Introduction to Algebra

H113

Mariusz Wodzicki

April 5, 2015

1 Preliminaries

1.1 The language of sets

1.1.1

The concepts of a *set* and of *being an element* of a set,

$$a \in A \qquad (\text{“}a \text{ belongs to } A\text{”}), \tag{1}$$

are the two foundations on which the edifice of modern Mathematics is built. Nearly everything else is expressed using just these two concepts.

1.1.2

A set A is a subset of set B if

$$\textit{for any } a \in A, \textit{ one has } a \in B. \tag{2}$$

We denote this using symbolic notation by $A \subseteq B$ and say that set A is *contained* in set B or, equivalently, that set B *contains* set A.

1.1.3

Sets A and B are declared equal if $A \subseteq B$ and $B \subseteq A$.

1.1.4

A safe guideline is to form new sets only from objects already known to be elements of some sets.

1.1.5

Very few assumptions are made about sets. They are called *axioms* of the Set Theory. Most important for us is the so-called *Separation Axiom* which, for any set A and a well-formed statement $\mathscr{R}(x)$, applicable to an arbitrary element x of A, gurantees the existence of the subset consisting of those $x \in A$ for which $\mathscr{R}(x)$ holds. This subset is denoted as follows

$$\{x \in A \mid \mathscr{R}(x)\}. \tag{3}$$

The name, *Separation Axiom,* signifies the fact that we separate elements $x \in A$ for which $\mathscr{R}(x)$ holds from those for which $\mathscr{R}(x)$ does not hold.

1.1.6

The Separation Axiom guarantees then the existence of the *singleton* sets $\{a\}$. Indeed, if $a \in A$, then

$$\{a\} = \{x \in A \mid x = a\}. \tag{4}$$

1.1.7 The union of two sets

Another axiom guarantees that, for any two sets A and B, there exists a set containing both A and B. If this is so, then we can guarantee that the union, $A \cup B$, exists. Indeed, let C be a set containing both A and B. Then

$$A \cup B = \{c \in C \mid c \in A \text{ or } c \in B\}. \tag{5}$$

1.1.8

Axiom 1.1.7 then guarantees the existence of the sets $\{a, b\}$. Indeed, if $a \in A$ and $b \in B$, then

$$\{a, b\} = \{x \in A \cup B \mid x = a \text{ or } x = b\}. \tag{6}$$

The following lemma is as simple as useful.

Lemma 1.1 *For any elements a, b, and c of a set A, one has*

$$\{a,b\} = \{a,c\} \quad \textit{if and only if} \quad b = c. \tag{7}$$

Proof. If $b \in \{a,c\}$, then either $b = a$ or $b = c$. If $b = a$, then $c \in \{a,b\} = \{b\}$ which means that $b = c$. □

1.1.9 The empty set

Finally, we need a guarantee that there is at least one set. If this is so, then there exists a set with no elements. Indeed, if A is a set, then the set

$$\{a \in A \mid a \notin A\} \tag{8}$$

has no elements.[1] Note that, for another set B,

$$\{a \in A \mid a \notin A\} = \{b \in B \mid b \notin B\}$$

since both are subsets of $C = A \cup B$ and two subsets X, X' of a given set C are equal if and only if

$$\textit{for any } c \in C, \textit{ one has } c \in X \textit{ if and only if } c \in X'. \tag{9}$$

The set with no elements is referred to as the *empty set* and denoted $\emptyset$.

1.1.10 The power set

The third and the last axiom concerned with formation of sets guarantees, for any set A, the existence of the *set of all subsets of A*. We shall denote this set by $\mathscr{P}(A)$.

1.1.11 Families of subsets of a set

A family of subsets of a set A is the same as a subset $\mathcal{X} \subseteq \mathscr{P}(A)$.

[1] Symbol $\notin$ denotes the negation of $\in$; hence, $a \notin A$ reads "a does not belong to A".

1.1.12 The union and intersection of a family of subsets

The *union* is defined as

$$\bigcup \mathcal{X} \ := \ \{a \in A \mid a \in X \text{ for some } X \in \mathcal{X}\} \tag{10}$$

while the *intersection* is defined as

$$\bigcap \mathcal{X} \ := \ \{a \in A \mid a \in X \text{ for all } X \in \mathcal{X}\}. \tag{11}$$

Notation

$$\bigcup_{X \in \mathcal{X}} X \qquad \text{and} \qquad \bigcap_{X \in \mathcal{X}} X$$

is also used.

Exercise 1 *Show that if $\mathcal{X}' \subseteq \mathcal{X}$, then*

$$\bigcup \mathcal{X}' \subseteq \bigcup \mathcal{X} \qquad \textit{and} \qquad \bigcap \mathcal{X}' \supseteq \bigcap \mathcal{X}. \tag{12}$$

1.1.13 The union and intersection of the empty family of subsets

The union and the intersection of a family $\mathcal{X} = \{X\}$ consisting of a single subset $X \subseteq A$, is X itself. The empty family of subsets of A is contained in $\{X\}$, therefore

$$\bigcup \emptyset \subseteq \bigcup \{X\} = X \qquad \text{and} \qquad \bigcap \emptyset \supseteq \bigcap \{X\} = X$$

for every $X \subseteq A$. It follows that

$$\bigcup \emptyset \subseteq \bigcap_{X \subseteq A} X = \emptyset \qquad \text{and} \qquad \bigcap \emptyset \supseteq \bigcup_{X \subseteq A} X = A.$$

Since $\bigcap \mathcal{X}$ for any $\mathcal{X} \subseteq \mathscr{P}(A)$ is a subset of A, we obtain

$$\bigcup \emptyset = \emptyset \qquad \text{and} \qquad \bigcap \emptyset = A.$$

1.1.14

By $\mathscr{P}^*(A)$ we shall denote the set of all nonempty subsets of A. It exists since

$$\mathscr{P}^*(A) \ = \ \{X \in \mathscr{P}(A) \mid X \neq \emptyset\}.$$

1.1.15 Natural numbers represented by sets

Having the empty set, we can construct *natural numbers* as sets:

$$\mathbf{0} := \emptyset, \quad \mathbf{1} := \{\mathbf{0}\}, \quad \mathbf{2} := \{\mathbf{0}, \mathbf{1}\}, \quad \mathbf{3} := \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}, \quad \ldots \tag{13}$$

or, in expanded form,

$$\mathbf{0} := \emptyset, \quad \mathbf{1} = \{\emptyset\}, \quad \mathbf{2} = \{\emptyset, \{\emptyset\}\}, \quad \mathbf{3} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots .$$

1.1.16

For any natural number n, the corresponding set $\boldsymbol{n}$ has as its elements $\boldsymbol{m}$, for all $m < n$. In particular, $\boldsymbol{m} \in \boldsymbol{n}$ for each $m < n$.

Proposition 1.2 *For any n, one has $\boldsymbol{n} \notin \boldsymbol{n}$.*

Proof. Suppose that the assertion does not hold. Let n be the smallest natural number such that $\boldsymbol{n} \in \boldsymbol{n}$. Note that $\mathbf{0} \notin \mathbf{0}$ because $\mathbf{0}$ has no elements. Hence $n > 0$. According to 1.1.16, there exists $m < n$ such that $\boldsymbol{n} = \boldsymbol{m}$. It follows that

$$\boldsymbol{m} \in \boldsymbol{n} = \boldsymbol{m}$$

which contradicts the facat that n is the minimal natural number for which the assertion of Proposition 1.2 fails. □

Corollary 1.3 *If $m \neq n$, then $\boldsymbol{m} \neq \boldsymbol{n}$.*

Proof. If $m < n$, then $\boldsymbol{m} \in \boldsymbol{n}$ but $\boldsymbol{n} \notin \boldsymbol{n}$. Thus $\boldsymbol{m}$ cannot be equal to $\boldsymbol{n}$. □

1.2 The product of sets

1.2.1 An ordered pair

For any elements s and t of a set S, let

$$(s, t) := \{\{s\}, \{s, t\}\}. \tag{14}$$

Note that (14) guaranteed to exist and is a subset of the power set $\mathscr{P}(S)$.

1.2.2

If

$$(s,t) = (s',t'),$$

then $\{s\} = \{s'\}$, in which case $s = s'$, or $\{s\} = \{s',t'\}$. In the former case, we apply Lemma 1.1 to deduce that

$$\{s,t\} = \{s',t'\}$$

and, since $s = s'$, to apply the same lemma again to deduce that $t = t'$.

In the latter case, both s' and t' would be elements of $\{s\}$, and that would mean that

$$s' = s = t', \qquad \text{and} \qquad (s',t') = \{\{s\}\}.$$

In particular,

$$\{s,t\} \in \{\{s\}\}$$

which means that $\{s,t\} = \{s\}$. This in turn implies that $t \in \{s\}$ which means that

$$s = t = s' = t'.$$

□

1.2.3

The above argument establishes the essential property of (14):

$$(s,t) = (s',t') \quad \text{if and only if } s = s' \text{ and } t = t'. \tag{15}$$

In all the applications of the notion of the ordered pair one uses only this property and not its specific realization. You can consider (14) to provide a proof that such an object indeed exists.

1.2.4 The (Cartesian) product of two sets

Definition 1.4 *For any sets X and Y we define their* Cartesian product *to be*

$$X \times Y := \{A \in \mathscr{P}(\mathscr{P}(X \cup Y)) \mid A = (x,y) \textit{ for some } x \in X \textit{ and } y \in Y\}. \tag{16}$$

Note that the set defined in (16) is guaranteed to exist and is a subset of $\mathscr{P}(\mathscr{P}(\mathscr{P}(X\cup Y)))$.

One can rewrite (16) in an informal way as saying

$$X\times Y=\{(x,y)\mid x\in X\text{ and }y\in Y\}. \tag{17}$$

That, however, would still require demonstrating that the set on the right-hand side of (17) exists. Definition (16) is free of this deficiency.

1.2.5 The (Cartesian) product of n sets

Given sets $X_1,\dots,X_n$ we can similarly define $X_1\times\cdots\times X_n$ as the set of n-tuples

$$(x_1,\dots,x_n)$$

with $x_1\in X_1,\dots,x_n\in X_n$. One needs only to provide a corresponding construction-definition of an n-tuple of elements of a set. The sole property of an n-tuple that is being used in the above definition-construction of the product of n sets is the equality principle: two n-tuples are equal if and only if all of their components are equal:

$$(x_1,\dots,x_n)=(x_1',\dots,x_n')\qquad\text{if and only if}\qquad x_1=x_1',\ \dots,\ x_n=x_n'.$$

A convenient implementation of this principle is obtained if we adopt as a model for $(x_1,\dots,x_n)$ the set of pairs

$$\{(1,x_1),\dots,(n,x_n)\}. \tag{18}$$

1.2.6

You may be surprised by the fact that instead of *defining* $(x_1,\dots,x_n)$, we only say that *one can take* (18) as a model for an n-tuple. This is an instance of a very general pheonomenon that has been a constant feature of Modern Mathematics: many important concepts appear as solutions to certain *formally posed problems*. While the solutions are not unique, they all lead to equivalent ways of developing conceptual basis of Mathematics.

1.2.7

Later we shall provide a uniform definition of the Cartesian product of an arbitrary family of sets indexed by another set.

1.2.8 The disjoint union of a family of subsets

The following subset of $\left(\bigcup \mathcal{X}\right) \times \mathcal{X}$,

$$\coprod \mathcal{X} := \left\{(x, X) \in \bigcup \mathcal{X} \times \mathcal{X} \,\middle|\, x \in X\right\} \tag{19}$$

is called the *disjoint union of* $\mathcal{X}$. The difference with the ordinary union is that every element of $\bigcup \mathcal{X}$ *remembers* what $X \in \mathcal{X}$ does it come from. Notation

$$\coprod_{X \in \mathcal{X}} X$$

is also used.

2 Relations

2.1 Relations as "verbs"

2.1.1

Given sets $X_1, \dots, X_n$, a relation $\mathscr{R}$ between elements of these sets should be thought of as a correspondence that assigns to a list of n arguments

$$x_1 \in X_1, \quad \dots, \quad x_n \in X_n,$$

a *statement* that either holds or it does not hold. Such a statement must of course be well formed and unambiguous. Note that the arguments are drawn from the sets $X_1, \dots, X_n$, that must be provided *before* the relation is spelled out. The corresponding relation is referred to as an n*-ary* relation.

2.1.2

For the values of n =1, 2, 3, or 4, we refer to n-ary relations as *unary, binary, ternary, quaternary* relations.

2.1.3

When $X_1, \cdots, X_n$ are equal to a set X, we often say that $\mathscr{R}$ is an n-ary relation *on* set X.

2.1.4 The graph of a relation

The graph of $\mathscr{R}$ is the subset of $X_1 \times \cdots \times X_n$ consisting of those n-tuples $(x_1, \ldots, x_n)$ for which $\mathscr{R}(x_1, \ldots, x_n)$ holds,

$$\Gamma_{\mathscr{R}} := \{(x_1, \ldots, x_n) \in X_1 \times \cdots \times X_n \mid \mathscr{R}(x_1, \ldots, x_n) \text{ holds}\}. \qquad (20)$$

The right hand side of (20) is also written as

$$\{(x_1, \ldots, x_n) \in X_1 \times \cdots \times X_n \mid \mathscr{R}(x_1, \ldots, x_n)\}.$$

2.1.5

Note that the *Separation Axiom* is a statement of the existence of the graph for *unary* relations. The existence of the graph for n-ary relations then follows if one notices that an n-ary relation between elements of $X_1, \ldots, X_n$ gives rise to a *unary* relation on the Cartesian product $X_1 \times \cdots \times X_n$ whose graph coincides with the graph of the original n-ary relation.

2.1.6 The relation associated with $E \subseteq X_1 \times \cdots \times X_n$

If the graph is a subset of $X_1 \times \cdots \times X_n$ canonically associated to a given relation, then there is also a relation canonically associated to a given subset $E \subseteq X_1 \times \cdots \times X_n$. Indeed, the statement

$$(x_1, \ldots, x_n) \in E$$

defines a relation whose graph is E. We shall denote it $\mathscr{R}_E$ and refer to it as the relation *canonically associated* to E. It is the relation of *membership* in E of the n-tuple $(x_1, \ldots, x_n)$.

2.1.7 Permutations acting on relations

Let σ be a permutation of numbers 1 through n. By a permutation we understand a list of n numbers,

$$\sigma(1) \quad , \ldots , \quad \sigma(n),$$

in which each natural number between 1 and n is encountered exactly once.

For any n-ary relation $\mathscr{R}$, we have an associated relation $\mathscr{R}^{\sigma}$ between elements of sets $X_{\sigma(1)}, \ldots, X_{\sigma(n)}$, where

$$\mathscr{R}^{\sigma}(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \tag{21}$$

is the statement

$$\mathscr{R}(x_1, \ldots, x_n).$$

2.2 Comparing relations

2.2.1

Given two n-ary relations between elements of sets $X_1, \ldots, X_n$, we say that $\mathscr{R}$ is *weaker* than $\mathscr{S}$ if

$$\mathscr{S}(x_1, \ldots, x_n) \text{ holds whenever } \mathscr{R}(x_1, \ldots, x_n) \text{ does.}$$

In this situation we also say that $\mathscr{S}$ is *stronger* than $\mathscr{R}$.

Exercise 2 *Show that $\mathscr{R}$ is weaker than $\mathscr{S}$ if and only if $\Gamma_{\mathscr{R}} \subseteq \Gamma_{\mathscr{S}}$.*

2.2.2 Equipotent relations

If $\mathscr{R}$ is both weaker and stronger than $\mathscr{S}$ we say that the two relations are *equipotent*. Note that $\mathscr{R}$ and $\mathscr{S}$ are equipotent if and only if $\Gamma_{\mathscr{R}} = \Gamma_{\mathscr{S}}$.

