the map $C_G(a)g \mapsto a^g$ is a well-defined bijection between $G/C_G(a)$ and a^G. □

Theorem 22.2.2 *Two elements of* Sym(X) *are conjugate if and only if they have the same cycle type.*

Proof: Suppose α and β have the same cycle structures. Write α and β as the product of disjoint cycles one under another in such a way that the cycles of the same length are one on top of another:

$$\alpha = (\dots a_1\, a_2\, a_3 \dots) \dots$$

$$\beta = (\dots b_1\, b_2\, b_3 \dots) \dots$$

Now let $g \in \mathrm{Sym}(X)$ send a's to b's in that order. Now $g\alpha g^{-1}(b_i) = g\alpha(a_i) = g(a_{i+1}) = b_{i+1}$, hence $g\alpha g^{-1} = \beta$.

Conversely, suppose that $g\alpha g^{-1} = \beta$. Suppose for example that $(a_1 \dots, a_n)$ is a cycle of α. It follows easily that $(g(a_1) \dots, g(a_n))$ is a cycle of β. □

Exercises.

1. By using Theorem 22.2.2, find the sizes of conjugacy classes in $\mathrm{Sym}(n)$ for $n = 2, 3, 4, 5, 6, 7$. By using Proposition 22.2.1, find the sizes of centralisers in $\mathrm{Sym}(n)$ for $n = 2, 3, 4, 5, 6$.

   Answer:

n	2	3	4	5	6
Id_n	1	1	1	1	1
(12)	1	3	6	10	15
(123)		2	8	20	40
(12)(34)			3	15	45
(1234)			6	30	90
(12)(345)				20	120
(12345)				24	144
(12)(34)(56)					15
(12)(3456)					90
(123)(456)					40
(123456)					120
Total	2	6	24	120	720

2. Show that the elements $(01)(12)(34)\ldots$ and $(12)(34)(56)\ldots$ of $\mathrm{Sym}(\omega)$ are not conjugate.

   Proof: They do not have the same cycle structure. The first one has no cycles of length 1, the second one has one cycle of length 1.

3. Can $(01)(23)(45)\ldots$ and $(12)(34)(56)\ldots$ of $\mathrm{Sym}(\omega)$ be conjugate in a larger group?

   Answer: Yes! In $\mathrm{Sym}(\mathbb{Z})$... Because in $\mathrm{Sym}(\mathbb{Z})$ they have the same cycle.

4. Show that $C_{\mathrm{Sym}(n)}(12\ldots n)$ is cyclic of order n.

   Proof: Clearly $\langle(12\ldots n)\rangle \leq C_{\mathrm{Sym}(n)}(12\ldots n)$. By Exercise 20.b, page 33 and 22.2.2, page 125, $|C_{\mathrm{Sym}(n)}(12\ldots n)| = n!/(12\ldots n)^G| = n!/(n-1)! = n$. It follows that $\langle(12\ldots n)\rangle = C_{\mathrm{Sym}(n)}(12\ldots n)$.

5. Let X be a set and $g \in \mathrm{Sym}(X)$. let $Y = \{x \in X : g(x) \neq x\}$. Show that $C_{\mathrm{Sym}(X)}(g) \simeq C_{\mathrm{Sym}(Y)}(g) \times \mathrm{Sym}(X \setminus Y)$.

   Proof: We view $\mathrm{Sym}(Y)$ and $\mathrm{Sym}(X \setminus Y)$ as subgroups of $\mathrm{Sym}(X)$ in the obvious way.

   We certainly have $C_{\mathrm{Sym}(Y)}(g)$, $\mathrm{Sym}(X\setminus Y) \leq C_{\mathrm{Sym}(X)}(g)$. Also $C_{\mathrm{Sym}(Y)}(g) \cap \mathrm{Sym}(X \setminus Y) = 1$ and the elements of $C_{\mathrm{Sym}(Y)}(g)$ commute with the elements of $\mathrm{Sym}(X\setminus Y)$. Thus $C_{\mathrm{Sym}(Y)}(g) \times \mathrm{Sym}(X\setminus Y) = \langle C_{\mathrm{Sym}(Y)}(g), \mathrm{Sym}(X\setminus Y) \leq C_{\mathrm{Sym}(X)}(g)$.

   Conversely, let $c \in C_{\mathrm{Sym}(X)}(g)$. Then $gc = cg$. If $x \in X \setminus Y$, we get $g(x) = gc(x) = cg(x)$, so that c fixes $g(x)$ and hence g sends $X \setminus Y$ into $X\setminus Y$. Similarly, if $x \in Y$, then $g(x) \neq gc(x) = cg(x)$, so that $g(x) \in Y$ and

hence g sends Y into Y. Now we can write $g = ab$ where $a \in \mathrm{Sym}(X \setminus Y)$ and $b \in \mathrm{Sym}(Y)$. Now $b = a^{-1}g \in \mathrm{Sym}(X \setminus Y)C_{\mathrm{Sym}(X)}(g) \leq C_{\mathrm{Sym}(X)}(g)$. It follows that $b \in C_{\mathrm{Sym}(Y)}(g)$. □

6. Let $\alpha = (1, \ldots, n_1)(n_1 + 1, \ldots, n_1 + n_2) \ldots (n_1 + \ldots + n_{k-1}, \ldots, n_1 + \ldots + n_{k-1} + n_k)$. Let $n = n_1 + \ldots + n_{k-1} + n_k$. Suppose that the cycle lengths n_i are all distinct. Show that $C_{\mathrm{Sym}(n)}(\alpha) = \{\alpha_1^{i_1} \ldots \alpha_k^{i_k} : i_j = 0, 1, \ldots, n_j - 1 \text{ for all } j = 1, \ldots, k\} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ where $\alpha_j = (n_1 + \ldots + n_{j-1}, \ldots, n_1 + \ldots + n_{j-1} + n_j)$.

7. Let $g = (01)(234)(5678)(9\,10\,11\,12\,13)\ldots$. What is the group structure of $C_{\mathrm{Sym}(\omega)}(g)$?

   Answer: By parts 4 and 5, $C_{\mathrm{Sym}(\omega)}(g) \simeq \oplus_{n=2}^{\infty}\mathbb{Z}/n\mathbb{Z}$.

8. Let $a = (123)(456)(789)(10\,11\,12)$ Show that $C_{\mathrm{Sym}(12)}(a) \simeq (\mathbb{Z}/3\mathbb{Z})^4 \rtimes \mathrm{Sym}(4)$.

   Proof: We embed Sym(4) in Sym(12) via

$$\begin{array}{lcl} \mathrm{Id}_3 & \mapsto & \mathrm{Id}_{12} \\ (12) & \mapsto & (14)(25)(36) \\ (13) & \mapsto & (17)(28)(39) \\ (23) & \mapsto & (47)(58)(79) \\ (123) & \mapsto & (147)(258)(369) \\ \text{etc} & & \end{array}$$

   In other words, we view Sym(4) as the permutations of the four cycles (123), (456), (789), (10 11 12).

   It is clear that the image of Sym(4) in Sym(12) is in $C_{\mathrm{Sym}(12)}(a)$.

   Let $g \in C_{\mathrm{Sym}(12)}(a)$. Then g permutes the four cycles (123), (456), (789), (10 11 12). Hence there is an $h \in \mathrm{Sym}(4)$ (or in its image) such that $h^{-1}g$ preserves the four cycles. Hence $h^{-1}g$ is in the centralizer of these four cycles, which is equal to $\langle (123), (456), (789), (10\,11\,12)\rangle$ and to

$$\langle (123)\rangle \oplus \langle (456)\rangle \oplus \langle (789)\rangle \oplus \langle (10\,11\,12)\rangle,$$

   hence isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$.

   Thus $C_{\mathrm{Sym}(12)}(a) = (C_{\mathrm{Sym}(12)}((123), (456), (789), (10\,11\,12)))\,\mathrm{Sym}(4) \simeq (\mathbb{Z}/3\mathbb{Z})^3 \rtimes \mathrm{Sym}(4)$. □

9. Show that, except for $n = 4$, the centralizer of a transposition is the smallest centralizer of involutions ($\equiv$ elements of order 2) in $\mathrm{Sym}(n)$.