2.2.3 Weakest and strongest relations

A relation between elements of sets $X_1, \ldots, X_n$, that is *never* satisfied is weaker than any other relation. Similarly, a relation always satisfied is *stronger* than any other relation. The graph of the latter is the whole Cartesian product $X_1 \times \cdots \times X_n$, the graph of the former is empty.

2.2.4 Weakest and strongest relations satisfying a given property

We shall say that a relation $\mathscr{R}$ is a *weakest* relation staisfying a given property $\mathcal{P}$ if $\mathscr{R}$ is weaker than any relation satisfying $\mathcal{P}$ and $\mathscr{R}$ satisfies $\mathcal{P}$ itself. Such a relation may not exist and, when it does exist, is not unique by the very nature of the concept. This is the reason why we employ the indefinite article: *a* weakest.

Exercise 3 *Formulate the dual concept of a strongest relation satisfying a given property $\mathcal{P}$.*

2.2.5 A supremum of a class of relations

Given a nonempty class $\mathcal{R}$ of relations between elements of sets $X_1, \ldots, X_n$, their graphs form a nonempty family of subsets of $X_1 \times \cdots \times X_n$. The relation $\mathscr{R}_{\text{sup}}$ canonically associated to the *union* of this family of subsets,

$$\bigcup_{\mathscr{R} \text{ is in } \mathcal{R}} \Gamma_{\mathscr{R}},$$

is a weakest relation that is stronger than any relation in $\mathcal{R}$. Any relation with this property will be called *a supremum* of the class $\mathcal{R}$.

2.2.6 An infimum of a class of relations

Similarly, the relation $\mathscr{R}_{\text{inf}}$ canonically associated to the *intersection* of the graphs

$$\bigcap_{\mathscr{R} \text{ is in } \mathcal{R}} \Gamma_{\mathscr{R}}$$

is a strongest relation that is weaker than any relation in $\mathcal{R}$. Any relation with this property will be called *an infimum* of the class $\mathcal{R}$.

2.3 Operations on relations

2.3.1 Negation

The statement $\neg\mathscr{R}(x_1, \ldots, x_n)$ is the *negation* of the statement $\mathscr{R}(x_1, \ldots, x_n)$. The graph of the negated relation $\neg\mathscr{R}$ is the complement in $X_1 \times \cdots \times X_n$ of the graph of $\mathscr{R}$,

$$\Gamma_{\neg\mathscr{R}} \;=\; \big(X_1 \times \cdots \times X_n\big) \setminus \Gamma_{\mathscr{R}}.$$

2.3.2 Alternative

The statement $\mathscr{R} \vee \mathscr{S}(x_1, \ldots, x_n)$ reads

$$\mathscr{R}(x_1, \ldots, x_n) \text{ or } \mathscr{S}(x_1, \ldots, x_n). \tag{22}$$

Note that both $\mathscr{R}$ and $\mathscr{S}$ are supposed to be n-ary relations between elements of the same sets. The relation $\mathscr{R}\wedge\mathscr{S}$ is called the *alternative* of $\mathscr{R}$ and $\mathscr{S}$. It is a supremum of the set of relations $\{\mathscr{R},\mathscr{S}\}$, i.e., it is a weakest relation stronger than both $\mathscr{R}$ and $\mathscr{S}$.

The graph of $\mathscr{R}\vee\mathscr{S}$ is the union of the graphs of $\mathscr{R}$ and $\mathscr{S}$,

$$\Gamma_{\mathscr{R}\vee\mathscr{S}} \;=\; \Gamma_{\mathscr{R}} \cup \Gamma_{\mathscr{S}}.$$

2.3.3 Conjunction

The statement $\mathscr{R}\wedge\mathscr{S}(x_1,\dots,x_n)$ reads

$$\mathscr{R}(x_1,\dots,x_n) \text{ and } \mathscr{S}(x_1,\dots,x_n). \tag{23}$$

The relation $\mathscr{R}\wedge\mathscr{S}$ is called the *conjunction* of $\mathscr{R}$ and $\mathscr{S}$. It is an infimum of the set of relations $\{\mathscr{R},\mathscr{S}\}$, i.,e, it is a strongest relation weaker than both $\mathscr{R}$ and $\mathscr{S}$.

The graph of $\mathscr{R}\wedge\mathscr{S}$ is the intersection of the graphs of $\mathscr{R}$ and $\mathscr{S}$,

$$\Gamma_{\mathscr{R}\wedge\mathscr{S}} \;=\; \Gamma_{\mathscr{R}} \cap \Gamma_{\mathscr{S}}.$$

2.3.4 Alternative and conjunction of an indexed family of relations

Given a family $\mathcal{R}$ of n-ary relations between elements of sets $X_1,\dots,X_n$, the statement $\bigvee\mathcal{R}(x_1,\dots,x_n)$ reads

$$\mathscr{R}(x_1,\dots,x_n) \quad \text{for some } \mathscr{R}\in\mathcal{R}, \tag{24}$$

while $\bigwedge\mathcal{R}(x_1,\dots,x_n)$ reads

$$\mathscr{R}(x_1,\dots,x_n) \quad \text{for all } \mathscr{R}\in\mathcal{R}. \tag{25}$$

The relations $\bigvee\mathcal{R}$ and $\bigwedge\mathcal{R}$ are called the *alternative* and, respectively, the *conjunction* of the family of n-ary relations $\mathcal{R}$.

2.3.5

The alternative is a supremum while the conjunction is an infimum of the family of relations $\mathcal{R}$. The alternative is a weakest relation stronger than every member of $\mathcal{R}$, the conjunction is a strongest relation weaker than every member of $\mathcal{R}$.

Exercise 4 *What are the graphs of $\bigvee\mathcal{R}$ and $\bigwedge\mathcal{R}$? Prove your answer.*

2.4 Binary Relations

2.4.1 The subsets of left and right relatives

Any binary relation $\mathscr{R}$ between elements of sets X and Y defines two families of subsets of X and Y, respectively,

$$\mathscr{R}y := \{x \in X \mid \mathscr{R}(x,y)\} \qquad \text{and} \qquad x\mathscr{R} := \{y \in Y \mid \mathscr{R}(x,y)\}. \tag{26}$$

Here $\mathscr{R}y$ is referred to as the *set of left $\mathscr{R}$-relatives* of y, while $x\mathscr{R}$ is the *set of right $\mathscr{R}$-relatives* of x.

2.4.2 The left and right quotient sets

The family of the sets of left $\mathscr{R}$-relatives

$$X_{/\mathscr{R}} := \{A \subseteq X \mid A = \mathscr{R}y \text{ for some } y \in Y\}, \tag{27}$$

will be referred to as the *left quotient set* of $\mathscr{R}$ while the family of the sets of right $\mathscr{R}$-relatives,

$${}_{\mathscr{R}\backslash}Y := \{B \subseteq Y \mid B = x\mathscr{R} \text{ for some } x \in X\}, \tag{28}$$

will be referred to as the *right quotient set* of $\mathscr{R}$.

2.4.3

By definition,

$$X_{/\mathscr{R}} \subseteq \mathscr{P}(X) \qquad \text{and} \qquad {}_{\mathscr{R}\backslash}Y \subseteq \mathscr{P}(Y).$$

The two quotient sets depend only on the graph of the relation.

Exercise 5 *Show that*

$$X_{/\mathscr{R}} = X_{/\mathscr{S}} \qquad \textit{and} \qquad {}_{\mathscr{R}\backslash}Y = {}_{\mathscr{S}\backslash}Y \tag{29}$$

if $\Gamma_{\mathscr{R}} = \Gamma_{\mathscr{S}}$.

2.4.4 Special notation

Binary relations traditionally are denoted using a slightly different notation. For example, the fact that $\mathscr{R}(x, x')$ holds is expressed symbolically as

$$x \sim_{\mathscr{R}} x' \tag{30}$$

or $x \sim x'$, if the binary relation is clear from the context. Various other symbols are used instead of $\sim$, especially for certain types of relations like, e.g., ordering relations.

2.4.5 Composition

Given a binary relation $\mathscr{R}$ between elements of X and Y, and a binary relation $\mathscr{S}$ between elements of Y and Z, we can define their composite $\mathscr{R} \circ \mathscr{S}$ as the relations between elements of X and Z, where the statement $(\mathscr{R} \circ \mathscr{S})(x, z)$ reads

$$\mathscr{R}(x, y) \text{ and } \mathscr{S}(y, z) \text{ for some } y \in Y. \tag{31}$$

2.4.6 Correspondences

We shall refer to subsets of $\mathscr{P}(X \times Y)$ as *correspondences* between sets X and Y. The graph of a binary relation $\mathscr{R}$ between X and Y is a correspondence. Vice-versa, any correspondence $E \subseteq X \times Y$ is the graph of a relation, e.g., of the relation $\mathscr{R}_E$, where $\mathscr{R}_E(x, y)$ is the statement:

$$(x, y) \in E\ . \tag{32}$$

2.4.7 Composition of correspondences

Given sets X, Y, Z, and subsets

$$E \subseteq X \times Y \qquad \text{and} \qquad F \subseteq Y \times Z,$$

let $E \circ F$ be the subset of $X \times Z$ consisting of pairs (x, z) such that

$$(x, y) \in E \quad \text{and} \quad (y, z) \in F \quad \text{for some} \quad y \in Y.$$

Exercise 6 *Prove that the composition of binary relations is associative and*

$$\Gamma_{\mathscr{R} \circ \mathscr{S}} \;=\; \Gamma_{\mathscr{R}} \circ \Gamma_{\mathscr{S}}. \tag{33}$$

2.4.8 The identity relation

For any set X, we shall denote by id_X the **identity** relation on X. The statementr $\mathrm{id}_X(x, x')$ reads

$$x = x'. \tag{34}$$

We may omit subscript X when the set in question is clear from the context.

Exercise 7 *Prove that*

$$\mathrm{id}_X \circ \mathscr{R} \ = \ \mathscr{R} \ = \ \mathscr{R} \circ \mathrm{id}_Y$$

where $\mathscr{R}$ is a binary relation between elements of X and Y.

2.4.9

The graph of the identity relation on X is the *diagonal*

$$\Delta_X := \{(x, x') \in X^2 \mid x = x'\}. \tag{35}$$

2.4.10 The opposite relation

For a relation $\mathscr{R}$ between X and Y, we define the *opposite* relation $\mathscr{R}^{op}$ as the relation between Y and X such that

$$\mathscr{R}^{op}(y, x) \qquad \text{if and only if} \qquad \mathscr{R}(x, y) \qquad (x \in X,\, y \in Y).$$

Note that $\mathscr{R}^{op} = \mathscr{R}^{\sigma}$ where σ is the permutation transposing 1 and 2.

Exercise 8 *Prove that*

$$(\mathscr{R} \circ \mathscr{S})^{op} \ = \ \mathscr{S}^{op} \circ \mathscr{R}^{op}.$$

2.5 Binary relations on a set

2.5.1

Let us consider binary relations on a given set X. For any natural number m, we define $\mathscr{R}^m$ as the m-tuple composition of $\mathscr{R}$,

$$\mathscr{R}^m \ := \ \mathscr{R} \circ \cdots \circ \mathscr{R} \qquad (m \text{ times}), \tag{36}$$

and $\mathscr{R}^0$ to be the identity relation id_X on X.

2.5.2 Transitive relations

We say that a binary relation $\mathscr{R}$ on a set X is *transitive* if, for any $x, x', x'' \in X$,

$$\mathscr{R}(x,x') \quad \text{and} \quad \mathscr{R}(x',x'') \qquad \text{implies} \qquad \mathscr{R}(x,x'').$$

Exercise 9 *Show that $\mathscr{R}$ is transitive if and only if $\mathscr{R}^2$ is weaker than $\mathscr{R}$.*

2.5.3 Transitive closure

Exercise 10 *Prove that, for any relation $\mathscr{R}$, the following relation*

$$\mathscr{R} \vee \mathscr{R}^2 \vee \mathscr{R}^3 \vee \cdots \tag{37}$$

is transitive.

We shall refer to (37) as the *transitive closure* of $\mathscr{R}$. It is a *weakest* transitive relation that is stronger than $\mathscr{R}$.

2.5.4 Symmetric relations

A binary relation on a set X is *symmetric*, if for any $x, x' \in X$,

$$\mathscr{R}(x,x') \qquad \text{implies} \qquad \mathscr{R}(x',x).$$

Exercise 11 *Show that $\mathscr{R}$ is symmetric if and only if $\mathscr{R}$ is weaker than $\mathscr{R}^{\mathrm{op}}$.*

Exercise 12 *Show that $\mathscr{R}$ is weaker than $\mathscr{S}$ if and only if $\mathscr{R}^{\mathrm{op}}$ is weaker than $\mathscr{S}^{\mathrm{op}}$. Deduce from this that $\mathscr{R}$ is symmetric if and only if $\mathscr{R}$ and $\mathscr{R}^{\mathrm{op}}$ are equipotent.*

2.5.5 Symmetric closure (symmetrization)

Exercise 13 *Show that $\mathscr{R} \vee \mathscr{R}^{\mathrm{op}}$ is symmetric.*

We shall refer to $\mathscr{R} \vee \mathscr{R}^{\mathrm{op}}$ as the *symmetric closure*, or *symmetrization*, of $\mathscr{R}$. It is a *weakest* symmetric relation stronger than $\mathscr{R}$.

2.5.6

For symmetric relations, one has $x\mathscr{R} = \mathscr{R}x$, hence the two quotient sets ${}_{\mathscr{R}}\backslash X$ and $X_{/\mathscr{R}}$ coincide. In this case, we shall simply refer to the *quotient of X by $\mathscr{R}$.*

2.5.7 Reflexive relations

A binary relation on a set X is *reflexive*, if $\mathscr{R}(x,x)$ holds for any $x \in X$.

Exercise 14 *Show that $\mathscr{R}$ is reflexive if and only if $\mathscr{R}$ is stronger than* id_X*.*

Exercise 15 *Show that* $\mathrm{id}_X \vee \mathscr{R}$ *is a weakest reflexive relation stronger than $\mathscr{R}$.*

2.5.8 Weakly antisymmetric relations

A binary relation on a set X is *weakly antisymmetric*, if for any $x, x' \in X$,

$$\mathscr{R}(x,x') \quad \text{and} \quad \mathscr{R}(x',x) \qquad \text{implies} \qquad x = x'.$$

Exercise 16 *Show that $\mathscr{R}$ is weakly antisymmetric if and only if $\mathscr{R} \wedge \mathscr{R}^{\mathrm{op}}$ is weaker than* id_X*.*

2.5.9 Preorders

A transitive reflexive relation on a set X is called a *preorder* or *quasiorder*.

Exercise 17 *Show that $\mathscr{R}$ is a preorder if and only if $\Gamma_{\mathscr{R}} \circ \Gamma_{\mathscr{R}} = \Gamma_{\mathscr{R}}$ and $\Delta_X \subseteq \Gamma_{\mathscr{R}}$.*

Exercise 18 *Show that*

$$\widehat{\mathscr{R}} := \mathscr{R}^0 \vee \mathscr{R} \vee \mathscr{R}^2 \vee \mathscr{R}^3 \vee \cdots \tag{38}$$

is a weakest preorder stronger than $\mathscr{R}$.

2.6 Ordering relations

2.6.1

A weakly antisymmetric preorder is called an *ordering* relation.

2.6.2 Notation for ordering relations

Generic notation for an ordering relation employs symbols like $\preceq$, $\leq$, or their variants.

2.6.3 Linear orders versus partial orders

An ordering relation on a set X such that for any $x, x' \in X$, either $\mathscr{R}(x, x')$ or $\mathscr{R}(x', x)$, is called a *linear* (or *total*) *order*. For emphasis, general ordering relations are often referred to as *partial orders*.

2.7 Equivalence relations

2.7.1

A symmetric preorder is called an *equivalence* relation.

2.7.2 Equivalence closure

A weakest equivalence relation stronger than $\mathscr{R}$ will be referred to as the *equivalence closure* of $\mathscr{R}$. Note that such a relation is, by definition, not unique, but any two are equipotent. Its existence follows from Exercise 19 below.

Exercise 19 *Show that $\widehat{\mathscr{R}}$ is symmetric if $\mathscr{R}$ is symmetric. Prove that the relation $\widehat{\mathscr{S}}$, where $\mathscr{S} = \mathscr{R} \vee \mathscr{R}^{\mathrm{op}}$ is the symmetrization of $\mathscr{R}$, is a weakest equivalence relation stronger than $\mathscr{R}$.*

2.7.3 The equivalence class of an element

Given an equivalence relation $\mathscr{R}$ on a set X and an element $x \in X$, the set of its $\mathscr{R}$-relatives, $x\mathscr{R} = \mathscr{R}x$ is referred to as the *equivalence class* of x, and is often denoted $\bar{x}$ or $[x]$.

2.7.4 A partition of a set

A family of subsets $\mathscr{Q} \subseteq \mathscr{P}(X)$ of X is called a *partition* of X if the union of $\mathscr{Q}$ equals X, i.e., if every element of X belongs to some member

$Q \in \mathscr{Q}$, and different members are disjoint,

$$Q \cap Q' \neq \emptyset \qquad \text{implies} \qquad Q = Q' \qquad (Q, Q' \in \mathscr{Q}).$$

Exercise 20 *Given a partition $\mathscr{Q}$ of X, show that the relation $\mathscr{R}_{\mathscr{Q}}$ given by*

$$\mathscr{R}_{\mathscr{Q}}(x, x') \quad \textit{if there exists } Q \in \mathscr{Q} \textit{ that contains both } x \textit{ and } x',$$

is an equivalence relation on X.

2.7.5

We shall call $\mathscr{R}_{\mathscr{Q}}$ the *equivalence relation associated with partition $\mathscr{Q}$*. For this relation,

$$\bar{x} \text{ is the unique member set } Q \in \mathscr{Q} \text{ that contains } x. \tag{39}$$

Exercise 21 *For any equivalence relation $\mathscr{R}$ on X, show that the quotient set $X_{/\mathscr{R}}$ is a partition of X and*

$$\Gamma_{\mathscr{R}} = \bigcup_{Q \in X_{/\mathscr{R}}} Q \times Q. \tag{40}$$

Exercise 22 *Let $\mathcal{R}$ be a family of binary relations on a set X. For each of the following properties: transitive, symmetric, weakly antisymmetric, relexive, preorder, order, equivalence, answer the following question:*

$$\textit{does } \bigwedge \mathcal{R} \textit{ have property } \mathcal{P} \textit{ if every member } \mathscr{R} \in \mathcal{R} \textit{ has it?}$$

Prove your answers.

2.8 Line geometries

2.8.1

A pair of sets $\mathcal{P}$ and $\mathcal{L}$ equipped with a binary relation $\mathscr{I}$ is said to be a *line geometry* if for all pairs of distinct elements $P, P' \in \mathcal{P}$ and $l, l' \in \mathcal{L}$, the corresponding sets of $\mathcal{I}$-relatives have no more than one element in common,

$$|P\mathscr{I} \cap P'\mathscr{I}| \leq 1 \qquad (P \neq P'), \tag{41}$$

and

$$|\mathscr{I}l \cap \mathscr{I}l'| \leq 1 \qquad (l \neq l'). \tag{42}$$

2.8.2 Terminology and notation

Elements of $\mathcal{P}$ are traditionally referred to as *points* while elements of $\mathcal{L}$ are called *lines*. The points are usually denoted by capital letters while the lines are denoted by lower case letters. Finally, $\mathscr{I}$ is called the *incidence relation* between points and lines. Statement $\mathscr{I}(P, l)$ reads:

P is incident to l.

Equivalently, we say that a line l *passes through* a point P or that P *lies on* a line l.

2.8.3 The pencil of lines

For any point P, the set $P\mathscr{I}$ of lines passing through P is called the *pencil* of lines *at* P.

2.8.4 The set of points on a line

Dually, for any line l, the set $\mathscr{I}l$ of points incident to l is called the set of points *on* l.

2.8.5

In geometric terminology $P\mathscr{I} \cap P'\mathscr{I} \neq \emptyset$ reads as

there is a line passing through P and P',

while $\mathscr{I}l \cap \mathscr{I}l' \neq \emptyset$ reads as

lines l and l' intersect each other.

Thus, the pair of conditions (41) and (42) expresses the fact that no more than one line passes through any pair of distinct points P and P', and any pair of distinct lines l and l' *intersects* at no more than a single point.

2.8.6 Collinearity of points

If, for a set of points $\mathcal{Q}$,

$$\bigcap_{P \in \mathcal{Q}} P\mathscr{I} \neq \emptyset,$$

then we say that the points of $\mathcal{Q} \subseteq \mathcal{P}$ are *collinear*.

2.8.7 Concurrence of lines

If, for a set of lines $\mathcal{M}$,

$$\bigcap_{l\in\mathcal{M}} \mathscr{I}l \neq \emptyset,$$

then we say that the lines of $\mathcal{M} \subseteq \mathcal{L}$ are *concurrent*.

2.8.8 Configurations of points and lines

If numbers of points $n = |\mathcal{P}|$ and lines $b = |\mathcal{L}|$ are finite, if the number of lines in each pencil $r = |P\mathscr{I}|$ does not depend on the point, and if the number of points on each line $k = |\mathscr{I}l|$ does not depend on the line, we say that $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ is an (n_r, b_k)*-configuration* of points and lines.

2.8.9 n_r-configurations

In the case when $n = b$ and $r = k$, we talk of n_r-configurations. These are the line geometries with n points and lines with r lines passing through every point and r points on every line.

2.8.10 Incidence geometries

Line geometries are instances of relational systems called *incidence geometries*. Their study has been been particularly intensive in the last 60 years and is at the crossroads of several branches of Mathematics like Combinatorics, Group Theory, Number Theory, Algebraic Geometry, Representation Theory.

2.8.11 Projective planes

By replacing in conditions (41) and (42) inequality by equality,

$$|P\mathscr{I} \cap P'\mathscr{I}| = 1 \qquad (P \neq P'), \tag{43}$$

and

$$|\mathscr{I}l \cap \mathscr{I}l'| = 1 \qquad (l \neq l'), \tag{44}$$

we obtain the definition of a *projective plane* if one, additionally, requests the following two *nondegeneracy* conditions:

$$\begin{array}{l}\textit{there exist three distinct points } P, P', P'' \in \mathcal{P} \\ \textit{such that } P\mathscr{I} \cap P'\mathscr{I} \cap P''\mathscr{I} = \emptyset,\end{array} \tag{45}$$

and, for every $P \in \mathcal{P}$, $P\mathscr{I}$ has at least 3 elements,

$$|P\mathscr{I}| \; > \; 2 \qquad (P \in \mathcal{P}). \tag{46}$$

2.8.12

Thus, the pair of conditions (43) and (44) expresses the fact that a unique line passes through any pair of distinct points P and P', and any pair of distinct lines l and l' *intersects* at a unique point.

Exercise 23 *Let $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ be a binary relation assumed only to satisfy condition* (41)*. Show that if any three distinct points are collinear, then there exists a single line $l \in \mathcal{L}$ such that all points lie on l.*

2.8.13

It follows that a line geometry failing condition (45) has all the points lying on a single line with all the other lines passing through no more than a single point.

Exercise 24 *Let $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ be a binary relation assumed only to satisfy conditions* (43) *and* (44)*. Show that it satisfies nondegeneracy condition* (45) *if and only it satisfies the dual condition*

$$\begin{array}{l} \textit{there exist three distinct lines } l, l', l'' \in \mathcal{L} \\ \textit{such that } \mathscr{I}l \cap \mathscr{I}l' \cap \mathscr{I}l'' = \emptyset, \end{array} \tag{47}$$

Exercise 25 *Let $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ be a binary relation assumed only to satisfy conditions* (43) *and* (44)*. Show that if two distinct lines pass through at least 2 points, then condition* (45) *is automatically satisfied.*

Exercise 26 *Let $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ be a binary relation assumed only to satisfy conditions* (43) *and* (44)*. Show that if two distinct lines pass through at least 3 points, then $(\mathcal{P}, \mathcal{L}, \mathscr{I})$ is a projective plane.*

2.8.14

It follows that the only line geometry satisfying the first 3 conditions defining a projective plane but failing condition (46) has all but one points lying on a single line l with all the other lines passing through exactly 2 points: the unique point *not* on l and a point on l.

The above considerations explain that while conditions (43) and (44) are fundamentally important, the other two conditions exclude just a few degenerate cases.

Exercise 27 *Show that there is a natural bijective correspondence between the pencil of lines $P\mathscr{I}$ passing through a point P and the set of points $\mathscr{I}l$ on a line not passing through P.*

2.8.15 Finite projective planes

Exercise 28 *Show that the number of points $|\mathcal{P}|$ of a projective plane is finite if and only if the number of lines $|\mathcal{L}|$ is finite. Show that in that case the projective plane is a n_r-configuration where $r = q+1$ and $n = q^2+q+1$ for an integer $q > 1$.*

2.8.16 The order of a finite projective plane

The number $q = r-1$ is called the *order* of the finite projective plane. Any power of prime $q = p^d$ occurs as the order and it is conjectured that the order is always a power of prime. Already for the smallest composite number $q = 2 \cdot 3$ proving that no projective plane of order 6 exists is quite difficult. Excluding the next case $q = 2 \cdot 5$ involved computers. General case is still open.

2.9 Mappings

2.9.1 Mappings of n variables

An $(n+1)$-ary relation $\mathscr{R}$ between elements of $X_1, \dots, X_n$ and Y is called a *mapping of n variables* if for every $x_1 \in X_1, \dots, x_n \in X_n$, there exists *precisely* one $y \in Y$ such that $\mathscr{R}(x_1, \dots, x_n, y)$. We shall refer to sets $X_1, \dots, X_n$ as *sources* and to Y as the *target* of the mapping.

2.9.2 Surjective mappings

A mapping is *surjective* if for any $y \in Y$, there exist $x_1 \in X_1, \ldots, x_n \in X_n$ such that $\mathscr{R}(x_1, \ldots, x_n, y)$. Surjective mappings are also called *surjections*.

2.9.3

In the special case of $n = 1$, the single source, denoted simply X, is also referred to as the *domain* of the mapping.

2.9.4 Injective mappings

We then say that the mapping is *injective* if for any $y \in Y$, there is no more than a single $x \in X$ such that $\mathscr{R}(x, y)$.

2.9.5 Bijective mappings

We also say that the mapping is *bijective* if for any $y \in Y$, there is exactly one $x \in X$ such that $\mathscr{R}(x, y)$. Bijective mappings are also called *bijections*.

Exercise 29 *Show that $\mathscr{R}$ is a bijection if and only if both $\mathscr{R}$ and $\mathscr{R}^{\mathrm{op}}$ are mappings.*

2.9.6 Functional notation for mappings

The single element $y \in Y$ such that $\mathscr{R}(x_1, \ldots, x_n, y)$ will be denoted

$$f_{\mathscr{R}}(x_1, \ldots, x_n) \tag{48}$$

or $f(x_1, \ldots, x_n)$, if the relation is clear from the context. We refer to (48) as the *value* of the mapping for $x_1, \ldots, x_n$. The symbol f in this generic notation may be replaced by many other symbols or by a word like exp, log, etc, which stands for an abbreviated name of the mapping.

2.9.7 Equality of mappings

We did not say what it means that two relations are *equal*. For mappings, however, we shall say that mappings $\mathscr{R}$ and $\mathscr{S}$ are equal if their sources and the target coincide *and* they take the same values, i.e.,

$$f_{\mathscr{R}}(x_1, \ldots, x_n) \;=\; f_{\mathscr{S}}(x_1, \ldots, x_n)$$

for all $x_1 \in X_1, \dots, x_n \in X_n$. In other words, mappings $\mathscr{R}$ and $\mathscr{S}$ are declared to be equal if and only if they are *equipotent* as relations, which happens precisely when their graphs coincide.

2.9.8 The arrow notation

For mappings from X to Y the notation

$$f\colon X \longrightarrow Y \qquad \text{or} \qquad X \xrightarrow{f} Y \tag{49}$$

is commonly used to signal that f is a mapping with the source X and the target Y. We shall extend it to mappings of n variables by placing the *list* of its sources at the tail,

$$f\colon X_1, \dots, X_n \longrightarrow Y \qquad \text{or} \qquad X_1, \dots, X_n \xrightarrow{\quad f \quad} Y\ . \tag{50}$$

2.9.9

The above should alert you to the fact that even though mappings between sets form a special kind of binary relations, they come with their own notational and terminological conventions.

From now on the word *mapping* means *mapping of a single variable* unless stated otherwise.

2.9.10 Composition of mappings

Since binary relations can be composed, mappings can be composed too.

Exercise 30 *Show that if $\mathscr{R}$ and $\mathscr{S}$ are mappings, then $\mathscr{R} \circ \mathscr{S}$ is a mapping.*

Note that in the *functional notation* the composition order is reversed:

$$f_{\mathscr{S}} \circ f_{\mathscr{R}} \;=\; f_{\mathscr{R} \circ \mathscr{S}}$$

This is due to the fact that we denote the value of f on x as $f(x)$ and not $(x)f$.

2.9.11 Composition of mappings of n variables

Mappings of n variables can be composed too but their composition is more elaborate. Given

$$X_1, \dots, X_m \xrightarrow{g} Y_i \qquad \text{and} \qquad Y_1, \dots, Y_n \xrightarrow{f} Z \ ,$$

the mapping

$$Y_1, \dots, Y_{i-1}, X_1, \dots, X_m, Y_{i+1}, \dots, Y_n \xrightarrow{f \circ_i g} Z \tag{51}$$

is defined by

$$\begin{aligned} f \circ_i g\,(y_1, \dots, y_{i-1}, x_1, \dots, x_m, y_{i+1}, \dots, y_n) & \\ := f(y_1, \dots, y_{i-1}, g(x_1, \dots, x_m), y_{i+1}, \dots, y_n). \end{aligned} \tag{52}$$

Note that the *source list* of $f \circ_i g$ is obtained by inserting the source list of g into the source list of f *in place* of the *target* of g.

2.9.12 The canonical inclusion maps

With any subset $A \subseteq X$, there is an associated the mapping

$$\iota_{A \subset X} \colon A \longrightarrow X, \qquad x \longmapsto x \qquad (x \in A).$$

When X is clear from the context, this mapping can be denoted ι_A, or simply ι.

2.9.13

Note that this mapping is defined also when A is empty. The inclusion of the empty set into a set X is the unique mapping from $\emptyset$ to X.

2.9.14 Retractions

Given a set X and a subset A, a mapping $f \colon X \longrightarrow X$ is said to be a *retraction* onto A if $f(X) = A$ and f restricted to A is the inclusion ι_A.

2.9.15 The image of a mapping

The set

$$\{y \in Y \mid y = f(x) \text{ for some } x \in X\}$$

is called the *image* of a mapping $f\colon X \longrightarrow Y$. The image is usually denoted $f(X)$ where X denotes the source of f.

Exercise 31 *Show that a mapping $f\colon X \longrightarrow X$ is a retraction onto $A \subseteq X$ if and only if $f \circ f = f$ and $f(X) = A$.*

2.9.16 The inverse mapping

The opposite relation for a mapping may not be a mapping. According to Exercise 29, it is if and only if the mapping is a bijection. In functional notation the opposite relation is then denoted f^{-1} and is referred to as the *inverse* mapping.