   Proof: An involution is a product of disjoint transpositions. For $2 \leq 2i \leq n$, let $a_i = (12)(34)\ldots(2i-1, 2i)$. We want to show that $|C_{\mathrm{Sym}(n)}(a_i)| \geq |C_{\mathrm{Sym}(n)}(a_1)|$ for all i and all $n \neq 4$. By Exercise 1, page 126, we may

assume that $n \geq 5$. By part 20, it is enough to show that $|a_i^{\mathrm{Sym}(n)}| \geq |a_1^{\mathrm{Sym}(n)}|$ for all i and all $n \geq 5$. By Exercise 22.2.2, page 125,

$$\begin{aligned} |a_i^{\mathrm{Sym}(n)}| &= \binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2i+2}{2}/i! \\ &= \tfrac{n!}{2^i(n-2i)!i!}. \end{aligned}$$

Hence we have to show that

$$\frac{n!}{2^i(n-2i)!i!} \geq \frac{n!}{2(n-2)!},$$

i.e. that

$$(n-2)! \geq 2^{i-1}(n-2i)!i!$$

for all $n \geq 5$ and all i such that $2 \leq 2i \leq n$. We proceed by induction on n. We know that the inequality must hold for $n = 5$ (by Exercise 1, page 126). Assume for n. We have to show that

$$(n-1)! \geq 2^{i-1}(n+1-2i)!i!$$

for all i such that $2 \leq 2i \leq n+1$. Then for all i such that $2 \leq 2i \leq n$, we have

$$\begin{array}{rclcl} (n-1)! & = & (n-1)(n-2)! & \geq & (n-1)2^{i-1}(n-2i)!i! \\ & \geq & (n+1-2i)2^{i-1}(n-2i)!i! & \geq & 2^{i-1}(n+1-2i)!i! \end{array}$$

It remains to prove the case $2i = n+1$, or $n = 2i-1$, i.e. we have to show that $(2i-2)! \geq 2^{i-1}i!$ for $i \geq 3$. This is easy to show.

10. Find and prove a similar statement for $\mathrm{Alt}(n)$.

22.3 Sylow p-Subgroups

Proposition 22.3.1 (Sylow p-subgroups of $\mathrm{Sym}(n)$) *Let $n \in \mathbb{N}$ and p a prime. Let $k = [n/p]$. Then a Sylow p-subgroup of $\mathrm{Sym}(n)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k \rtimes P$ where P is a Sylow p-subgroup of $\mathrm{Sym}(k)$ and P acts on $(\mathbb{Z}/p\mathbb{Z})^k$ by permuting the components.*

The generators of $(\mathbb{Z}/p\mathbb{Z})^k$ can be taken to be the cycles

$$\sigma_i = ((i-1)p+1, \ldots, ip)$$

for $i = 1, \ldots, k$. The element $\sigma_1\sigma_2\ldots\sigma_k$ is in the center of the Sylow p-subgroup. And the center of the Sylow p-subgroup is in $(\mathbb{Z}/p\mathbb{Z})^k$.

Proof: Let P be a Sylow p-subgroup of $\mathrm{Sym}(n)$. We first note that $|P| = p^{[n/p]+[n/p^2]+\cdots}$.

If p does not divide n, then $P \leq \mathrm{Sym}(n-1) \leq \mathrm{Sym}(n)$. So we may assume that p divides n. Let $n = kp$. Now we have $|P| = p^{[n/p]+[n/p^2]+\cdots} = p^{k+[k/p]+[k/p^2]\cdots}$.

Since P has a nontrivial center, there is an element z of order p in $Z(P)$. Conjugating if necessary, we may assume that

$$z = z_i = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \ldots ((i-1)p+1, (i-1)p+2, \ldots, ip)$$

for some $i = 1, \ldots, k$. Thus $P \leq C_{\mathrm{Sym}(n)}(z_i)$. Now we compute $|C_{\mathrm{Sym}(n)}(z_i)|$ and choose i so that $p^{[n/p]+[n/p^2]+\cdots}$ (which is equal to $p^{k+[k/p]+[k/p^2]\cdots}$) divides $|C_{\mathrm{Sym}(n)}(z_i)|$.

It is clear that

$$|z_i^{\mathrm{Sym}(n)}| = \frac{\binom{n}{p}(p-1)!\binom{n-p}{p}(p-1)!\ldots\binom{n-(i-1)p}{p}(p-1)!}{i!} = \frac{n!}{p^i i!}$$

Thus

$$|C_{\mathrm{Sym}(n)}(z_i)| = |\mathrm{Sym}(n)|/|z_i^{\mathrm{Sym}(n)}| = p^i i!$$

The maximal power of p that divides $p^i i!$ is $p^i p^{[i/p]+[i/p^2]+\cdots} = p^{i+[i/p]+[i/p^2]+\cdots}$. Thus if we take $i = k$, then $C_{\mathrm{Sym}(n)}(z_i)$ will be large enough to contain P.

We now find $C_{\mathrm{Sym}(n)}(z_k)$. Recall that it has $p^k k!$ elements. Let

$$\sigma_i = ((i-1)p+1, \ldots, ip)$$

for $i = 1, \ldots, k$. Then

$$(\mathbb{Z}/p\mathbb{Z})^k \simeq \langle \sigma_1, \sigma_2, \ldots \sigma_k \rangle = \langle \sigma_1 \rangle \oplus \langle \sigma_2 \rangle \oplus \ldots \oplus \langle \sigma_k \rangle \leq C_{\mathrm{Sym}(n)}(z_k).$$

Also the elements of $\mathrm{Sym}(n)$ that permute the cycles of σ_i are in $C_{\mathrm{Sym}(n)}(z_k)$. Consider the ones of the form $\{\sigma :$ for all $i = 1, \ldots, k$, $\sigma(ip) = jp$ for some j and $\sigma(ip-\ell) = \sigma(ip) - \ell$ for all $\ell = 1, \ldots, p-1\} \simeq \mathrm{Sym}(k)$. It is easy to see that $C_{\mathrm{Sym}(n)}(z_k) \simeq (\mathbb{Z}/p\mathbb{Z})^k \rtimes \mathrm{Sym}(k)$, where $\mathrm{Sym}(k)$ permutes the components. Thus P is isomorphic to a Sylow p-subgroup of $(\mathbb{Z}/p\mathbb{Z})^k \rtimes \mathrm{Sym}(k)$, which is $(\mathbb{Z}/p\mathbb{Z})^k \rtimes Q$ for some Sylow p-subgroup Q of $\mathrm{Sym}(k)$. The last statements are easy to prove. □

Corollary 22.3.2 (Sylow p-subgroups of $\mathrm{Alt}(n)$) *If $p \neq 2$ then Sylow p-subgroup of $\mathrm{Sym}(n)$ are in $\mathrm{Alt}(n)$.*

If $p = 2$, then with the notation of the theorem above, a Sylow 2-subgroup of $Alt(n)$ is isomorphic to

$$\{(a_0, \ldots, a_{k-1}) : \sum_{i=0}^{k-1} a_i \text{ is even}\} \rtimes P$$

where P is a Sylow 2-subgroup of $\mathrm{Sym}(k)$ and it acts on the normal part by permuting the components.

Corollary 22.3.3 *Let G be a finite p-group. Then there is a finite p-subgroup P such that $G \leq P$ and $Z(P) \simeq \mathbb{Z}/p\mathbb{Z}$.*

Exercises.

1. Find the Sylow 3-subgroups of Sym(n) for $n = 1, \ldots, 27$.
2. Show that the center of the Sylow p-subgroups of Sym(p^n) has p-elements.