2.10 Indexed families

2.10.1 Families of elements of a set indexed by a set

A family of elements of a set X indexed by a set I is the same as an arbitrary mapping $I \longrightarrow X$. The only difference is the notation used, $(x_i)_{i \in I}$ and

$$i \longmapsto x_i \qquad (i \in I),$$

instead of, say, $f\colon I \longrightarrow X$ and $f(i)$. This terminology is traditionally employed when the focus is on x_i themselves as members of X while the indexing set I plays an auxiliary role. We typically encounter this situation when talking about *sequences* of elements of a set. In this case, it is of secondary importance whether we label terms of a sequence by the set of natural numbers $\mathbf{N}$, by the set of positive integers $\mathbf{Z}_+$, or by the set of positive even integers.

2.10.2 I-tuples

Families $(x_i)_{i \in I}$ of elements of a set X are also referred to as I-tuples.

2.11 Operations involving indexed families of sets

2.11.1 Families of sets indexed by a set

A family of sets indexed by a set I, is defined provided it is understood that all X_i are subsets of some common set, say A. It is the same as a family of elements of $\mathscr{P}(A)$ indexed by I.

2.11.2 The union of an indexed family of sets

For any family of sets, one can take A to be the *union* of all X_i,

$$\bigcup_{i\in I} X_i \ := \ \{a \in A \mid a \in X_i \text{ for some } i \in I\}. \tag{53}$$

Note that the set defined in (53) *does not* depend on A as long as A contains *every* X_i.

2.11.3 The intersection of an indexed family of sets

For any family of sets, one can take A to be the *union* of all X_i,

$$\bigcap_{i\in I} X_i \ := \ \{a \in A \mid a \in X_i \text{ for some } i \in I\}. \tag{54}$$

Note that the set defined in (53) *does not* depend on A as long as A contains at least a single X_i.

2.11.4 The disjoint union of a family of sets indexed by a set

The following subset of $\left(\bigcup_{i\in I} X_i\right)\times I$,

$$\coprod_{i\in I} X_i \ := \ \left\{(x,i) \in \bigcup_{i\in I} X_i\times I \,\middle|\, x \in X_i\right\} \tag{55}$$

is called the *disjoint union of* $(X_i)_{i\in I}$. The difference with the ordinary union is that every element of $\bigcup_{i\in I} X_i$ rememberes what X_i does it come from.

Exercise 32 *Show that the canonical mapping*

$$\coprod_{i\in I} X_i \longrightarrow \bigcup_{i\in I} X_i, \qquad (x,i) \longmapsto x, \tag{56}$$

is surjective. Show that it is injective if and only if all X_i *are disjoint, i.e.,*

$$X_i \cap X_j \neq \emptyset \qquad \textit{implies that} \qquad i = j.$$

2.11.5 The canonical inclusions into the disjoint union

For any $j \in I$, the mapping

$$\iota_j \colon X_j \longrightarrow \coprod_{i\in I} X_i, \qquad x \longmapsto (x,j), \tag{57}$$

will be called the *canonical inclusion* of X_j into the disjoint union.

2.11.6 The universal property of the disjoint union

The family of canonical inclusions $(\iota_j)_{j\in I}$ has the property that, for any set Y and any family of mappings $(f_j)_{j\in I}$,

$$f_j \colon X_j \longrightarrow Y \qquad (j \in I),$$

there exists a unique mapping $f \colon \coprod_{i\in I} X_i \longrightarrow Y$ such that

$$f_j \;=\; f \circ \iota_j \qquad (j \in I).$$

Indeed, let

$$f\big((x,i)\big) \;:=\; f_i(x) \qquad (i \in I).$$

2.11.7 The Cartesian product of an indexed family of sets

The product of $(X_i)_{i\in I}$ is defined as the set of I-tuples $(x_i)_{i\in I}$ in

$$A \;=\; \bigcup_{i\in I} X_i$$

such that each x_i is a member of X_i,

$$\prod_{i\in I} X_i \;:=\; \big\{ (x_i)_{i\in I} \mid x_i \in X_i \text{ for each } i \in I \big\}. \tag{58}$$

2.11.8 The canonical projections from the Cartesian product

For any $j \in I$, 'evaluation at j' defines a mapping that sends an I-tuple to its j-th component,

$$\pi_j \colon \prod_{i \in I} X_i \longrightarrow X_j \tag{59}$$

that will be called the *canonical projection onto* X_j.

2.11.9 The universal property of the Cartesian product

The family of canonical projections $(\pi_j)_{j \in I}$ has the property that, for any set W and any family of mappings $(g_j)_{j \in I}$,

$$g_j \colon W \longrightarrow X_j \qquad (j \in I),$$

there exists a unique mapping $g \colon W \longrightarrow \prod_{i \in I} X_i$ such that

$$g_j \;=\; \pi_j \circ g \qquad (j \in I).$$

Indeed, let $g(w)$ be an I-tuple whose j-th component equals

$$g(w)_j \;:=\; g_j(w) \qquad (j \in I).$$

2.11.10 The duality between disjoint union and Cartesian product

The universal properties enjoyed by disjoint union and Cartesian product are dual to each other. They can be also expressed as natural bijective correspondences

$$\Big\{ \big(f_j \colon X_j \longrightarrow Y\big)_{j \in I} \Big\} \;\longleftrightarrow\; \Big\{ f \colon \coprod_{i \in I} X_i \longrightarrow Y \Big\} \tag{60}$$

and

$$\Big\{ \big(g_j \colon W \longrightarrow X_j\big)_{j \in I} \Big\} \;\longleftrightarrow\; \Big\{ g \colon W \longrightarrow \prod_{i \in I} X_i \Big\}. \tag{61}$$

2.11.11 Some special cases

When $I = \{1, \ldots, n\}$, we often use notation

$$X_1 \sqcup \cdots \sqcup X_n$$

instead of

$$\coprod_{i\in\{1,\ldots,n\}} X_i \qquad \text{or} \qquad \coprod_{i=1}^{n} X_i,$$

and

$$X_1 \times \cdots \times X_n$$

instead of

$$\prod_{i\in\{1,\ldots,n\}} X_i \qquad \text{or} \qquad \prod_{i=1}^{n} X_i.$$

2.11.12

When $X_i = X$ for all $i \in I$, we employ the notation X^I instead of

$$\prod_{i\in I} X.$$

2.11.13 Mappings of several versus mappings of a single variable

The Cartesian product allows one to convert a mapping f of n variables from $X_1, \ldots, X_n$ to Y into a mapping of a single variable from $X_1 \times \cdots \times X_n$ to Y,

$$\bar{f}\big((x_1, \ldots, x_n)\big) := f(x_1, \ldots, x_n).$$

Vice versa, any mapping from $X_1 \times \cdots \times X_n$ to Y, arises this way from a unique mapping of n variables. From the notational point of view the difference is cosmetic, from the point of view of concepts the difference is, however, enormous. The above remark allows to represent mappings of several variables as mappings of a single variable.

2.11.14 The Cartesian product of a family of mappings

With a family of mappings $f_i\colon X_i \longrightarrow Y_i$, one can naturally associate a mapping

$$\prod_{i\in I} f_i\colon \prod_{i\in I} X_i \longrightarrow \prod_{i\in I} Y_i \qquad (x_i)_{i\in I} \longmapsto \big(f_i(x_i)\big)_{i\in I}. \tag{62}$$

Note that its source and its target are the products of the sources and, respectively, of the targets of the component mappings f_i.

2.11.15

For $I = \{1, \dots, n\}$ we use the notation

$$f_1 \times \cdots \times f_n : X_1 \times \cdots \times X_n \longrightarrow Y_1 \times \cdots \times Y_n.$$

2.12 Operations involving indexed families of relations

2.12.1 Alternative and conjunction

Given a family $(\mathscr{R}_i)_{i\in I}$ of n-ary relations between elements of sets $X_1, \dots, X_n$, the statement $\bigvee_{i\in I} \mathscr{R}_i(x_1, \dots, x_n)$ reads

$$\mathscr{R}_i(x_1, \dots, x_n) \quad \text{for some } i \in I, \tag{63}$$

while $\bigwedge_{i\in I} \mathscr{R}_i(x_1, \dots, x_n)$ reads

$$\mathscr{R}_i(x_1, \dots, x_n) \quad \text{for all } i \in I. \tag{64}$$

The relations $\bigvee_{i\in I} \mathscr{R}_i$ and $\bigwedge_{i\in I} \mathscr{R}_i$ are called the *alternative* and, respectively, the *conjunction* of the family of n-ary relations $(\mathscr{R}_i)_{i\in I}$.

2.12.2

The alternative is a *weakest* relation *stronger than every relation* of the family $(\mathscr{R}_i)_{i\in I}$. The conjunction is a *strongest* relation *weaker than every relation* of that family.

2.13 The kernel equivalence

2.13.1

Let $\mathscr{R}$ be a binary relation between elements of sets X and Y.

Exercise 33 *Show that $\mathscr{R} \circ \mathscr{R}^{op}$ is symmetric.*

Exercise 34 *Show that $\mathscr{R} \circ \mathscr{R}^{op}$ is reflexive if and only if $x\mathscr{R}$ is not empty for any $x \in X$.*

2.13.2 Transitive families of sets

We shall say that a family $(X_i)_{i \in I}$ of sets is *transitive* if

$$X_i \cap X_j \neq \emptyset \quad \text{and} \quad X_j \cap X_k \neq \emptyset \quad \text{implies} \quad X_i \cap X_k \neq \emptyset. \tag{65}$$

Exercise 35 *Show that $\mathscr{R} \circ \mathscr{R}^{op}$ is transitive if and only if the family $(x\mathscr{R})_{x \in X}$ of subsets of Y is transitive.*

2.13.3

Any family of sets having no more than one element is obviously transitive, hence $\mathscr{R} \circ \mathscr{R}^{op}$ is an equivalence relation on X when $\mathscr{R}$ is a mapping from X to Y. It is called the *kernel equivalence* associated with the mapping. The equivalence classes of this relation are called the *fibers* of the mapping.

3 Algebraic operations

3.1 n-ary operations

3.1.1

A mapping

$$\mu \colon X^n \longrightarrow X$$

is called an n-ary operation on a set X. The result of applying the operation to n elements $x_1, \dots, x_n$, i.e., the value $\mu(x_1, \dots, x_n)$, is referred to as the *product* of $x_1, \dots, x_n$ and the operation os often referred as the *multiplication*.

3.1.2 n-ary operations as $(n+1)$-ary relations

An n-ary operation on a set X determines an $(n+1)$-ary relation, $\mathscr{R}_\mu$, where

$$\mathscr{R}_\mu(x_1,\ldots,x_n,x_{n+1})$$

is the statement

$$\mu(x_1,\ldots,x_n)=x_{n+1}.$$

Vice-versa, any $(n+1)$-ary relation $\mathscr{R}$ on a set X such that, for any elements $x_1,\ldots,x_n\in X$, there is a unique x_{n+1} such that $\mathscr{R}(x_1,\ldots,x_n,x_{n+1})$ holds, is obtained in this way.

3.1.3 0-ary operations

Since X^0 has exactly one element (namely $\iota_{\emptyset\subset X}$), a 0-ary operation on a set X amounts to making one element of X a *distinguished* element.

3.1.4

For the values of $n=$0, 1, 2, 3, or 4, we refer to n-ary operations as *nullary, unary, binary, ternary, quaternary* operations.

3.1.5 Prefix notation

If one denotes the product by

$$\mu x_1\ldots x_n \tag{66}$$

then one can dispose of the need to use parentheses even for iterated applications of the product. For example, for a ternary operation, denoted $\triangleright$,

$$\triangleright\triangleright\triangleright xyzxyxy$$

parses as $\triangleright(\triangleright(\triangleright(x,y,z),x,y),x,y)$ while

$$\triangleright x\triangleright y\triangleright zxyxy$$

parses as $\triangleright(x,\triangleright(y,\triangleright(z,x,y),x),y)$.

3.1.6 Postfix notation

This prefix notation was introduced around 1924 by Polish logician Jan Łukasiewicz. By symmetry, one can also employ the postfix notation

$$x_1 \dots x_n \mu \tag{67}$$

Both prefix and postfix notation are well suited to stack manipulation of data in computers. The latter is more popular than the former, the reason being probably that in languages written left-to-right it is easier to parse expressions from left-to-right. It is often referred to as the *Reverse Polish Notation*.

Exercise 36 *Parse the following expression in the postfix notation where $/$ denote a binary operation*

$$xyz/yx/// \tag{68}$$

(*Hint. You should be parsing from left to right, each time you encounter symbol $/$, you should perform the corresponding operation and replace the involved symbols by the result and start the parsing process again.*)

Exercise 37 *Parse the following expression in the postfix notation where $/$ denote a binary operation*

$$xxx/y/z/xx/x/z/// \tag{69}$$

3.2 n-ary structures

3.2.1

A set equipped with an n-ary operation is often referred to as an *n-ary structure*.

3.2.2 Substructures

A subset $X' \subseteq X$ is said to be *closed* under the operation if

$$\mu(x_1, \dots, x_n) \in X' \qquad \text{whenever} \qquad x_1, \dots, x_n \in X'.$$

In that case restricting μ to $(X')^n$ and narrowing its target to X' defines an n-ary structure on X'. The obtained operation will be called the *restriction of μ to X'*.

Exercise 38 *Let $(X'_i)_{i \in I}$ be a family of subsets of X such that each X'_i is closed under μ. Show that their intersection*

$$\bigcap_{i \in I} X'_i \tag{70}$$

is closed under μ too.

3.2.3 The substructure generated by a subset

For any subset $A \subseteq X$ of an n-ary structure (X, μ), the family of subsets $X' \subseteq X$ containing A and closed under μ is nonempty: it contains, for example X itself. By Exercise 38, their intersection is closed under μ. The intersection is the smallest subset of X containing A with this property. It will be denoted $\langle A \rangle$ henceforth. The corresponding substructure of (X, μ) is called the *substructure of (X, μ) generated by a subset $A \subseteq X$*.

Exercise 39 *Given a family of subsets $X_i \subseteq X$ closed under μ, their intersection* (70) *is the largest subset of X, closed under μ, which is contained in each X_i. What is the* smallest *subset of X which is closed under μ and contains every X_i?*

3.2.4 Sets of generators

We say that a subset $A \subseteq X$ *generates* (X, μ) if $\langle A \rangle = X$. We refer to such A as a *set of generators* for (X, μ).

3.2.5 The n-ary structure of words

Consider the set of *finite* sequences of elements of a set A,

$$A^{<\infty} := A \cup A \times A \cup A \times A \times A \cup \cdots \tag{71}$$

Note that all the summands are disjoint.[2] We shall refer to elements of $A^{<\infty}$ as *words in alphabet A*. Concatenation of n words of lengths $l_1, \ldots, l_n$ produces a word of length $l_1 + \cdots + l_n$,

$$\big((a_{11}, \ldots, a_{1l_1}), \ldots, (a_{n1}, \ldots, a_{nl_n})\big) \longmapsto (a_{11}, \ldots, a_{1l_1}, \ldots, a_{n1}, \ldots, a_{nl_n}).$$

[2] A student voiced an objection whether we can be certain that the summands in (71) are indeed disjoint. The answer is immediately seen to be *yes*, if we view $A^{<\infty}$ as the union

$$A^1 \cup A^2 \cup A^3 \cup \cdots,$$

This produces a bijective mapping

$$A^{l_1}\times\cdots\times A^{l_n}\longrightarrow A^{l_1+\cdots+l_n}$$

and, since $\left(A^{<\infty}\right)^n$ is a disjoint union of the family of n-tuple products

$$A^{l_1}\times\cdots\times A^{l_n}$$

indexed by n-tuples $(l_1,\dots,l_n)\in\mathbf{Z}_+^n$, we obtain an operation

$$\mathrm{conc}_n\colon\left(A^{<\infty}\right)^n\longrightarrow A^{<\infty}\tag{72}$$

called *concatenation of n words.*

3.2.6 Notation

When possible we shall omit commas separating terms in a finite sequence, thus

$$a_1,a_2,\dots,a_l$$

becomes

$$a_1a_2\dots a_l.$$

This is where the 'words' terminology comes from.