Chapter 23

Classification of Finite Abelian Groups

Theorem 23.0.4 *Let G be a torsion abelian group. Then*

$$G = \bigoplus_p G_p$$

where

$$G_p = \{g \in G : g^{p^n} = 1 \text{ for some } n \in \mathbb{N} \setminus \{0\}\}$$

and p ranges over all primes.

Proof: It is clear that each G_p is a subgroup and that for any prime q, $G_q \cap \langle G_p : p \neq q \rangle = 1$. Thus

$$\langle G_p : p \rangle = \bigoplus_p G_p.$$

To be continued... pppp

Theorem 23.0.5 (Classification of Finite Abelian p-Groups) *Let p be a prime and G a finite abelian p-group. Then $G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$ for some unique $n_1 \geq n_2 \geq \ldots \geq n_k$.*

Proof: Let $p^n = \exp(G)$. Let $h \in G$ be an element of maximal order, i.e. of order p^n. Let $H = \langle h \rangle$. We will show that H has a complement in G. (This may be false if h is not chosen to be of maximal order, as an exercise find a counterexample). Let K be a subgroup of G maximal with respect to intersecting H trivially. Note that $\langle H, K \rangle = HK = H \oplus K$. We will show that $G = HK$. Assume not. Let $g \in G \setminus HK$. We would be done if the subgroup generated by K and g did not intersect H. Unfortunately this is false if g is not chosen properly (find a counterexample, but do not choose K maximal because otherwise there is no g outside of HK, as we will soon show!) Some nontrivial p^{th} power of g is in HK. Assume $g^{p^i} \in G \setminus HK$

but $g^{p^{i+1}} \in HK$. Replacing g by g^{p^i}, we may assume that $g^p \in HK$. Thus $g^p = hk$ for some (unique) $h_1 \in H$ and $k \in K$. Since $o(g^p) \leq p^{n-1}$ and $HK = H \oplus K$, $o(h_1) \leq p^{n-1}$. But $h_1 \in H = \langle h \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$ and it is an element of order p^{n-1}. It follows from Lemma **??** that h_1 is a p^{th} power in H. hence $h_1 = h_2^p$ for some $h_2 \in H$. Now $(gh_2^{-1})^p = g^p h_2^{-p} = g^p h_1^{-1} = k \in K$. Also, $gh_2^{-1} \in G \setminus KH$ because otherwise g would be in KH, contradicting its choice. Therefore, replacing g by gh_2^{-1}, we may assume that $g^p \in K$. Now consider the subgroup $\langle K, g \rangle = K \cup Kg \cup \ldots \cup Kg^{p-1}$. We claim that $Kg^i \cap H = \emptyset$ if $i = 1, \ldots, p-1$. Indeed, otherwise g^i would be in HK, and since $(p, i) = 1$ and $g^p \in K \leq KH$, we would also have $g \in KH$, contradicting the choice of g. Thus

$$\langle K, g \rangle \cap H = (K \cup Kg \cup \ldots \cup Kg^{p-1}) \cap H = K \cap H = 1.$$

This contradicts the fact that K was maximal with respect to intersecting H trivially.

Now by induction on $|G|$, $K \simeq \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$ for some unique $n_2 \geq \ldots \geq n_k$. Clearly $p^{n_2} = \exp(K) \leq p^n$. We now have $G = H \oplus K \simeq \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$ where $n \geq n_2 \geq \ldots \geq n_k$. Uniqueness of the exponents is clear. □

Exercises.

1. Find all isomorphism types of abelian groups of order 1728.

Chapter 24

Divisible Groups

24.1 Generalities

A group G is called **divisible** if for every $g \in G$ and integer $n > 0$ there is an $h \in G$ such that $h^n = g$. The additive group $\mathbb{Q}$ is divisible.

Theorem 24.1.1 (Divisible Groups) *A quotient of a divisible group is divisible. In particular, a divisible group does not have a proper subgroup of finite index.*

Let p be a prime. A group G is called **p-divisible** if for every $g \in G$ and there is an $h \in G$ such that $h^p = g$.

exercise

1. Show that a torsion group without elements of order p is p-divisible.

2. ¶ Find the fields K and integers n for which the groups $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{PGL}_n(K)$, $\mathrm{PSL}_n(K)$ are divisible.

3. Let G be an abelian group. Suppose G has a normal abelian subgroup A such that A and G/A are p-divisible. Then G is p-divisible.

4. The statement above is false if G is not abelian; more precisely, there is a group G with a normal subgroup A such that A and G/A are abelian and p-divisible, but G not p-divisible.

24.2 Divisible Abelian Groups

A group G is called **divisible** if for every $g \in G$ and integer $n > 0$ there is an $h \in G$ such that $h^n = g$. The additive group $\mathbb{Q}$ is divisible.

Theorem 24.2.1 (Classification of Torsion-Free Divisible Abelian Groups) *Any divisible abelian torsion-free group is a vector space over $\mathbb{Q}$. Thus such a group is isomorphic to a direct sum of $\mathbb{Q}$'s. In particular any two divisible torsion-free abelian group of the same uncountable cardinality are isomorphic.*

Theorem 24.2.2 (Splitting of Divisible Subgroups) *Let G be an abelian group and A a divisible subgroup of G. Then A splits in G, i.e. $G = A \oplus B$ for some $B \leq G$.*

Let p be a prime. The set $\{z \in \mathbb{C} : z^{p^n} = 1\}$ is a subgroup of $\mathbb{C}^*$. It is called **Prüfer p-group** and is denoted by $\mathbb{Z}_{p^\infty}$. It is a divisible p-group. For each n, it has a unique cyclic subgroup of order p^n.

Theorem 24.2.3 (Classification of divisible abelian groups) *Any divisible abelian group is isomorphic to*

$$(\oplus_I \mathbb{Q}) \oplus (\oplus_{p \text{ prime}} (\oplus_{I_p} \mathbb{Z}_{p^\infty})).$$

The isomorphism type is determined by the cardinalities of the index sets I and I_p.

A subgroup A of an abelian group G is called **pure** if $nG \cap A = nA$.

Theorem 24.2.4 (Finitely Generated Subgroups of $\mathbb{Q}$) *For a/b, $c/d \in \mathbb{Q}$, $\langle a/b, c/d \rangle = \langle \gcd(ad, bc)/bd \rangle$. Thus a finitely generated subgroup of $\mathbb{Q}$ is in fact generated by one element.*

Theorem 24.2.5 (Classification of Subgroups of $\mathbb{Q}$) *Let G be a nontrivial subgroup of $\mathbb{Q}^+$. Then there are unique $a \in \mathbb{N} \setminus \{0\}$ and $f : \{\text{primes of } \mathbb{N}\} \longrightarrow \mathbb{N} \cup \{\infty\}$ such that*

$$G = \mathbb{Q}(a, f) = a\{x/p_1^{n_1} \dots p_k^{n_k} : k \in \mathbb{N}, \, p_i \text{ prime and } n_i \leq f(p_i) \text{ forall } i\}.$$

Exercises.

1. Show that $\mathbb{Z}_{p^\infty}$ is the only infinite subgroup of $\mathbb{Z}_{p^\infty}$. Show that if $H < \mathbb{Z}_{p^\infty}$, then $\mathbb{Z}_{p^\infty}/H \simeq \mathbb{Z}_{p^\infty}$.

2. Show that a divisible subgroup of $(\mathbb{Z}_{p^\infty})^n$ is isomorphic to $\mathbb{Z}_{p^\infty}$ for some $i \leq n$.

3. **(Splitting of Pure and Bounded Subgroups)** Let G be an abelian group and A a pure subgroup of bounded exponent of G. Then A splits in G, i.e. $G = A \oplus B$ for some $B \leq G$.

4. Find the isomorphism type of $\mathbb{Q}/\mathbb{Q}(a, f)$. Is it isomorphic to a subgroup of $\mathbb{Q}$?

5. When do we have $\mathbb{Q}(a, f) \simeq \mathbb{Q}(a_1, f_1)$?

6. Can you find a group theoretic characterization of subgroups of $\mathbb{Q}$?

7. Try to classify subgroups of $\mathbb{Q} \times \mathbb{Q}$. **Note:** I do not know the answer to the above problem. On the other hand, Simon Thomas proved that, in some sense, classification of subgroups of $\mathbb{Q} \times \mathbb{Q}$ is "harder than (i.e. not reducible to) the classification of subgroups of $\mathbb{Q}$.