Exercise 40 *Under which conditions A generates the n-ary structure of words?*

3.2.7

Among all n-ary structures containg a given set A and generated by A, there is one that is fundamentally important. We shall give its construction now.

since each A^n is the set of mappings from n to A and the sets of different cardinalities are different, hence $A^m\neq A^n$ for $m\neq n$. But also the set A itself must be disjoint from each A^n: otherwise it would contain a mapping $\alpha\colon n\longrightarrow A$. Such a mapping is defined only if A is defined. In other words, all its elements must be *determined* prior to considering any mappings into A. So α must be defined *before* one can define any mappings into A. But α is a mapping into A so it was defined only *after* all elements of A have been determined. This difficulty indicates that one cannot accept as valid sets that could contain mappings into themselves as their own elements. In other words, A must be considered disjoint with each A^n, including A^1. Of course, it is a common practice to *identify* A with A^1 even though the two sets are not equal.

3.2.8 The free n-ary structure generated by a set

Given a set A, let us adjoin to it an element, denoted $*$, that does not belong to it (e.g., we can take $*$ to be the unique element of A^0 which, by definition, does not belong to A). Let $\tilde{A} := A \cup \{*\}$.

Consider the following n-ary operation on $\tilde{A}^{<\infty}$ obtained by concatenating $n+1$ words in alphabet $\tilde{A}$ with $*$ placed as the first word,

$$(w_1, \ldots, w_n) \longmapsto \mathrm{conc}_{n+1}(*, w_1, \ldots, w_n). \tag{73}$$

We shall refer to (73) as *free n-ary multiplication*.

If we consider the n-ary structure on $\tilde{A}^{<\infty}$ given by free n-ary multiplication, then the substructure generated by $A \subseteq \tilde{A}^{<\infty}$ is called the *free n-ary structure on A*. We shall denote it $F_n(A)$. When $A = \{a_1, \ldots, a_n\}$ (with all a_i different), then $F_n(A)$ will be also denoted $F_n(a_1, \ldots, a_n)$.

3.3 Congruences

3.3.1 The induced operation on the power set

An n-ary operation μ on a set X, *induces* an n-ary operation on the set of all subsets $\mathscr{P}(X)$,

$$(A_1, \ldots, A_n) \ \longmapsto \ \mu(A_1, \ldots, A_n)$$

where $\mu(A_1, \ldots, A_n)$ is defined as the subset of X formed by all n-ary products $\mu(a_1, \ldots, a_n)$ where $a_q, \ldots, a_n$ run through the elements of $A_1, \ldots, A_n$,

$$\{x \in \mathrm{X} \mid x = \mu(a_1, \ldots, a_n) \text{ for some } a_1 \in A_1, \ldots, a_n \in A_n\}. \tag{74}$$

3.3.2

Since $AB \neq \emptyset$ when both A and B are nonempty, the set of nonempty subsets $\mathscr{P}^*(X)$ is closed under μ and $(\mathscr{P}^*(X), \mu)$ becomes a substracture of $(\mathscr{P}(X), \mu)$.

3.3.3

An equivalence relation $\sim$ on a set X equipped with an n-ary operation μ is said to be a *congruence* if

$$x_1 \sim x_1', \; \ldots, \; x_n \sim x_n' \qquad \text{implies} \qquad \mu(x_1, \ldots, x_n) \sim \mu(x_1', \ldots, x_n') \quad (75)$$

for any $x_1, \ldots, x_n, x_1', \ldots, x_n' \in X$.

Exercise 41 *Prove that, for any congruence relation, the product of the equivalence classes of $x_1, \ldots, x_n$ (in the sense of Section 3.3.1) is contained in the equivalence class of $\mu(x_1, \ldots, x_n)$,*

$$\mu(\bar{x}_1, \ldots, \bar{x}_n) \subseteq \overline{\mu(x_1, \ldots, x_n)} \qquad (x_1, \ldots, x_n \in X). \qquad (76)$$

3.3.4 Quotient structures

The n-ary operation induces on the quotient set $X_{/\sim}$ the operation by setting

$$\bar{\mu}(C_1, \ldots, C_n) \qquad (77)$$

to be the *unique* equivalence class containing the product $\mu(C_1, \ldots, C_n)$ of equivalence classes $C_1, \ldots, C_n$. We refer to $(X_{/\sim}, \bar{\mu})$ as the *quotient structure*.

3.3.5 Product structures

Given a pair of n-ary structures (X, μ) and $(X,', \mu')$, we obtain a canonical n-ary structure on $X \times X'$,

$$\mu \times \mu' \colon (X \times X')^n \longrightarrow X \times X'$$

where

$$\mu \times \mu'\big((x_1, x_1'), \ldots, (x_n, x_n')\big) := \big(\mu(x_1, \ldots, x_n), \mu'(x_1', \ldots, x_n')\big). \qquad (78)$$

Exercise 42 *Prove that an equivalence relation $\sim$ on X is a congruence if and only if $\Gamma_\sim \subseteq X \times X$ is closed under $\mu \times \mu$.*

3.3.6

In other words, $\sim$ is a congruence precisely when its graph is a substructure of $(X\times X, \mu\times\mu)$. For this reason, we shall be also talking of the *quotients of* (X, μ) *by substructures of* $(X\times X, \mu\times\mu)$.

3.3.7 Products of arbitrary families of structures

Given any family of n-ary structures $\Big((X_i, \mu_i)\Big)_{i\in I}$, the product set $\prod_{i\in I} X_i$ is naturally equipped with the n-ary operation

$$\Big(\prod_{i\in I} X_i\Big)^n \longrightarrow \prod_{i\in I} X_i^n \longrightarrow \prod_{i\in I} X_i \tag{79}$$

where the second arrow is the product of mappings μ_i, cf. (62), while the first arrow identifies $\Big(\prod_{i\in I} X_i\Big)^n$ with $\prod_{i\in I} X_i^n$ by viewing both of these repeated products as the single product of the family

$$(i,j) \longmapsto X_i \qquad (i \in I;\, 1 \leq j \leq n),$$

of sets indexed by $I\times\{1,\dots,n\}$. Explicitly,

$$\Big((x_{i1})_{i\in I}, \dots, (x_{in})_{i\in I}\Big) \longmapsto \Big(\mu_i(x_{i1}, \dots, x_{in})\Big)_{i\in I}. \tag{80}$$

We shall refer to operation (80) on $\prod_{i\in I} X_i$ as the *product* of operations μ_i, $i \in I$.

4 Binary structures

4.1 Binary operations

4.1.1 Infix notation

In the case of a binary operation, the product $\mu(x, y)$ is usually denoted

$$x\cdot y \qquad \text{or} \qquad xy.$$

There are situations when instead of $\cdot$ a different symbol is used, e.g., $+$, $\times$, etc. The infix notation is both traditional and is particularly useful in expressions with iterated applications of the operation.

Exercise 43 *Rewrite expression* (68) *in infix notation.*

Exercise 44 *Rewrite expression* (69) *in infix notation.*

4.1.2 The induced binary operation on the power set

If the notation $x \cdot y$ or xy is employed to denote the product of two elements, then the notation for the product of two subsets is $A \cdot B$ or AB.

A notable special case occurs when one of the two sets has just one element. In this case we employ a simplified notation

$$aB := \{a\}B \qquad \text{and} \qquad Ab := A\{b\}. \tag{81}$$

4.1.3 Example: webs

Let A be a set equipped with 3 equivalence relations $\sim$, $\sim'$ and $\sim''$. Its elements will be referred to as "points". The associated partitions will be denoted L, L' and L'', and its elements will be referred to as "lines". Lines belonging to the same partition will be said to be "parallel". Such a structure is called a *web* if

any two lines that are not parallel intersect in exactly one point. (82)

Define the following mapping

$$L' \times L'' \longrightarrow L, \qquad (l', l'') \longmapsto l' * l'' \tag{83}$$

where $l' * l''$ is the unique line of L passing through the point of intersection of lines $l' \in L'$ and $l'' \in L''$.

Fix three lines $e \in L$, $e' \in L'$ and $e'' \in L''$ which intersect at a single point.

Exercise 45 *Show that the correspondences* $L \longrightarrow L'$ *and* $L \longrightarrow L''$ *given by*

$$l \longmapsto m' \qquad \textit{and} \qquad l \longmapsto m''$$

are bijective where $m' \in L'$ *denotes the unique line passing through the point of intersection of* l *with* e'' *and* $m'' \in L''$ *denotes the unique line passing through the point of intersection of* l *with* e'*.*

Exercise 46 *Show that*

$$e' * m'' = l = m' * e''. \tag{84}$$

It follows that all three families of lines have the same cardinality. For any set Q and any choice of bijections between Q and sets L, L', L'', the operation (83) induces a binary operation on set Q,

$$(q,r) \longmapsto q \cdot r \qquad (q,r \in Q). \tag{85}$$

Exercise 47 *Show that, for any $q,r,s \in Q$, the equations*

$$q \cdot x = s \qquad \text{and} \qquad x \cdot r = s$$

have a unique solution $x \in Q$.

4.1.4 Quasigroups

Any binary structure having the above property is said to be a *quasigroup*. The quasigroup Q defined above is referred as the *coordinate quasigroup* of the web $(A, \sim, \sim', \sim'')$. Its definition involves a choice of identifications of families L, L' and L'' with a given set Q.

Exercise 48 *Show that a quasigroup structure on a set X is the same as a ternary relation $\mathscr{R}$ on X such that $\mathscr{R}^\sigma$ is a mapping $X \times X \longrightarrow X$ for any permutation σ of 1, 2 and 3.*

4.1.5 The web associated with a quasigroup

Given a quasigroup $(Q, \cdot)$, let $A := Q^2$. Consider the equivalence relations on A,

$$(q',q'') \sim' (r',r'') \quad \text{if} \quad q' = r', \qquad (q',q'') \sim'' (r',r'') \quad \text{if} \quad q'' = r''$$

and

$$(q',q'') \sim (r',r'') \quad \text{if} \quad q' \cdot q'' = r \cdot r''.$$

Exercise 49 *Show that $(Q^2, \sim, \sim', \sim'')$ is a web whose coordinate quasigroup is $(Q, \cdot)$.*

4.1.6 Example: cubic plane curves

Let C be the set of points in k^2 where k is a field, satisfying a given cubic equation

$$p(X, Y) = 0. \tag{86}$$

For any distinct points $\boldsymbol{a}$ and $\boldsymbol{b}$ on C, the unique line passing through them intersects C in a unique third point or is tangent to C at $\boldsymbol{a}$ or $\boldsymbol{b}$. Indeed, if we substitute the parametric equation of the line

$$\boldsymbol{x}(t) = \boldsymbol{a} + t(\boldsymbol{b} - \boldsymbol{a}),$$

into (86), then we obtain a cubic equation in t with roots $t = 0$ and $t = 1$. Such an equation then has also a third root τ in k. Denote $\boldsymbol{x}(\tau)$ by $\boldsymbol{a} \cdot \boldsymbol{b}$. If $t = 0$ is a *double* root, then we set $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a}$, if $t = 1$ is a *double* root, then we set $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{b}$.

We define $\boldsymbol{a} \cdot \boldsymbol{a}$ by replacing the line connecting $\boldsymbol{a}$ and $\boldsymbol{b}$ by the line *tangent* to C at point $\boldsymbol{a}$.

This is the so called *chordal addition* of points on a cubic curve. Note that it defines on the set of points of C a structure of a quasigroup for which all 6 ternary relations $\mathscr{R}$ coincide. In other words, if $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{c}$, then

$$\boldsymbol{b} \cdot \boldsymbol{c} = \boldsymbol{a}, \qquad \boldsymbol{c} \cdot \boldsymbol{a} = \boldsymbol{b} \qquad \text{and} \qquad \boldsymbol{b} \cdot \boldsymbol{a} = \boldsymbol{c}.$$

Such quasigroups are said to be *totally symmetric*.

4.1.7 Involutions

Totally symmetric quasigroups are analogs, for $n = 3$, of *involutions*, i.e., unary operations $f\colon X \longrightarrow X$ such that $f = f^{-1}$.

4.1.8 Power associative structures

Let us define the powers of an element in a binary structure $(X, \cdot)$ inductively by

$$x^1 := x, \qquad x^{n+1} := x \cdot x^n \qquad (n \in \mathbf{Z}_+). \tag{87}$$

We say that the multiplication is *power associative* if

$$x^m \cdot x^n = x^{m+n} \qquad (m, n \in \mathbf{Z}_+). \tag{88}$$

4.1.9 Semigroups

We say that the multiplication is *associative* if it satisfies the identity

$$(x \cdot x') \cdot x'' \;=\; x \cdot (x' \cdot x'') \qquad (x, x', x'' \in X). \tag{89}$$

The binary structure $(X, \cdot)$ with associative multiplication is called a *semigroup*

4.1.10 Example: Jordan multiplication of square matrices

The following binary operation on the set of rational square matrices of size n

$$A \cdot B \;:=\; \frac{AB + BA}{2}, \tag{90}$$

is power associative but not associative.

4.1.11 Example: Map X

Composition of mappings makes the set Map X of self-mappings $f\colon X \longrightarrow X$ into a semigroup with the identity mapping id_X as its identity element.

4.1.12 Example: the semigroup of words

Concatenation of of a pair of words

$$\mathrm{conc}_2\colon A^{<\infty} \times A^{<\infty} \longrightarrow A^{<\infty}$$

is associative and makes $(A^{<\infty}, \mathrm{conc}_2)$ into a semigroup. Concatenation of n words, cf. (72) is obtained by iterating binary concatenation $n-1$ times.

4.1.13 Subsemigroups

Any substracture of a semigroup is automatically a semigroup.

4.2 Idempotents

4.2.1

Let $(X, \cdot)$ be a binary structure.

Definition 4.1 *An element $e \in X$ is an **idempotent** if $e \cdot e = e$.*

4.2.2 Semilattices

A commutative semigroup $(S, \cdot)$ is called a *semilattice* if every element $s \in S$ is an idempotent.

4.2.3 The canonical order on a semilattice

In a binary structure $(X, \cdot)$ consider the binary relation $\mathscr{R}$ on X where $\mathscr{R}(x, y)$ is the statement

$$x = xy. \tag{91}$$

Exercise 50 *Show that the relation defined in* (91) *orders X if $(X, \cdot)$ is a semilattice. Prove that*

$$\inf\{x, y\} = xy \qquad (x, y \in X) \tag{92}$$

and, more generally,

$$\inf\{x_1, \ldots, x_n\} = x_1 \cdots x_n \qquad (x_1, \ldots, x_n \in X). \tag{93}$$

4.2.4

The binary operation of a semilattice not only induces a partial order such that any nonempty finite subset has infimum but, as identity (92) demonstrates, one can recover the binary operation from the ordering relation.

Exercise 51 *Suppose that $(X, \leq)$ is a partially ordered set with the property that any nonempty finite subset of X has infimum. Show that the binary operation*

$$(x, y) \longmapsto xy := \inf\{x, y\} \qquad (x, y \in X),$$

is associative and every element $x \in X$ is an idempotent.

4.2.5 Example

Both $(\mathscr{P}(A), \cup)$ and $(\mathscr{P}(A), \cap)$ are semilattices.