24.3 Divisible Nilpotent Groups

Chapter 25

Free Groups

25.1 Definition

Let X be a set. A **free group over** X is a group F_X together with a map $i : X \longrightarrow F_X$ such that for any group G and map $f : X \longrightarrow G$ there is a unique group homomorphism $\phi : F_X \longrightarrow G$ such that $\phi \circ i = f$.

Theorem 25.1.1 *Free groups exist and are unique up to isomorphism.*

Theorem 25.1.2 *F_X is generated by X.*

Theorem 25.1.3 *A group is generated by a subset X is a quotient of F_X*

25.2 Free Abelian Groups

Let X be a set. A **free abelian group over** X is a group A_X together with a map $i : X \longrightarrow A_X$ such that for any abelian group G and map $f : X \longrightarrow G$ there is a unique group homomorphism $\phi : F_X \longrightarrow G$ such that $\phi \circ i = f$.

Theorem 25.2.1 *Free abelian groups exist, are unique up to isomorphism and are abelian. Furthermore $A_X \simeq F_X/F'_X$.*

Theorem 25.2.2 *A_X is generated by X.*

Theorem 25.2.3 *An abelian group is generated by a subset X is a quotient of A_X*

Theorem 25.2.4 *$A_X \simeq \oplus_X \mathbb{Z}$.*

Theorem 25.2.5 (Subgroups of $\mathbb{Z} \times \mathbb{Z}$) *If $G \leq \mathbb{Z} \times \mathbb{Z}$ is a subgroup which is not generated by one element then there are unique integers x, y, z such that $0 \leq x < z$, $0 < y$ and $G = \langle (x, y), (z, 0) \rangle$.*

Theorem 25.2.6 (Subgroups of $\mathbb{Z}^n$) *Any subgroup of $\mathbb{Z}^n$ is generated by at most n elements and is isomorphic to $\mathbb{Z}^i$ for some $i = 0, 1, \ldots, n$.*

Exercises.

1. Classify all subgroups of $\mathbb{Z}^3$.

Chapter 26

General Linear Groups

Chapter 27

Automorphism Groups of Abelian Groups

¶ Note that an abelian group is nothing else than a $\mathbb{Z}$-module.

Lemma 27.0.7 *If A is an abelian group, then* $\mathrm{End}(A)$ *is a ring and* $\mathrm{Aut}(A) = \mathrm{End}(A)^*$.

If G is an arbitrary group, $\mathrm{Hom}(G, A)$ *is naturally an abelian group.*

Theorem 27.0.8 *Let p be a prime. Then*

i. $\mathrm{End}(\mathbb{Z}/p^n\mathbb{Z}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

ii. $\mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathbb{Z}/p^{n-1} \times \mathbb{Z}/(p-1)\mathbb{Z}$ *and is cyclic.*

iii. $\mathrm{Aut}(\mathbb{Z}/2^n\mathbb{Z}) \simeq (\mathbb{Z}/2^n\mathbb{Z})^* \simeq \mathbb{Z}/2^{n-2} \times \mathbb{Z}/2\mathbb{Z}$ *if* $n \geq 2$.

Theorem 27.0.9 (General Linear Groups over $\mathbb{Z}/p^n\mathbb{Z}$) *Let p be a prime and n and m two natural naturals. Set $R = \mathbb{Z}/p^n\mathbb{Z}$ and $M = p\mathbb{Z}/p^n\mathbb{Z}$. Then* $\mathrm{End}(R^m) \simeq \mathrm{Mat}_{m\times m}(R)$ *and* $\mathrm{Aut}(R^m) \simeq \mathrm{GL}_m(R)$. *Furthermore,*

i. $|\mathrm{GL}_m(R)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1})p^{(n-1)m^2}$.

ii. The set of matrices with entries of the diagonal from $1 + M$ and the entries below the diagonal from M is a Sylow p-subgroup of $\mathrm{GL}_n(R)$.

Theorem 27.0.10 (Automorphisms of the Prüfer p-Groups) $\mathrm{End}(\mathbb{Z}_{p^\infty}) \simeq \mathbb{Z}_p$ *(the p-adic integers, see below) and* $\mathrm{Aut}(\mathbb{Z}_{p^\infty}) \simeq \mathbb{Z}_p^*$.

Theorem 27.0.11 $\mathrm{End}(\mathbb{Z}_{p^\infty}^n) \simeq \mathrm{Mat}_{n\times n}\,\mathbb{Z}_p$ *and* $\mathrm{Aut}(\mathbb{Z}_{p^\infty}^n) \simeq \mathrm{GL}_n(\mathbb{Z}_p)$.

Exercises.

1. When is $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ cyclic?
2. What is the nilpotency class of the Sylow p-subgroup of $\mathrm{GL}_m(\mathbb{Z}/p^n\mathbb{Z})$?
3. What is the group structure of $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z})$?

4. Find elements of order p of $\mathrm{GL}_2(\mathbb{Z}_p)$. Find the Sylow p-subgroups (i.e. the maximal p-subgroups) of $\mathrm{GL}_n(\mathbb{Z}_p)$. Find the involutions (elements of order 2) of $\mathrm{GL}_2(\mathbb{Z}_p)$. Find the Sylow 2-subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Chapter 28

Permutation Groups

Let G be a group and X any set. A map $G \times X \longrightarrow X$ is called an **action** of the group G on the set X if for all $g, h \in G$ and $x \in X$ (we will denote the image of the pair $(g, x) \in G \times X$ by gx)

i. $g(hx) = (gh)x$,

ii. $1x = x$.

The action of the group G on the set X gives rise naturally to a group homomorphism $\tilde{}$ from G into $\mathrm{Sym}(X)$ defined by $g \mapsto \tilde{g}$ where $\tilde{g}(x) = gx$ for $x \in X$. Conversely any group homomorphism $\tilde{} : G \longrightarrow \mathrm{Sym}(X)$ gives rise to a group action of G on X via $gx := \tilde{g}(x)$.

The pair (G, X) is called a **permutation group**. The kernel $\mathrm{Ker}(\tilde{})$ of the homomorphism $\tilde{}$ is called the **kernel** of the action. Clearly the kernel is a normal subgroup of G. An action is called **faithful** if its kernel is trivial; this means that if $gx = x$ for all $x \in X$, then $g = 1$.

Lemma 28.0.12 *Let (G, X) be a permutation group. If $H \lhd G$ is a subgroup of $Ker(\tilde{})$, then G/H acts on X in a natural way via $\overline{g}x := gx$. The kernel of this action is* $\mathrm{Ker}(\tilde{})/H$. *In particular* $G/\mathrm{Ker}(\tilde{})$ *acts faithfully on X.*

If $x \in X$, then the **G-orbit** of X is the set Gx. The **stabilizer** of x is defined to be $G_x := \{g \in G : gx = x\}$.

Lemma 28.0.13 *i. $G_x \leq G$ and there is a natural one to one correspondence between the left coset space G/G_x and the G-orbit Gx given by $gG_x \mapsto gx$.*

ii. Any two G-orbits are either equal or disjoint.

iii. For $x \in X$ and $g \in G$, $G_x^g = G^{g^{-1}x}$.

iv. If $|X|$ is finite, then $|X| = \sum_x |G/G_x|$ where the summation is over a set of representatives of distinct orbits.

Corollary 28.0.14 *Let G be a group.*

i. If $H \leq G$ has finite index in G, then $|\{H^g : g \in G\}| = |G/N_G(H)|$.

ii. If $a \in G$ be such that $C_G(a)$ has finite index in G, then $|\{a^g : g \in G\}| = |G/C_G(a)|$.

iii. A finite p-group has a nontrivial center.

A permutation group (G, X) is called **n-transitive** if for any two pairs of distinct n-tuples $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ of points from X there is a $g \in G$ such that $gx_i = y_i$ for all $i = 1, \ldots, n$. The action is called **sharply n-transitive** if the above element g of G is unique. Sharply 1-transitive group actions are often called **regular** actions.

Examples and Exercises.

1. $\mathrm{Sym}(n)$ acts on $\{1, \ldots, n\}$ in a natural way. $\mathrm{Sym}(n)$ is sharply n and $(n-1)$-transitive on $\{1, \ldots, n\}$. Also $\mathrm{Alt}(n)$ is sharply $(n-2)$-transitive on $\{1, \ldots, n\}$.

2. If G acts on X, then any subgroup of G acts on X. If $Y \subseteq X$ is such that $gY \subseteq Y$ for all $g \in G$, then G acts on Y.

3. If G acts on X and $Y \subseteq X$, then G acts on $\{gY : g \in G\}$.

4. ¶ The group of homeomorphisms of a topological space acts on the space. For any first order structure M, $\mathrm{Aut}(M)$ acts on M.

5. The group of rotations of $\mathbb{R}^2$ act on $\mathbb{R}^2$. Find the orbits of this action. Similarly with translations.

6. $\mathrm{GL}_n(K)$ acts on K^n naturally. This action is not transitive. The action of $\mathrm{GL}_n(K)$ on $K^n \setminus \{0\}$ is transitive but not doubly transitive unless $K = \mathbb{F}_2$. The action of $\mathrm{GL}_n(K)$ on K^n gives rise naturally to an action of $\mathrm{GL}_n(K)$ on the set of i-dimensional subspaces of K^n. Find the stabilizers of vectors in $\mathrm{GL}_n(K)$.

7. $\mathrm{GL}_n(K)$ acts on the set $\pi_{n-1}(K)$ of lines through the origin 0. The kernel of this action is $Z(\mathrm{GL}_n(K))$. Thus $\mathrm{PGL}_n(K)$ acts on $\pi_{n-1}(K)$. The set $\pi_{n-1}(K)$ is called the **$(n-1)$-dimensional projective space** over the field K. The 1 and 2-dimensional projective spaces are called **projective line** and **projective plane** respectively. Find the cardinality of $\pi_{n-1}(\mathbb{F}_q)$. Find the stabilizers of a line of $\pi_{n-1}(K)$ in $\mathrm{PGL}_n(K)$. If $K = \mathbb{F}_q$ what is the index of the stabilizer of a line in $\mathrm{PGL}_n(K)$?

8. (**Left coset action.**) Let G be a group and $H \leq G$. Consider the left coset space G/H. Then the group G acts on G/H via $g(xH) = gxH$. This action is transitive and its kernel is the core (see Theorem 3.2.3).

   If $H = 1$, then this action is regular and is called the **regular action** of G.

9. Let G be a group and $A \subseteq G$. Let $X = \{A^g : g \in G\}$. Then G acts on X by conjugation. What is the kernel of this action if $A \leq G$? If $A = \{a\}$?

10. Let G act on X. Then G acts on X^n componentwise. The group G also acts on $X_n := X^n \setminus \{x \in X^n : x_i \neq x_j \text{ if } i \neq j\}$. Then (G, X) is (sharply) n-transitive if and only if (G, X_n) is transitive (regular).

Two permutation groups (G, X) and (H, Y) are called **equivalent** if there is a group isomorphism $\phi : G \longrightarrow H$ and a bijection $f : X \longrightarrow Y$ such that $f(gx) = \phi(g)f(x)$ for all $g \in G$ and $x \in X$, i.e. if $f \circ \tilde{g} = \widetilde{\phi(g)} \circ f$ for all $g \in G$.

Proposition 28.0.15 *Let (G, X) be a transitive permutation group. Let $x \in X$. Then the permutation group (G, X) is equivalent to the permutation group $(G, G/G_x)$ given in Example 7 above.*

Proposition 28.0.16 *Let G act transitively on X and let $n > 1$. Then (G, X) is (sharply) n-transitive on X if and only if for any (equivalently, for some) $x \in X$, G_x acts (sharply) $(n-1)$-transitive on $X \setminus \{x\}$.*

Exercises

1. i. The permutation group (G, X) is doubly transitive (resp. sharply 2-transitive) if and only if $G = H_x \sqcup H_x \omega H_x$ for some (equivalently, any) $\omega \in G \setminus H$ (resp. and if the representation is unique).

   ii. A group G acts double transitively (resp. sharply 2-transitive) on a set if and only if it has a subgroup H such that $G = H \cup H\omega H$ for some (equivalently, any) $\omega \in G \setminus H$ (resp. and if the representation is unique).

2. If $n \geq 3$ then $\mathrm{PGL}_n(K)$ is 2-transitive on π_{n-1} but not 3-transitive. On the other hand $\mathrm{PGL}_2(K)$ is sharply 3-transitive on $\pi_1(K)$.

3. How transitive is $\mathrm{PSL}_2(K)$ on $\pi_1(K)$?

4. Let K be a field. The group (called the **affine group**) of matrices of the form
$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$$
where $x \in K^*$ and $y \in K$ acts sharply 2-transitively on the set of vectors of the form
$$\begin{pmatrix} x \\ 1 \end{pmatrix}$$
where $x \in K$.

Let (G, X) be a permutation group. A subset Y of X is called a **set of imprimitivity** if for all $g, h \in G$ either $gY \cap hY = \emptyset$ or $gX = gY$. Any singleton set is a set of imprimitivity. The set X is a set of imprimitivity. The permutation group (G, X) is called **primitive** if it has no other set of imprimitivity.

Lemma 28.0.17 *A transitive group (G, X) is primitive if and only if G_x is a maximal subgroup for some (equivalently, for all) $x \in X$.*

Lemma 28.0.18 *A doubly transitive group is primitive.*

Lemma 28.0.19 *Let (G, X) be a doubly transitive permutation group and $x \in X$. Let $D \neq 1$ be a normal subset of G then $G = DH$ if $D \cap H \neq \emptyset$ and $G = DH \cup H$ if $D \cap H = \emptyset$.*

Exercises.

1. Find a maximal subgroup of $\mathrm{GL}_n(K)$.
2. Show that a simple group with a subgroup of index n is isomorphic to a subgroup of $\mathrm{Sym}(n)$.
3. Show that a simple group cannot have a subgroup of index ≤ 4.
4. Show that a simple group with a subgroup of index 5 is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ or $\mathrm{Alt}(5)$.
5. Let H be a subgroup of index n in G. Show that there is an $m \in \mathbb{N} \setminus \{0\}$ such that for every $g \in G$, $g^m \in H$.

   Proof: Take $m = n!$ in Theorem 3.2.3.
6. Show that a divisible group cannot have a proper subgroup of finite index.

   Proof: Let G be a divisible group and $H \leq G$ a subgroup of index n. Let $g \in G$. Let $h \in G$ be such that $g = h^{n!}$. By Theorem 3.2.3, $g = h^{n!} \in H$. So $G = H$.
7. No group of order ≤ 59 is nonabelian and simple.
8. Show that $\mathrm{Alt}(5) \simeq \mathrm{SL}_2(\mathbb{F}_4)$.
9. Show that a simple group of order 60 is isomorphic to $\mathrm{Alt}(5) \simeq \mathrm{SL}_2(\mathbb{F}_4)$.

28.1 Frobenius Groups

Lemma 28.1.1 *Let (G, X) be a transitive permutation group. Let $x \in X$. Then no nontrivial element of G fixes two distinct elements of X if and only if for any $g \in G \setminus G_x$, $G_x^g \cap G_x = 1$.*

Lemma 28.1.2 *A group G acts transitively but not regularly on a set as in the lemma above if and only if G has a proper nontrivial subgroup H such that for any $g \in G \setminus H$, $H^g \cap G_x = 1$.*

A group as in the lemma above is called a **Frobenius group**. The subgroup H is called a **Frobenius complement**.