4.2.6 Absorption identities

We say that a pair of binary operations $\wedge$ and $\vee$ on a set X satisfies *Absorption Identities* if

$$x = x \wedge (x \vee y) \qquad \text{and} \qquad x \vee (x \wedge y) \qquad (x, y \in X). \tag{94}$$

Exercise 52 *Prove that any element of X is an idempotent with respect to a binary operation $\vee$ if there exists another operation $\wedge$ on X such that $\wedge$ and $\vee$ satisfy Absorption Identities* (94)*.*

Note that the second Absorption Idetity is obtained from the first one if we exchange $\wedge$ and $\vee$.

4.2.7 Lattices

Suppose that $(X, \leq)$ is a partially ordered set with the property that any nonempty finite subset of X has infimum and supremum. It follows from Exercise 51 that $(X, \wedge)$ and $(X, \vee)$, where

$$x \wedge y := \inf\{x, y\} \qquad \text{and} \qquad x \vee y := \sup\{x, y\}, \tag{95}$$

are semilattices.

Exercise 53 *Show that the the two operations* (95) *satisfy Absorption Identities.*

4.2.8

A set X equipped with two associative and commutative binary relations $\wedge$ and $\vee$ satisfying Absorption Idnetities is called a *lattice*.

Exercise 54 *Given a lattice $(X, \wedge, \vee)$, let $\mathscr{R}$ be the relation defined for $\wedge$ in Section 4.2.3. Show that $\sup\{x, y\}$ exists, for any $x, y \in X$, and equals*

$$\sup\{x, y\} = x \vee y.$$

4.2.9

We observe that a structure of a lattice on any set induces a structure of a partially ordered set whose finite nonempty subsets have both infima and suprema and vice-versa, any such pratially ordered set is of this form for a unique lattice structure on X.

This is the reason why the same term, a *lattice*, is used interchangably for the corresponding algebraic structure and for a partially oredered set.

Exercise 55 *Prove that, for any congruence $\sim$ on the binary structure $(X, \cdot)$ and any idempotent $e \in X$, the equivalence class $\bar{e}$ is closed under multiplication, i.e. defines a substructure of $(X, \cdot)$.*

4.3 Identity elements, zeros, nilpotents

4.3.1

Definition 4.2 *An element $e \in X$ is a **left identity** if $e \cdot x = x$ for any $x \in X$. Right identities are defined similarly.*

4.3.2 Example

Let X be any set. Consider the projection onto the second factor

$$\pi_2 \colon X \times X \longrightarrow X, \qquad (x_1, x_2) \longmapsto x_2, \tag{96}$$

as a binary operation on X. *Any* element of X is a left identity. Binary structure (96) possesses no right identity except when X is a one-element set. Note that (96) is associative, i.e., $(X, \pi_2 \colon X \times X \longrightarrow X)$ is a semigroup.

4.3.3 The semigroup of retractions

The subset $\mathrm{Retr}_A(X)$ of retractions $X \longrightarrow X$ onto $A \subseteq X$ is a sub-semigroup of the semigroup $\mathrm{Map}\, X$ of all self-mappings $X \longrightarrow X$.

Exercise 56 *Show that for any two $f, g \in \mathrm{Retr}_A(X)$, one has*

$$f \circ g \;=\; g,$$

i.e., every element in $\mathrm{Retr}_A(X)$ is a left identity.

4.3.4

The above examples emphatically demonstrate that one-sided identities are generally far from unique. However, if e is any left identity and e' is any right identity, then they are equal:

$$e = ee' = e'.$$

4.3.5 Unital binary structures

It follows that in any binary structure with at least one left and at least one right identity, the two coincide, thus there exists a *two-sided* identity and it is necessary unique. In this case we say that the binary structure is *unital*.

Exercise 57 *Consider the bijections $L \longrightarrow L'$ and $L \longrightarrow L''$ introduced in Exercise 45 and the associated multiplication on the set of lines L,*

$$L \times L \longrightarrow L, \qquad (l_1, l_2) \longmapsto l_1 \cdot l_2 := m'_1 * m''_2.$$

Show that

$$e \cdot l = l = l \cdot e. \tag{97}$$

4.3.6 Loops

A quasigroup with a two-sided identity is called a *loop*. Exercise 57 demonstrates that among the coordinate quasigroups of a web, there is always a loop.

4.3.7 Monoids

A semigroup with a two-sided identity is called a *monoid*.

4.3.8 Submonoids

Any substracture of a monoid M is automatically a semigroup. It is a monoid if it has an identity element. That element may not be, however, the identity element of M as the following example illustrates.

4.3.9 Example

Let M be the set of 2×2 matrices (with integer coefficients)

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

equipped with the matrix multiplication. It is a monoid with the identity element

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

Consider the set of matrices M'

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

It is closed under multiplication and the matrix

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

is its identity element that is not the identity element of M.

If one considers the identity element to be a part of monoid structure, then it is natural to call a subsemigroup M' of a monoid M a *submonoid* if the identity element of M *belongs* to M'.

4.3.10 Example: $\mathscr{P}(X\times X)$

Composition introduced in Section 2.4.7 makes $(\mathscr{P}(X^2), \circ)$ into a monoid with the identity element being the diagonal subset Δ_X.

4.3.11 Example: Map X

The identity mapping id_X as an identity element of Map X.

4.3.12 Zeros

Definition 4.3 *An element $e \in X$ is a **left zero** (also called a **left sink**), if $z \cdot x = z$ for any $x \in X$. Right zeros are defined similarly.*

One-sided zeros need not be unique. In Example 4.3.2 every element is a right zero. If X is not a singleton set, then no element is a left zero in semigroup (4.3.2).

However, if $z \in X$ is a left zero, and $z' \in X$ is a right zero, then they must be equal:

$$z = zz' = z'.$$

Thus, like in the case of one-sided identities, in a binary structure with at least one left zero and at least one right zero, the two coincide, thus there exists a *two-sided* zero, and it is necessarily unique.

Exercise 58 *For each of the semigroups* $(\mathscr{P}(S), \cup)$ *and* $(\mathscr{P}(S), \cap)$, *determine which element is the identity and which is the zero element.*

4.3.13 Nilpotents

An element $x \in X$ of a power associative structure with zero is said to be *nilpotent* if $x^n = 0$ for some positive integer n.

4.3.14 Example: strictly upper triangular matrices

Any strictly upper triangular $n \times n$-matrix

$$A = \begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ & \ddots & & \vdots \\ & & 0 & a_{n-1,n} \\ & & & 0 \end{pmatrix}$$

with whatever coefficients satisfies $A^n = 0$.

4.3.15 Inverse elements

Definition 4.4 *If a pair of elements* x, x' *in a monoid satisfies equality* $xx' = e$, *then* x' *is said to be a* right inverse *of* x *and* x *is said to be a* left inverse *of* x'.

A given element x may have many right inverses or left inverse. If x' is a right inverse and x'' is a left inverse of the same element x, then they coincide, however:

$$x' = ex' = (x''x)x' = x''(xx') = x''e = x''.$$

In particular, any right inverse in that situation is also a right inverse and vice-versa. That unique two-sided inverse is then denoted x^{-1}.

4.3.16 Invertible elements

Elements possessing an inverse are referred to as *invertible elements*.

4.3.17 Groups

If every element is invertible, the monoid is called a *group*.

Exercise 59 *For a monoid $(M, \cdot)$, let $G(M)$ denote the subset of invertible elements in M. Show, that $(G(M), \cdot)$ is a group.*

Thus, M is a group if and only if $G(M) = M$.

4.3.18 Example: Bij X

Invertible self-mappings $f\colon X \longrightarrow X$ are precisely self-bijections of X. Thus $(\operatorname{Bij} X, \circ) = G(\operatorname{Map} X, \circ)$.

4.3.19 Subgroups

A substracture of a group is a semigroup and nothing more in general. Take, for example, the additive group of integers and consider the set of positive even integers. In a marked contrast to the situation with monoids, however, if a substracture G' of a group G is a monoid itself, then the identity element of G belongs to G'. This is due to the fact that the only idempotent in a group is its identity element.

Exercise 60 *Show that the identity element in a group is its only idempotent.*

In particular, if a substructure G' of a group is a group itself, then the inverse of every element g' in G' is also the inverse if we consider g' as an element of G. Thus, a *subgroup* is substructure of G which is a group itself.

Exercise 61 *Show that, if z is a left (or right) zero element of a group G, then $G = \{z\}$.*

4.4 Central elements

4.4.1

Let again $(X, \cdot)$ be an arbitrary binary structure.

Definition 4.5 *An element $c \in X$ is **central** if it* commutes *with every element of X,*

$$cx = xc \qquad (x \in X).$$

4.4.2 Normal subsets

A subset $N \subseteq X$ of a binary structure is normal if

$$aN \;=\; Na \tag{98}$$

for each $a \in X$.

Exercise 62 *Show that a subset $N \subseteq X$ is normal if and only if N is a central element of $(\mathscr{P}(X), \cdot)$.*

4.4.3 Center

The set of all central elements is called the *center* of $(X, \cdot)$. We will denote it $Z(X, \cdot)$, or simply $Z(X)$, when the binary operation is clear from the context.

Exercise 63 *Prove that the center of a **semigroup** is closed under multiplication and thus is a sub-semigroup.*

4.4.4 Commutative binary structures

If $Z(X, \cdot) = X$, i.e., if any two elements commute, then we say that the binary structure is *commutative*. Thus, we have commutative semigroups, commutative monoids. Instead of 'commutative' groups, however, we talk of *abelian* groups. This terminology was in use before the term 'commutative' was applied to general binary operations. It honors the Norwegian mathematician Niels Hendrik Abel (1802-1828).

4.4.5 Additive notation for commutative semigroups and abelian groups

In theory of abelian groups (and, to a lesser extent, in theory of commutative semigroups) it is a common practice to denote the result of the binary operation applied to elements x and y as $x + y$. Accordingly, the identity element in additive notation is denoted 0 and is referred to as *zero*. Confusing this element with the *zero elements* of Section 4.3.12 is rarely possible in view of the fact that the only group that has a zero element in the sense of Section 4.3.12 is the so called *trivial group*, i.e., the group with one element, and that single element is simultaneously the identity and the zero element in the sense of Section 4.3.12.

4.4.6

The n-th power of an element in additive notation becomes

$$nx := x + \cdots + x \qquad (n \text{ times}) \tag{99}$$

while the 0-th power becomes $0x = 0$. For $n < 0$, we set $nx := (-n)x$.

Exercise 64 *Show that in an abelian group $(A, +)$, one has*

$$(m + n)a = ma + na$$

for any $a \in A$ and for any integers m and n.

4.5 Coset relations in groups

4.5.1 Characterization of subgroups

Let $(G, \cdot)$ be a group and $H \subseteq G$ be a subset. By H^{-1} we shall denote the set of inverses of elements of H,

$$H^{-1} := \{h^{-1} \mid h \in H\}. \tag{100}$$

Exercise 65 *Prove that H is a subgroup if and only if $H \cdot H^{-1} = H$.*

4.5.2 Cosets

Given a subset $H \subseteq G$, consider the family of subsets

$$\{gH \mid g \in G\}. \tag{101}$$

Its memebers are called **left cosets** of H in G.[3]

Exercise 66 *Prove that* (101) *is a partition of set G if and only if the coset aH which contains the identity element, e, is a subgroup of G.*

4.5.3 Coset relations

Consider the following relation on set G:

$$a \sim_H b \quad \text{if} \quad a \in bH. \tag{102}$$

Exercise 67 *Prove that*

1. *$\sim_H$ is reflexive if and only if H contains the identity element of G;*
2. *the inverse relation, $(\sim_H)^{-1}$, coincides with $\sim_{H^{-1}}$; in particular, $\sim_H$ is symmetric if and only if $H = H^{-1}$;*
3. *$\sim_H$ is transitive if and only if $H \cdot H \subseteq H$;*
4. *$\sim_H$ is an equivalence relation if and only if H is a subgroup of G;*
5. *$\sim_H$ is a congruence if and only if H is a normal subgroup of G.*

4.5.4 Order of a group

The cardinality of a group G is denoted $|G|$ and referred to as the *order* of G.

4.5.5 Index of a subgroup

When H is a subgroup of G, the cardinality of the quotient set $G/_{\sim_H}$ is denoted G/H and its cardinality is denoted

$$|G : H| \tag{103}$$

and referred to as the *index* of H in G.

[3] Subsets Hg, where $g \in G$, are called *right cosets*.

4.5.6 Leibniz Theorem

Exercise 68 *Prove that for a finite group G and any subgroup $H \subseteq G$, one has*

$$|G| \;=\; |G:H|\,|H|. \tag{104}$$

4.5.7 Congruences on groups

Every congruence $\sim$ on a group G is the coset relation $\sim_H$ for the subset $H := \bar{e}$, i.e., the equivalence class of the identity element (H in this case must be a normal subgroup of G).

Exercise 69 *Prove that any congruence $\sim$ on a group G is of the form $\sim_N$ for some normal subgroup $N \subseteq G$.*

4.5.8 Notation for normal subgroups

The fact that N is a normal subgroup of a group G is often expressed using the notation

$$N \lhd G \qquad \text{or} \qquad G \rhd N. \tag{105}$$

5 Rings

5.1 Binary rings

5.1.1

Definition 5.1 *A set R equipped with two binary operations, $+$ and $\cdot$, which are customarily referred to as **addition** and **multiplication**, is called a **ring**, if:*

$$(R,+) \text{ is an abelian group} \tag{106}$$

and the two operations are compatible in the following natural sense:

$$a(b+c) = ab + ac \qquad (\textit{left distributivity}) \tag{107}$$

and

$$(b+c)a = ba + ca \qquad (\textit{right distributivity}) \tag{108}$$

for any $a, b, c \in R$.

Exercise 70 *Prove that 0 is indeed a* zero *of the multiplicative structure, $(R, \cdot)$, i.e., that*

$$0 \cdot a = a \cdot 0 = 0$$

for any $a \in R$.

5.1.2 The additive group of a ring

The group $(R, +)$ is called the *additive* group of the ring, and its identity element is called *zero* and denoted 0. For any positive integer n we use the notation

$$nr := r + \cdots + r \qquad (n \text{ times}).$$

5.1.3 The characteristic of a ring

The smallest positive integer n such that $nr = 0$ for all $r \in R$, is called the *characteristic* of R. If no such n exists, we say that R is of *characteristic zero*.

Exercise 71 *Explain why $(\mathscr{P}(S), \cup, \cap)$ is not a ring according to Definition 5.1. Slightly modify* one *of the two operations so that the power set becomes an associative and commutative ring with identity.*

5.1.4

In the context of rings such terms as *associative*, *commutative*, *unital*, *idempotent*, *central element*, the *center*, *nilpotent*, etc, are always meant with respect to the binary operation of multiplication.

5.1.5 Zero divisors

A nonzero element $r \in R$ is a *left zero divisor*, if $rs = 0$ for some nonzero $s \in R$. Right zero divisiors are defined similarly.

5.1.6 Domains

Rings without zero divisiors are called *domains*. The set of nonzero elements $R^* := R \setminus \{0\}$ in a domain is a substracture of $(R, \cdot)$.

5.1.7 Division rings

Domains such that $(R^*, \cdot)$ is a quasigroup are called *division rings*.

5.1.8 Fields

Commutative division rings are called *fields*.

5.1.9 Boolean rings

Associative rings in which *every* element is an idempotent are called *Boolean rings*. In other words, an associative ring is Boolean if its multiplicative semigroup is a semilattice.

Exercise 72 *Show that any Boolean ring has characteristic 2 and is commutative.*

5.1.10 Lie rings

A binary ring $(R, +, \cdot)$ satisfying the *Jacobi Identity*

$$(ab)c + (bc)a + (ca)b = 0 \qquad (a, b, c \in R) \tag{109}$$

and such that

$$a^2 = 0 \qquad (a \in R), \tag{110}$$

is called a *Lie ring*. In theory of such rings the binary multiplication is almost always denoted $[a, b]$ (with the comma separating the arguments occasionally dropped. For this reason, the "multiplication" in a Lie ring is often referred to as the *bracket*.