Examples.

1. $\langle x \rangle < F_2$ where F_2 is the free group generated by x and y is a Frobenius group.
2. If F is a field and $T \leq F^*$, then $F \rtimes T$ is a Frobenius group.
3. Any sharply 2-transitive group is a Frobenius group.

Theorem 28.1.3 *Let G be a finite Frobenius group with $H < G$ as the Frobenius complement. Assume that H has an involution. Then $G = A \rtimes H$ for some normal abelian subgroup A.*

The splitting part of the theorem above also holds in case H has no involutions (Frobenius), but the proof is much harder. Later Thompson proved that the normal complement A is nilpotent (a very hard and important theorem).

In the theorem above we have $A = I(G)^2 = iI(G) = (G \setminus \bigcup_{g \in G} H^g) \cup \{1\}$.

28.2 Sharply 2-Transitive Groups

In this subsection, we let (G, X) to be a sharply 2-transitive group. We fix $x \in X$ and we let $H = G_x$. The set of involutions of G is denoted by $I(G)$ or by I. Finally we let

$$N = (G \setminus \bigcup_g H^g) \cup \{1\} = \{g \in G : gy \neq y \text{ all } y \in X\}.$$

Proposition 28.2.1 *i. H is a maximal subgroup.*

ii. $H \cap H^g \neq 1$ if and only if $g \in H$. In particular $N_G(H) = H$ and $C_G(h) \leq H$ for any $h \in H^*$.

iii. G has involutions and they are all conjugate.

iv. H has at most one involution.

If G_x has an involution, we say that $\mathrm{char}(G) \neq 2$. Otherwise we say that $\mathrm{char}(G) = 2$. When H has an involution, we denote it by i.

Proposition 28.2.2 *i. If $A \lhd G$ is such that $Z(A) \neq 1$, then $G = Z(A) \rtimes H$.*

ii. $I(G) = \begin{cases} j^H & \text{for any } j \in I(G) \quad \text{if } \mathrm{char}(G) = 2 \\ j^H \cup \{i\} & \text{for any } j \in I(G) \setminus \{i\} \quad \text{if } \mathrm{char}(G) \neq 2 \end{cases}$

iii. If $\mathrm{char}(G) \neq 2$, then $I^2 \setminus \{1\}$ is one conjugacy class.

iv. $I^2 \setminus \{1\} \subseteq N$.

v. If $a \in N^*$ then $C_G(a) \subseteq N$.

Theorem 28.2.3 *If G is finite then $G = A \rtimes H$ for some elementary abelian p-subgroup $A \lhd G$. In fact $A = N = I^2$.*

Theorem 28.2.4 *If $G = A \rtimes H$ for some subgroup $A \lhd G$ then $A \subseteq N$ and is abelian.*

Theorem 28.2.5 *If H is abelian, then (G, X) is equivalent to the example of Exercise 4.*

Conjecture 28.2.6 *It is unknown whether or not $G = A \rtimes H$ for some subgroup $A \lhd G$.*

Exercises.

1. Show that if G is solvable, then $G = A \rtimes H$ for some $A \lhd G$.
2. A group of the form $G = A \rtimes H$ is doubly transitive on G/H if and only if H acts (by conjugation) regularly on A^*.

Chapter 29

Miscellaneous Problems in Group Theory

1. Find the isomorphism types of the additive groups $\mathbb{R}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{C}/\mathbb{R}$.
2. Find the isomorphism types of the multiplicative groups $\mathbb{R}^*/\mathbb{Q}^*$, $\mathbb{C}^*/\mathbb{R}^{>0}$, $\mathbb{C}^*/\mathbb{R}^*$.
3. Show that $C_{Sym(n)}((12)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{Sym}(n-2)$.
4. Any two involutions of a finite group are either conjugate or commute with a third one.
5. Show that a finite group with a fixed-point-free automorphism of order 2 is abelian.
6. Find a centerless group with a fixed-point-free automorphism of order 2.
7. Let G be a finite group and let H be a proper subgroup of G. Show that G is not the set-theoretic union of all conjugates of H.
8. Find all groups that have exactly three subgroups.
9. Is it true that an infinite group cannot be a union of finitely many proper subgroups?
10. Prove that $\mathrm{Aut}(D_8) \simeq D_8$.
11. Let p, q be two distinct primes. Show that a group of order pq is solvable.
12. Let p, q, r be three distinct primes. Show that a group of order pqr cannot be simple.

Part VII

Intermediate Field Theory

Chapter 30

Field Extensions

Chapter 31

Algebraic Field Extensions

Chapter 32

Transcendence Basis

Part VIII

Intermediate Ring Theory

Chapter 33

Dedekind Domains

Part IX

Galois Theory

Part X

Exams

33.1 First Semester

33.1.1 Fall 2002 Midterm

1. Let H, $K \leq G$. Show that $\{HxK : x \in G\}$ is a partition of G. (3 pts.)

   Proof: The relation $x \equiv y$ defined by "$HxK = HyK$" is certainly reflexive and symmetric. Let us prove the transitivity. It is clear that $HxK = HyK$ if and only if $x \in HyK$. Thus if $x \in HyK$ and $y \in HzK$, then $x \in HHzKK \subseteq HzK$.

2. Let $H \leq G$. Show that there is a natural one to one correspondence between the left coset space of H in G and the right coset space of H in G. (3 pts.)

   Proof: Consider the map $xH \mapsto Hx^{-1}$. This is well defined and one to one because $xH = yH$ if and only if $y^{-1}x \in H$ if and only if $y^{-1} \in Hx^{-1}$ if and only if $Hy^{-1} = Hx^{-1}$. It is also onto.

3. Let $H, K \leq G$. Show that $xH \cap yK$ is either empty or of the form $z(H \cap K)$ for some $z \in G$. (5 pts.)

   Proof: Assume $xH \cap yK \neq \emptyset$. Let $z \in xH \cap yK$. Then $xH = zH$ and $yK = zK$. So $xH \cap yK = zH \cap zK = z(H \cap K)$.

4. a) Show that the intersection of two subgroups of finite index is finite. (5 pts.)

   b) If $[G : H] = n$ and $[G : K] = m$, what can you say about $[G : H \cap K]$? (7 pts.)

   Proof: (a) Let H and K be two subgroups of index n and m of a group G. Then for any $x \in G$, $x(H \cap K) = xH \cap xK$ and there are at most n choices for xH and m choices for xK. Hence $[G : H \cap K] \leq nm$.

   (b) If $C \leq B \leq A$ and if the indices are finite then $[A : C] = [A : B][B : C]$ because cosets of C partition B and cosets of B partition A, i.e. if $B = \sqcup_{i=1}^{r} b_i C$ and $A = \sqcup_{j=1}^{s} a_j B$, then $A = \sqcup_{i=1}^{r} \sqcup_{j=1}^{s} b_i a_j C$.

   Thus $[G : K \cap H] = [G : H][H : H \cap K] = [G : K][K : H \cap K]$. It follows that n and m both divide $[G : K \cap H]$, hence $\mathrm{lcm}(n, m)$ divides $[G : K \cap H]$. Further in part (a) we have seen that $[G : K \cap H] \leq mn$.

5. Let G be a group and $H \leq G$ a subgroup of index n. Let $X = G/H$ be the left coset space. For $g \in G$, define $\tilde{g} : G/H \longrightarrow G/H$ by $\tilde{g}(xH) = gxH$ for $x \in G$.

   a) Show that $\tilde{g} \in \mathrm{Sym}(X)$. (2 pts.)

   b) Show that $\tilde{} : G \longrightarrow \mathrm{Sym}(X)$ is a homomorphism of groups. (3 pts.)

   c) Show that $\mathrm{Ker}(\tilde{})$ is the largest normal subgroup of G contained in H. (5 pts.)

   d) Show that $[G : \mathrm{Ker}(\tilde{})]$ divides $n!$. (5 pts.)

e) Conclude that there is an $m \in \mathbb{N} \setminus \{0\}$ such that for every $g \in G$, $g^m \in H$. (3 pts.)

f) Conclude that a divisible group[1] cannot have a proper subgroup of finite index. (7 pts.)

Proof: (a) $\tilde{g}$ is one to one because if $\tilde{g}(xH) = \tilde{g}(x_1H)$ then $gxH = gx_1H$, and so $xH = x_1H$. $\tilde{g}$ is onto because if $xH \in G/H$, then $\tilde{g}(g^{-1}xH) = xH$.

(b) Let g, $h \in G$ be any two elements. Since $(\tilde{g} \circ \tilde{h})(xH) = \tilde{g}(\tilde{h})(xH)) = \tilde{g}(hxH) = ghxH = \widetilde{gh}(xH)$ for all $xH \in G/H$, $\tilde{g} \circ \tilde{h} \widetilde{gh}$. Hence $\tilde{}$ is a group homomorphism.

(c) $\mathrm{Ker}(\tilde{})$ is certainly a normal subgroup of G. Also $\mathrm{Ker}(\tilde{}) = \{g \in G : \tilde{g} = \mathrm{Id}\} = \{g \in G : gxH = xH \text{ for all } x \in G\} = \{g \in G : x^{-1}gx \in H \text{ for all } x \in G\} = \{g \in G : g \in xHx^{-1} \text{ for all } x \in G\} = \cap_{x \in G} H^x$. It is now clear that $\mathrm{Ker}(\tilde{})$ is the largest normal subgroup of G contained in H.

(d) By above $G/\mathrm{Ker}(\tilde{})$ embeds in $\mathrm{Sym}(G/H) \simeq \mathrm{Sym}(n)$.

(e) Take $m = n!$.

(f) Let G be a divisible group and $H \leq G$ a subgroup of index n. Let $g \in G$. Let $h \in G$ be such that $g = h^{n!}$. By the above, $g = h^{n!} \in H$. So $G = H$.

6. Recall that $Z(G) = \{z \in G : zg = gz\}$.

   a) Show that $Z(G) \lhd G$. (3 pts.)

   b) Assume that $G/Z(G)$ is cyclic. Show that G is abelian. (7 pts.)

   Proof: (a) If $z, z_1 \in Z(G)$, then for all $g \in G$, $(zz_1)g = z(z_1g) = z(gz_1) = (zg)z_1 = (gz)z_1 = g(zz_1$, so that $zz_1 \in Z(G)$. Thus $Z(G)$ is closed under multiplication. Clearly $1 \in Z(G)$. Finally, if $z \in Z(G)$, since for all $g \in G$, $gz = zg$, multiplying by z^{-1} from left and right, we see that $gz^{-1} = z^{-1}g$, i.e. $z^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup.

   If $z \in Z(G)$ and $g \in G$, then $g^{-1}zg = z$, so that $g^{-1}Z(G)g \subseteq Z(G)$. This means exactly that $Z(G)$ is a normal subgroup of G.

7. Let G' be the subgroup generated by $\{xyx^{-1}y^{-1} : x, y \in G\}$.

   a) Show that $G' \lhd G$. (5 pts.)

   b) Show that G/G' is abelian. (5 pts.)

   c) Let $H \lhd G$. Show that if G/H is abelian then $G' \leq H$. (5 pts.)

   d) Show that G' is the smallest normal subgroup H of G such that G/H is abelian. (3 pts.)

   e) Let $H = \langle g^2 : g \in G\rangle$. Show that $H \leq G'$. (5 pts.)

   Proof: (a) For x, y, $g \in G$, $g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg)$ and so $g^{-1}(xyx^{-1}y^{-1})g = (g^{-1}xg)(g^{-1}yg)(g^{-1}xg)^{-1}(g^{-1}yg)^{-1}$. Hence $g^{-1}\langle xyx^{-1}y^{-1} : x, y \in G\rangle g \leq$

[1] A group G is called divisible if for any $g \in G$ and any integer $n \geq n$ there is an $h \in G$ such that $g = h^n$.

$\langle xyx^{-1}y^{-1} : x,\, y \in G\rangle$, i.e. $G' := \langle xyx^{-1}y^{-1} : x,\, y \in G\rangle$ is a normal subgroup of G.

(b) For any $\overline{x},\, \overline{y} \in G$, $\overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x^{-1}y^{-1}xy} = \overline{1}$ because $x^{-1}y^{-1}xy \in G'$.

(c) For any $x,\, y \in G$, $\overline{1} = \overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x^{-1}y^{-1}xy}$, i.e. $x^{-1}y^{-1}xy \in H$. It follows that $G' \leq H$.

(d) Follows directly from part (c)

(e) We first claim that if G is a group in which every element has order 2, then G is abelian. Indeed, for any $g, h \in G$, $ghgh = (gh)^2 = 1$, so that $gh = h^{-1}g^{-1} = hg$.

Now we prove (e). Clearly, for any $\overline{g} \in G/H$, $\overline{g}^2 = \overline{1}$. Such a group must be abelian. Thus $G' \leq H$ by part (c).

8. Let X be a set. Let Γ be the set of subsets of X with two elements. On Γ define the relation $\alpha R \beta$ if and only if $\alpha \cap \beta = \emptyset$. Then Γ becomes a graph with this relation.

   a) Calculate $\mathrm{Aut}(\Gamma)$ when $|X| = 4$. (5 pts.)

   b) Draw the graph Γ when $X = \{1, 2, 3, 4, 5\}$. (3 pts.)

   c) Show that Sym(5) imbeds in $\mathrm{Aut}(\Gamma)$ naturally. (5 pts.)

   d) Show that $\mathrm{Aut}(\Gamma) \simeq \mathrm{Sym}(5)$. (7 pts.)

   Answer: (a) The graph Γ is just six vertices joined two by two. A group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ preserves the edges. And Sym(3) permutes the edges. Thus the group has $8 \times 3! = 48$ elements.

   More formally, one can prove this as follows. Let the points be $\{1, 2, 3, 4, 5, 6\}$ and the edges be $v_1 = (1, 4)$, $v_2 = (2, 5)$ and $v_3 = (3, 6)$. We can embed Sym(3) in $\mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(6)$ via

$$\begin{array}{lcl} \mathrm{Id}_3 & \mapsto & \mathrm{Id}_6 \\ (12) & \mapsto & (12)(45) \\ (13) & \mapsto & (13)(46) \\ (23) & \mapsto & (23)(56) \\ (123) & \mapsto & (123)(456) \\ (132) & \mapsto & (132)(465) \end{array}$$

   For any $\phi \in \mathrm{Aut}(\Gamma)$ there is an element α in the image of Sym(3) such that $\alpha^{-1}\phi$ preserves the three edges $v_1 = (1, 4)$, $v_2 = (2, 5)$ and $v_3 = (3, 6)$. Thus $\alpha^{-1}\phi \in \mathrm{Sym}\{1, 4\} \times \mathrm{Sym}\{2, 5\} \times \mathrm{Sym}\{3, 6\} \simeq (\mathbb{Z}/2\mathbb{Z})^3$. It follows that $\mathrm{Aut}(\Gamma) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathrm{Sym}(3)$ (to be explained next year).

   (b) There are ten points. Draw two pentagons one inside the other. Label the outside points as $\{1, 2\}$, $\{3, 4\}$, $\{5, 1\}$, $\{2, 3\}$, $\{4, 5\}$. Complete the graph.

   (c and d) Clearly any element of $\sigma \in \mathrm{Sym}(5)$ gives rise to an automorphism $\tilde{\sigma}$ of Γ via $\tilde{\sigma}\{a, b\} = \{\sigma(a), \sigma(b)\}$. The fact that this map preserves the

incidence relation is clear. This map is one to one because if $\tilde{\sigma} = \tilde{\tau}$, then for all distinct a, b, c, we have $\{\sigma(b)\} = \{\sigma(a), \sigma(b)\} \cap \{\sigma(b), \sigma(c)\} = \tilde{\sigma}\{a, b\} \cap \tilde{\sigma}\{b, c\} = \tilde{\tau}\{a, b\} \cap \tilde{\tau}\{b, c\} = \{\tau(a), \tau(b)\} \cap \{\tau(b), \tau(c)\} = \{\tau(b)\}$ and hence $\sigma(b) = \tau(b)$.