5.1.11 The commutator operation in a binary ring

For any binary ring, the formula

$$(a, b) \longmapsto [a, b] := ab - ba \tag{111}$$

defines what is called the (ring) *commutator* of elements a and b.

5.1.12 The associator operation in a binary ring

For any binary ring, the formula

$$(a,b,c) \longmapsto [a,b,c] := (ab)c - a(bc) \tag{112}$$

defines what is called the *associator* of elements a and b.

Exercise 73 *Show that the left hand side of the Jacobi identity for the commutator operation in a binary ring is the antisymmetrization of the associator,*

$$[[a_1,a_2],a_3] + [[a_2,a_3],a_1]] + [[a_3,a_1],a_2] = \sum_{\sigma}(-1)^{\tilde{\sigma}}\left[a_{\sigma(1)},a_{\sigma(2)},a_{\sigma(3)}\right], \tag{113}$$

where the summation is over all permutations σ of $\{1,2,3\}$ and $\tilde{\sigma}$ is the ***parity*** *of the permutation: $\tilde{\sigma} = 0$ for the identity permutation and two cycles of length 3, $(2\ 3\ 1)$ and $(3\ 1\ 2)$, and $\tilde{\sigma} = 1$ for each of the three transpositions.*

Exercise 74 *Prove the following commutator-associator identity*

$$a[b,c] - [ab,c] + [a,c]b = [a,c,b] - [a,b,c] - [c,a,b]\ . \tag{114}$$

Exercise 75 *Prove the following associator identity*

$$a[b,c,d] - [ab,c,d] + [a,bc,d] - [a,b,cd] + [a,b,c]d = 0\ . \tag{115}$$

5.1.13 The associated Lie ring of an associative ring

It follows that the commutator operation in an associative binary ring satisfies the Jacobi identity. The Lie ring $(R,+;[\ ,\ ])$ is called the *associated Lie ring*.

5.1.14 Cross-product

Exercise 76 *Show that the cross-product of vectors in $\mathbf{R}^3$ satisfies both properties of the Lie bracket.*

The Lie ring $(\mathbf{R}^3,+,\times)$ plays a special role not only in Multivariable Calculus.

5.1.15 Alternative rings

A binary ring is *alternative* if

$$[a,a,b]=0 \tag{116}$$

and

$$[a,b,b]=0 \tag{117}$$

for any pair of elements of R.

Exercise 77 *Show that in any alternating ring the associator is an* alternating *function of its arguments, i.e., for any permutation σ of $\{1,2,3\}$, one has*

$$\left[a_{\sigma(1)},a_{\sigma(2)},a_{\sigma(3)}\right]=(-1)^{\tilde{\sigma}}[a_1,a_2,a_3] \qquad (a_1,a_2,a_3\in R). \tag{118}$$

Show that in any binary ring satisfying identities (118) *one has*

$$2[a,a,b]=2[a,b,b]=0 \qquad (a,b\in R).$$

5.1.16 Complex numbers

A complex number is a formal expresion $z=a+bi$ with $a,b\in\mathbf{R}$ and i being a reserved symbol. The multiplication of such expressions is dictated by the desire that multiplication by i is a linear transformation of the corresponding 2-dimensional vector space with basis consisting of 1 and i subject to the requirement that i supplies the missing square root of -1, i.e., $i^2=1$. The real numbers a and b are called the *real* and, respectively, the *imaginary* parts of z.

5.1.17 Quaternions

A *quaternion* is a formal expression $\alpha=z+wi$ with the "real" and "imaginary" parts being *complex numbers*. In order not to confuse the imaginary unit i with the internal imaginary units of z and w, we shall denote the latter by j. Multiplication is subjet to the same conditions as before, namely, multiplication by i must be a linear transformation of the corresponding $2\cdot 2=4$ dimensional real vector space with basis $\{1,i,j,ij\}$, with i^2, j^2, and also $(ij)^2$, all being equal to -1. The latter condition implies that symbols i and j *anticommute*.

Exercise 78 *Show that the requirement* $(ij)^2 = -1$ *is equivalent, assuming that the multiplication is associative, to*

$$ij = -ji.$$

5.1.18

The product ij is denoted k. The resulting ring of quaternions is denoted $\mathbf{H}$ and is an example of an associative noncommutative division ring.

5.1.19 The quaternion group

The set

$$\{\pm 1, \pm i, \pm j, \pm k\} \tag{119}$$

is closed under the multiplication and forms a group which is usually referred to as the *quaternion group* (of order 8). It is denoted either Q or Q_8.

5.1.20 Octonions

An *octonion* is a formal expression $\zeta = \alpha + \beta i$ with the "real" and "imaginary" parts being *quaternions*. In order not to confuse the imaginary unit i with the internal imaginary units i, j and k of α and β, we shall denote it by l.

5.1.21 Imaginary units

Multiplication by l is subject to the standard requirements that it is a linear transformation of the $2 \cdot 4 = 8$ dimensional real vector space with the basis consisting of 1 and the seven *imaginary units,*

$$\{i, j, k, l, il, jl, kl\}, \tag{120}$$

and that the square of any of them equals -1.

5.1.22 Embedded copies of the ring of quaternions

Assuming that multiplication in the subring generated by any two imaginary units is associative, this implies, in view of Exercise 78, that any two distinct imaginary units anticommute and the subring they generate is a copy of the ring of quaternions. There are $\binom{7}{2} = 21$ such pairs and each embedded copy of quaternions contains exactly three such units. Choosing any two of them generates the same subring. Hence we get $21/3 = 7$ embedded copies of the ring of quaternions. (Notice that the subring generated by a single imaginary unit is an embedded copy of the ring of complex numbers $\mathbf{C}$.)

5.1.23 The 7_3-configuration of copies of C and H

Those seven embedded copies of $\mathbf{C}$ form the points while the seven embedded copies of $\mathbf{H}$ form the lines of the smallest projective plane that happens also to be the smallest n_3-configuration.

Exercise 79 *Let i_1 and i_2 be any two distinct imaginary units in the ring of octonions. Show that they satisfy the identity*

$$i_1 i_2 i_1 = i_2.$$

5.1.24 Twisted associativity

The above still does not completely determine the multiplication table of octonions. The remaining requirements are: the set

$$\{\pm 1, \pm i, \pm j, \pm k, \pm l, \pm il, \pm jl, \pm kl\} \tag{121}$$

is closed under multiplication, and

$$(i_1 i_2) i_3 = \epsilon(i_1, i_2, i_3)\, i_1 (i_2 i_3) \tag{122}$$

where

$$\epsilon(i_1, i_2, i_3) := \left\{ \begin{array}{cr} 1 & \text{if } i_1, i_2, i_3 \text{ are collinear} \\ -1 & \text{if they are not} \end{array} \right. . \tag{123}$$

Collinearity of i_1, i_2, i_3 means that they generate a copy of $\mathbf{H}$. This happens if either two of the three units coincide, or that one is, up to a sign, the product of the other two.

5.1.25

The above considerations completely determine the multiplication table of octonions if one requires that multiplication is linear in each argument. For example,

$$(jl)(il) = -j(lil) = -ji = k$$

since i, j, l are not collinear.

Exercise 80 *Calculate* $(kl)(jl)$.

5.1.26

The corresponding ring of octonions is today most often denoted $\mathbf{O}$ and is an example of a nonassociative alternating division ring.

5.1.27 Moufang loops

A loop $(L, \cdot)$ satisfying the *Moufang identity,*

$$(lm)(nl) = \big(l(mn)\big)l \qquad (l, m, n \in L), \tag{124}$$

is called a *Moufang loop.*

Exercise 81 *Show that* (121) *is a Moufang loop.*

5.1.28 Complex numbers with real and imaginary parts being octonions?

Such expressions form a real $2 \cdot 8 = 16$ dimensional vector space with basis provided by 1, seven imaginary units in octonions and their eight products with "external" imaginary unit. This yields $7 + 8 = 15$ imaginary units. It is clear that any single unit should generate a copy of $\mathbf{C}$, any pair of distinct units should generate a copy of $\mathbf{H}$, and any triple of *non-collinear* units should generate a copy of $\mathbf{O}$. The resulting ring, if it exists, contains 15 embedded copies of $\mathbf{C}$ and $\mathbf{O}$ each, and 35 embedded copies of $\mathbf{H}$.

The resulting configuration of *points* (copies of $\mathbf{C}$), *lines* (copies of $\mathbf{H}$), and *planes* (copies of $\mathbf{O}$), forms the smallest 3-dimensional projective space (and one of the simplest examples of the incidence geometry of points, lines and planes).

5.2 Congruences on binary rings

5.2.1 Ideals

A subgroup I of the additive group of a ring R is said to be a *left ideal* if

$$ra \in I \qquad (r \in R, a \in I). \tag{125}$$

Right ideals are defined similarly. If I is both a left and a right ideal, it is called a *twosided* ideal or, simply an *ideal*.

5.2.2

Since a congruence $\sim$ of the ring structure $(R, +, \cdot)$ is also a congruence of the additive structure $(R, +)$, any ring congruence is the coset equivalence $\sim_I$ where I is the equivalence class $\bar{0}$ of 0. Mind that the coset of r is written $r + I$ (not rI), since the group operation is $(R, +)$ is written additively as $r + s$ (not rs).

Exercise 82 *Given a congruence $\sim$ on a binary ring $(R, +, \cdot)$ show that the equivalence class $\bar{0}$ of 0 is an ideal. Vice-versa, show that the coset relation $\sim_I$ is a ring congruence if I is an ideal.*

6 Algebraic structures (in the strict sense)

6.1 ν-ary structures

6.1.1 Arity functions

Given a function

$$\nu\colon J \longrightarrow \mathbf{N}, \qquad j \longmapsto \nu(j) := \text{the arity of } \mu_j \tag{126}$$

we call a set X equipped with a family of operations $M = (\mu_j)_{j \in J})$ on X a *ν-ary structure*

6.1.2 Universal Algebra

A branch of Mathematics studying general ν-ary structures and properties of various classes of such structures is called *Universal Algebra*. In Universal Algebra what we call here a ν-ary structures is referred to as *algebras*. This is one of the several uses of the term "algebra" in Mathematics.

6.1.3

When the arity function ν is injective, then there is no need to use an auxiliary indexing set J, or one can say that the family of operations is naturally indexed by the arity, μ_j being the unique operation of arity i.

6.2 Substructures

6.2.1

If a subset $X' \subseteq X$ is closed under *every* operation μ_j, $j \in J$, then by restricting each μ_j to $(X')^{\nu(j)}$ and narrowing its target to X', we obtain a *ν-substructure* of $\big(X, (\mu_j)_{j \in J}\big)$.

6.2.2 The lattice of substructures

The set of all substructures $\operatorname{Substr}\big(X, (\mu_j)_{j \in J}\big)$ corresponds to the subset of $\mathscr{P}(X)$ consisting of all subsets of X closed under every operation μ_j. That set is partially ordered by containment. In what follows we do not distinguish between a substructure of $\big(X, (\mu_j)_{j \in J}\big)$ and a subset of X that is closed under every opereation μ_j.

6.2.3

By definition, the largest substructure is $\big(X, (\mu_j)_{j \in J}\big)$ itself.

6.2.4 The infimum of a family of substructures

According to Exercise 38, the intersection of any family $\mathcal{S}$ of substructures is a substructure. It is obviously the largest substructure contained in each member of $\mathcal{S}$. It is called the *infimum* of family $\mathcal{S}$. Thus,

$$\inf \mathcal{S} \;=\; \bigcap \mathcal{S}. \tag{127}$$

6.2.5 The supremum of a family of substructures

In any partially ordered set $(A, \leq)$, the existence of infima of arbitrary subsets guarantees also the existence of their suprema: one can show that the supremum of a subset B coincides with the infimum of the set of all *upper bounds* of B.

Accordingly, the *supremum* of a family $\mathcal{S}$ of substructures is the intersection of the substructures containing their union

$$\sup \mathcal{S} \;=\; \bigcap_{X' \supseteq \bigcup \mathcal{S}} X'. \tag{128}$$

6.2.6 The substructure generated by a subset

For any subset $A \subseteq X$ we define the substructure *generated* by A as the infimum of the family $\mathcal{A}$ of substructures of $(X, (\mu_j)_{j \in J})$ which contain A. We shall denote it $\langle A \rangle$. Note that

$$\sup \mathcal{S} \;=\; \left\langle \bigcup \mathcal{S} \right\rangle.$$

6.2.7 The smallest substructure

The smallest substructure is $\langle \emptyset \rangle$. It is the intersection of all substructuresof $(X, (\mu_j)_{j \in J})$. It is empty precisely when none of the operations μ_j is nullary and it contains all the elements of X that correspond to those operations among μ_j which are nullary.

6.2.8 Sets of generators

A subset $A \subseteq X$ is said to *generate* (X, M) if $\langle A \rangle = X$.

6.2.9 The free ν-ary structure generated by a set

Given a set A, let us adjoin to it elements, denoted $*_i$, not belonging to it and all distinct (e.g., we can take $*_i = (*, i) \in \coprod_{i \in I} A^0$ where $*$ is the unique element of A^0). Let

$$\tilde{A} := A \cup \{*_i \mid i \in I\}.$$

(Alternatively, we could take $\tilde{A}$ to be the disjoint union $A \sqcup I$ of A and I.) For each $i \in I$, consider the following $\nu(i)$-ary operation on $\tilde{A}^{<\infty}$

obtained by concatenating $\nu(i)+1$ words in alphabet $\tilde{A}$ with $*_i$ placed as the first word,

$$\big(w_1,\dots,w_{\nu(i)}\big) \longmapsto \mathrm{conc}_{\nu(i)+1}\big(*_i,w_1,\dots,w_{\nu(i)}\big). \tag{129}$$

If we consider the ν-ary structure on $\tilde{A}^{<\infty}$ given by the family of free multiplications (129), indexed by I, then the substructure generated by $A \subseteq \tilde{A}^{<\infty}$ is called the *free ν-ary structure on A*. We shall denote it $F_\nu(A)$. When $A = \{a_1,\dots,a_n\}$ (with all a_i different), then $F_\nu(A)$ will be also denoted $F_\nu(a_1,\dots,a_n)$.

6.2.10 Product structures

Products of ν-ary structures are formed exactly like the corresponding products of n-ary structures for a single n-ary operation, see Sections 3.3.5 and 3.3.7, the j-th operation on $\prod_{i\in I} X_i$ being the product of the corresponding j-th operations on the component sets X_i, $i \in I$.

6.3 Quotient structures

6.3.1 Congruences

If an equivalence relation $\sim$ is given which is a congruence for *every* operation μ_j, $j \in J$, then $X_{/\sim}$ inherits the ν-ary structure from $\big(X,(\mu_j)_{j\in J}\big)$.

6.3.2

According to Execrcise 42, an equivalence relation $\sim$ is a congruence if and only if its graph $\Gamma_\sim$ is a substructure of the product structure $\big(X\times X,(\mu_j\times\mu_j)_{j\in J}\big)$.

6.3.3 A weakest congruence stronger than a given binary relation

Let $\mathscr{R}$ be a binary relation on X. Considers the class $\mathfrak{C}_{\mathscr{R}}$ of congruences on $\big(X\times X,(\mu_j\times\mu_j)_{j\in J}\big)$ that are stronger than $\mathscr{R}$. It is not empty, since $X\times X$ is a relation with $x \sim x'$ for all $x, x' \in$ is a congruence.