Let $\phi \in \mathrm{Aut}(\Gamma)$. We will compose ϕ by elements of Sym(5) to obtain the identity map. There is an $\sigma \in \mathrm{Sym}(5)$ such that $\phi\{1, 2\} = \tilde{\sigma}\{1, 2\}$ and $\phi\{3, 4\} = \tilde{\sigma}\{3, 4\}$. Thus, replacing ϕ by $\sigma^{-1}\phi$, we may assume that ϕ fixes the vertices $\{1, 2\}$ and $\{3, 4\}$. Now ϕ must preserve or exchange the vertices $\{3, 5\}$ and $\{4, 5\}$. By applying the element (34) of Sym(5) we may assume that these two vertices are fixed as well. Now ϕ must preserve or exchange the vertices $\{1, 3\}$ and $\{2, 3\}$. By applying the element (12) of Sym(5) we may assume that these two vertices are fixed as well. Now all the vertices must be fixed.

33.1.2 Fall 2003 Resit

Throughout G stands for a group.

1. Let $g \in G$ have order n and m an integer. What can you say about the order of g^m? (5 pts.)
2. Let $H, K \leq G$. Show that $\{HxK : x \in G\}$ is a partition of G. (3 pts.)
3. Let $H \leq G$. Show that there is a natural one to one correspondence between the left coset space of H in G and the right coset space of H in G. (3 pts.)
4. Show that the product of two groups is divisible[2] if and only if each factor is divisible. (4 pts.)
5. Show that if $G/Z(G)$ is cyclic then G is abelian. (5 pts.)
6. Find the torsion elements of

   a) $\mathbb{Q}/\mathbb{Z}$. (5 pts.)

   b) $\mathbb{R}/\mathbb{Q}$. (5 pts.)
7. Let $H, K \leq G$. Assume that for all $k \in K$, $H^k \leq H$. Show that $H^k = H$ for all $k \in K$. (5 pts.)
8. Find the isomorphism type of the group $(\mathbb{Z}/11\mathbb{Z})^*$. (5 pts.)
9. Find the isomorphism type of the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (8 pts.)
10. Let p be a prime.

    a. Find the group $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. (5 pts.)

    b. Find $|\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})|$. (5 pts.)

[2] A group G is called divisible if for any $g \in G$ and any integer $n \geq n$ there is an $h \in G$ such that $g = h^n$.

11. Find Aut($\mathbb{Z}$). (5 pts.)
12. Find Aut($\mathbb{Q}$). (5 pts.)
13. Find Aut($\mathbb{Q}^*$). (10 pts.)
14. Find Aut($\mathbb{Z} \times \mathbb{Z}$). (15 pts.)
15. Show that if G is centerless then there is an imbedding of G in Aut(G) (i.e. a one to one group homomorphism from G into Aut(G)). (7 pts.)

33.2 PhD Exams

Part I. Do three (3) of these problems.

1. If a subgroup G of the symmetric group S_n contains an odd permutation, then $|G|$ is even and exactly half the elements of G are odd permutations.
2. Let R be a commutative ring with no nonzero nilpotent elements (that is, $a^n = 0$ implies $a = 0$). If the polynomial $f(X) = a_0 + a_1X + \ldots + a_mX^m$ in $R[X]$ is a zero-divisor (that is, $g(X)f(X) = 0$ for some nonzero polynomial $g(X) \in R[X]$), prove that there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \ldots ba_m = 0$.
3. Let V be a finite-dimensional vector space over a field F. An endomorphism ϕ of V is called a *pseudoreflection* if $\phi - 1$ has rank at most 1. Prove:

   a ϕ is a pseudoreflection precisely if there exists a basis of V such that the matrix of ϕ has the form

$$\begin{pmatrix} * & * & * & \ldots & * \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

   b Show that the Jordan canonical form of a pseudoreflection ϕ is

$$\begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \text{ or } \begin{pmatrix} * & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

I.4 Let $F \supseteq K$ be an algebraic extension of fields and let R be a subring of F with $R \supseteq K$. Show that R is a field.

Part II Do two (2) of these problems.

II.1 Let G be a finite group and let H be a proper subgroup of G. Show that G is not the set-theoretic union of all conjugates of H.

II.2 Let K be the splitting field over the rationals $\mathbb{Q}$ for the polynomial $f(x)$. For each of the following examples, find the degree $[K:\mathbb{Q}]$, determine the structure of the Galois group $G(K/\mathbb{Q})$, describe its action on the roots of $f(x)$ and identify the group.

a) $f(x) = x^4 - 3$

b) $f(x) = x^4 + x^2 - 6$

II.3 Let G be a group of order $165 = 3 \cdot 5 \cdot 11$. Prove:

a) G has a normal Sylow 11-subgroup, say C.

b) G/C is cyclic. (HINT: Show that every group of order 15 is cyclic.)

c) G has normal subgroups of orders 33 and 55.

Questions. **1.** Assume $F \leq K$ is finite and Galois with G as the Galois group. Is there an $\alpha \in K$ such that $G\alpha$ is a basis of K/F (as a vector space)?

2. Let $F \leq K \leq \overline{F}$ where $\overline{F}$ is the algebraic closure of F and $F \leq K$ is finite and Galois with G as the Galois group. For $f = \sum_{i=1}^{m} \alpha_{\vec{i}} X^{\vec{i}}$ and $\sigma \in G$, define $\sigma f = \sum_{i=1}^{m} \sigma(\alpha_{\vec{i}}) X^{\vec{i}}$. For $f_1, \ldots, f_k \in K[\overline{X}]$, define $V_{\overline{F}}(f_1, \ldots, f_k) = \{\overline{x} \in \overline{F}^n : f_j(\overline{x}) = 0 \text{ for all } j = 1, \ldots, k\}$. Assume that $V_{\overline{F}}(f_1, \ldots, f_k) = V_{\overline{F}}(\sigma f_1, \ldots, \sigma f_k)$. Is it true that $V_{\overline{F}}(f_1, \ldots, f_k) = V_{\overline{F}}(g_1, \ldots, g_\ell)$ for some $g_1, \ldots, g_\ell \in F[\overline{X}]$?

3. Let $F \leq K \leq \overline{F}$ be as above. Let $\tau_1, \ldots, \tau_r$ be a basis of K/F. Let $f = \sum_{i=1}^{m} \alpha_{\vec{i}} X^{\vec{i}}$. Write $\alpha_{\vec{i}} = \sum_{\ell=1}^{r} a_{\vec{i},\ell} \tau_\ell$. Then $f = \sum_{i=1}^{m} \sum_{\ell=1}^{r} a_{\vec{i},\ell} \tau_\ell X^{\vec{i}} = \sum_{\ell=1}^{r} \tau_\ell \left(\sum_{i=1}^{m} a_{\vec{i},\ell} \overline{X}^{\vec{i}} \right)$. For $\ell = 1, \ldots, r$, set $(f)_\ell = \sum_{i=1}^{m} a_{\vec{i},\ell} \overline{X}^{\vec{i}}$. Thus $f = \sum_{\ell=1}^{r} \tau_\ell (f)_\ell$.

Now let $V_{\overline{F}}(f_1, \ldots, f_k)$ be as above and assume that $V_{\overline{F}}(f_1, \ldots, f_k) = V_{\overline{F}}(\sigma f_1, \ldots, \sigma f_k)$. Is it true that $V_{\overline{F}}(f_1, \ldots, f_k) = V_{\overline{F}}((f_i)_\ell : i = 1, \ldots, k, \ \ell = 1, \ldots, r)$.

Bibliography

[**C**] J. W. S. Cassels, **Local Fields**, Cambridge University Press, London Mathematical Society Students Texts 3, 1986.

Index