The intersection of the family of the graphs $\Gamma_{\mathscr{C}}$ of congruences $\mathscr{C}$ that are stronger than $\mathscr{R}$ is the graph of the conjunction of a family of equivalence relations on X, hence is the graph of an equivalence relation itself. It is also the infimum of a family of substructures of $\big(X\times X, (\mu_j\times\mu_j)_{j\in J}\big)$, hence a substructure itself. By combining these two observations, we infer that it is the graph of a congruence, and this congruence is weaker than any congruence stronger than $\mathscr{R}$.

6.4 Equationally defined classes

6.4.1

Alegebraic structures (in the strict sense) are generally considered to be subclasses of the class of algebras of a certain type ν. The structures that we have so far encountered are all of this type.

6.4.2 Example: Sets

Sets are ν-ary structures for $I = \emptyset$ and ν being the inclusion of the empty set into $\mathbf{N}$. In other words, sets correspond to the case when *no* operations are given.

6.4.3 Example: G-sets

Let G be a semigroup. A *G-set* is a set X equipped with a family of *unary* operations $(\lambda_g)_{g\in G}$ satisfying the following identities

$$\lambda_{g'}\big(\lambda_{g''}(x)\big) \;=\; \lambda_{g'g''}(x) \qquad (g', g'' \in G;\, x \in X). \tag{130}$$

6.4.4

We say in this case that the semigroup G *acts* on a set X.

6.4.5

If G is a monoid with the identity element e, then one requires also the following identity to hold

$$\lambda_e(x) \;=\; x \qquad (x \in X). \tag{131}$$

6.4.6

We say in this case that the *monoid* G *acts* on a set X.

Exercise 83 *Prove that when* G *is a group acting on a set* X*, then*

$$\lambda_{g^{-1}} \;=\; \left(\lambda_g\right)^{-1} \qquad (g \in G;\, x \in X).$$

6.4.7 Right G-sets

The structure defined above is of a *left* G-set. A *right* G*-set* is a set equipped with a family of *unary* operations $(\rho_g)_{g\in G}$ satisfying the following identities

$$\rho_{g'}\left(\rho_{g''}(x)\right) \;=\; \rho_{g''g'}(x) \qquad (g', g'' \in G;\, x \in X). \tag{132}$$

6.4.8 Example: R-modules

Let R be a binary ring. An R*-module* is an abelian group $(M, +)$ which is simultaneously a G-set for $G = (R, \cdot)$, the multiplicative semigroup of a ring R, such that the following distributivity identities hold

$$\lambda_r(m + m') = \lambda_r(m) + \lambda_r(m') \tag{133}$$

and

$$\lambda_{r+r'}m = \lambda_r(m) + \lambda_{r'}(m). \tag{134}$$

6.4.9 Right modules

The structure defined above is of a *left* R-module. The definition of a *right* R*-module* is obtained by replacing left by *right* action of the multiplicative semigroup of R.

6.4.10 Unitary R-modules

When R has identity and the identity element in R acts on M as the identity map id_M, then we say that the module structure is *unitary*.

6.4.11 Example: (R,S)-bimodules

Given two rings R and S, an (R,S)-bimodule is a an abelian group $(M,+)$ equipped with a *left* R-module structure, a *right* S-module structure such that the two structures commute, i.e.,

$$[\lambda_r, \rho_s] = 0 \qquad (r \in R,\ s \in S). \tag{135}$$

6.4.12

When $R = S$, we speak of R-bimodules.

6.4.13 Example: the bimodule of $m \times n$ matrices

Let k be a ring. Let $R = M_m(k)$ and $S = M_n(k)$ be the rings of $m \times m$ and $n \times n$ matrices with coefficients in k and, finally, let $M = M_{mn}(k)$ be the additive group of $m \times n$ matrices with coefficients in k. Multiplication on the left by $m \times m$ matrices and on the right by $n \times n$ matrices defines a $(M_m(k), M_n(k))$-bimodule structure on $M_{mn}(k)$.

6.4.14

Semigroups and G-sets when G is a given semigroup or monoid are examples of *equationally defined classes* of algebraic structures. Among all structures of given arity they are defined exclusively in terms of certain *identities*.

6.4.15

On the other hand, monoids, groups, division rings, fields, etc, are defined in terms of identities *and* conditions *expressed in terms of quantifiers* like the condition

> *for any $r \in R$, if $r \neq 0$, then there exists $s \in R$ such that $rs = sr = 1$,*

which is encountered in the definition of *division rings*.

This simple observation distinguishes equationally defined classes of algebraic structures among all algebraic structures.

6.4.16 Identities in ν-ary structures

General identities involving l elements of a ν-ary structure are of the form

$$w_1 = w_2 \tag{136}$$

where w_1 and w_2 are elements of the free ν-ary structure $F_\nu(t_1, \dots, t_l)$ on the alphabet consisting of l independent variables $t_1, \dots, t_l$.

We say that identity (136) is *satisfied* in a ν-ary structure (X, M) if equality in (136) holds when we perform the operations *prescribed* by w_1 and w_2 on l arbitrarily chosen elements $x_1, \dots, x_l$ of X.

6.4.17 Example: the associativity identity

Consider the words

$$w_1 := **t_1t_2t_3 \qquad \text{and} \qquad w_2 := *t_1 * t_2t_3$$

in the free binary structure on the alphabet $\{t_1, t_2, t_3\}$.

Performing the operations prescribed by w_1 and w_2 on a triple of arbitrary elements x_1, x_2, x_3 in a binary structure (X, μ) yields

$$\mu\mu x_1x_2x_3 = \mu x_1\mu x_2x_3$$

(in prefix notation), or

$$\mu(\mu(x_1, x_2)x_3) = \mu(x_1, \mu(x_2, x_3))$$

(using functional notation with parentheses), or

$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$$

(using infix notation).

6.4.18 Equational classes on ν-ary structures

Any set $\mathcal{I}$ of identities of the form (136) defines the corresponding equational class. We shall say that a ν-ary structure (X, M) is *of the equational class* $\mathcal{I}$ if all the identities in $\mathcal{I}$ are satisfied in (X, M).

6.4.19

Any *substructure*, *quotient structure*, and any *product* of ν-ary structures satisfying a certain identy will automatically satisfy the same identity. It follows that substructures, quotient structures and arbitrary products of ν-structures of equational class $\mathcal{I}$ belongs to the same class.

6.4.20 The congruence $\sim_{\mathcal{I}}$

Given a set of identities $\mathcal{I}$, calculate the left-hand-sides and the right-hand-sides of all identities $\mathscr{I}$ in $\mathcal{I}$ by substituting under variables $t_1, t_2, \dots,$ all possible elements of X. The corresponding pairs $\left(\mathrm{LHS}_{\mathscr{I}}, \mathrm{RHS}_{\mathscr{I}}\right)$ form a subset of $X \times X$. Denote the associated binary relation on X by $\mathscr{R}_{\mathcal{I}}$. A weakest congruence stronger than $\mathscr{R}_{\mathcal{I}}$ is also a weakest congruence such that the quotient structure $\left(X_{/\sim}, (\bar{\mu}_j)_{j \in J}\right)$ satisfies all identities form $\mathcal{I}$.

6.4.21

Passing from a structure $\left(X, (\mu_j)_{j \in J}\right)$ to $\left(X_{/\sim}, (\bar{\mu}_j)_{j \in J}\right)$ is often referred to as *enforcing* a given set of identities.

6.4.22 Free ν-ary structure satifying identities $\mathcal{I}$

The quotient structure obtained by enforcing identities $\mathcal{I}$ on a free ν-ary structure $F_\nu(A)$ will be denoted $F_{\nu,\mathcal{I}}$ and called the ν-ary structure satisfying identities $\mathcal{I}$ *freely generated* by a set A. Structures of this kind are fundamentally important.

6.5 Redefining a structure to make it equational

6.5.1

Various structures that are not *equationally* defined can be often redefined as equational structures of *different* arity.

6.5.2 Case study: monoids

A monoid can be defined as a structure consisting of a single *nullary* operation, i.e., a distinguished element e, and a single *binary* operation that satisfies the following three identies

$$(xy)z = x(yz), \quad ex = x \quad \text{and} \quad xe = x \qquad (x, y, z \in X). \tag{137}$$

6.5.3 Case study: groups

A group can be defined as a structure consisting of a single *nullary* operation e, a single *unary* operation, written

$$x \longmapsto x^{-1},$$

and a single *binary* operation that satisfies the monoid identities (137) and the following two identities involving the *pasing-to-the-inverse* operation

$$xx^{-1} = e \qquad \text{and} \qquad x^{-1}x = e \qquad (x \in X). \tag{138}$$

6.5.4

Define a new binary operation on a group

$$x/y \;:=\; xy^{-1} \tag{139}$$

or, in prefix notation, $/xy$.

Exercise 84 *Show that operation* (139) *satisfies the identity that, in postfix notation, is written as*

$$xxx/y/z/xx/x/z/// \;=\; y. \tag{140}$$

Note that the left hand side of (140) *is the expresssion* (69).

Exercise 85 *Define the nullary, unary and binary operations of the group in terms of the operation* $/$.

6.5.5

One can show that if the operation $/$ satisfies identity (69), then the corresponding nullary, unary and binary operations satisfy identities (137) and (138). In particular, the group structure can be defined using a single binary operation that satisfies a single identity.

6.6 Example: Implicational structures

6.6.1

Consider a binary structure $(X, \supset)$ satisfying the following two identities

$$(x \supset y) \supset x \;=\; x \tag{141}$$

and

$$(x \supset y) \supset y \;=\; (y \supset x) \supset x. \tag{142}$$

Exercise 86 *Show that the identity*

$$x \supset (x \supset y) \;=\; x \supset y \tag{143}$$

is a consequence of identity (141)*.*

Exercise 87 *Show that the identity*

$$x \supset x \;=\; (x \supset y) \supset (x \supset y) \tag{144}$$

is a consequence of identities (141)–(143)*.*

Exercise 88 *Show that the identity*

$$x \supset x \;=\; y \supset y \tag{145}$$

is a consequence of identities (144) *and* (142)*.*

6.6.2 The "truth" element

Let us denote by t the element $x \supset x$ of X which, according to Exercise 88, does not depend on $x \in X$.

Exercise 89 *Show that the identities*

$$(x \supset x) \supset x \;=\; x \qquad \text{and} \qquad x \supset (x \supset x) \;=\; x \supset x, \tag{146}$$

are consequences of identities (141) *and* (143)*, respectively.*

Thus the *truth* element t is a *left* but not right identity, and a right but not left zero.

6.6.3 Implication algebras

A binary structure $(X, \supset)$ satisfying identities (141), (142) and the identity

$$x \supset (y \supset z) \;=\; y \supset (x \supset z) \tag{147}$$

is sometimes called an *implication algebra*.

6.6.4 An example: the power set as an implication algebra

Given a set A, define an operation $\supset$ on $\mathscr{P}(A)$ by

$$X \supset Y \;:=\; (A \setminus X) \cup Y. \tag{148}$$

Exercise 90 *Show that*

$$X \supset Y = Y \qquad \text{if and only if} \qquad X \cup Y = A$$

and

$$X \supset Y = X \qquad \text{if and only if} \qquad X = Y = A.$$

Exercise 91 *Verify that* $(\mathscr{P}(A), \supset)$ *satisfies identities* (141), (142) *and* (147), *i.e, is an implication algebra.*

7 Morphisms

7.1 Morphism between relations

7.1.1

Let $(X_1, \dots, X_n, \mathscr{R})$ and $(X'_1, \dots, X'_n, \mathscr{R}')$ be two n-ary relations.

Definition 7.1 *A collection of maps* $\phi = (\phi_1, \dots, \phi_n)$*, where* $\phi_i \colon X_i \longrightarrow Y_i$*, is called a* ***morphism*** *from* $\mathscr{R}$ *to* $\mathscr{R}'$ *if*

$$\mathscr{R}(x_1, \dots, x_n) \quad \text{implies} \quad \mathscr{R}'\big(\phi_1(x_1), \dots, \phi_n(x_n)\big). \tag{149}$$

We shall extend the arrow notation from maps between sets to morphisms between relations and other structures:

$$\phi \colon \mathscr{R} \longrightarrow \mathscr{R}'.$$

7.1.2 The identity morphism

In the case when $X_i = X'_i$, for all $i = 1, \dots, n$, and $\mathscr{R} = \mathscr{R}'$, we can consider the identity morphism

$$\mathrm{id}_{\mathscr{R}} \colon \mathscr{R} \longrightarrow \mathscr{R} \tag{150}$$

where each ϕ_i is the identity map $X_i \longrightarrow X_i$.

7.1.3 Composition of morphisms

If $(X''_1, \dots, X''_n, \mathscr{R}'')$ is a third n-ary relation and $v \colon \mathscr{R}' \longrightarrow \mathscr{R}''$ is a morphism,

$$v = (v_1, \dots, v_n),$$

then the *composite* $v \circ \phi$ is defined as:

$$v \circ \phi := (v_1 \circ \phi_1, \dots, v_n \circ \phi_n).$$

Note that $v \circ \phi$ is a morphism from $\mathscr{R}$ to $\mathscr{R}''$.

7.1.4 Isomorphisms

If, for a morphism $\phi \colon \mathscr{R} \longrightarrow \mathscr{R}'$, there exists a morphism $\psi \colon \mathscr{R}' \longrightarrow \mathscr{R}$ such that $\phi \circ \psi = \mathrm{id}'_{\mathscr{R}}$ and $\psi \circ \phi = \mathrm{id}_{\mathscr{R}}$, then we say that ϕ is an *isomorphism* between $\mathscr{R}$ and $\mathscr{R}'$, and ψ is the *inverse* of ϕ.

7.1.5 Endomorphisms and automorphisms

A morphism $\phi \colon \mathscr{R} \longrightarrow \mathscr{R}$ is often called an *endomorphism of* $\mathscr{R}$. If, additionally, ϕ is an isomorphism, we say that ϕ is an *automorphism* of $\mathscr{R}$.

7.2 Morphisms between mappings

7.2.1

In the case of mappings of n variables we have the following simple characterization of isomorphisms.

Exercise 92 *Prove that a morphism $\phi = (\phi_1, \dots, \phi_n, \phi_{n+1})$ between mappings is an isomorphism if and only if each $\phi_i \colon X_i \longrightarrow X'_i$ and $\phi_{n+1} \colon Y \longrightarrow Y'$ are bijections.*

A morphism ϕ from a map $f \colon X_1 \longrightarrow X_2$ to a map $g \colon X'_1 \longrightarrow X'_2$ is the same as a pair of maps $\phi_i \colon X_i \longrightarrow X'_i$, where $i = 1$ or 2, such that the following diagram commutes:

$$\begin{tikzcd} X_1 \arrow[r, "f"] \arrow[d, dashed, "\phi_1"'] & X_2 \arrow[d, dashed, "\phi_2,"] \\ X'_1 \arrow[r, "g"'] & X'_2 \end{tikzcd}$$

i.e., $\phi_2 \circ f = g \circ \phi_1$.

7.2.2

In the special case when some X_i is *assumed* to coincide with some X_j, one can require from morphisms between such relations to satisfy $\phi_i = \phi_j$. We shall refer to such morphisms as *strict* morphisms. An example of this situation arises in the case of n-ary operations on sets.

7.3 Morphisms between operations

7.3.1 Homotopisms

Given two sets equipped with n-ary operations

$$\mu \colon X \times \cdots \times X \longrightarrow X$$

and

$$\mu' \colon X' \times \cdots \times X' \longrightarrow X'$$

one can consider morphisms between them to be the morphisms between the corresponding $(n+1)$-ary relations, i.e., the $(n+1)$-tuples of maps $(\phi_1, \dots, \phi_{n+1})$ from X to X' such that, for any $x_1, \dots, x_n \in X$,

$$\mu'\big(\phi_1(x_1), \dots, \phi_n(x_n)\big) = \phi_{n+1}\big(\mu(x_1, \dots, x_n)\big). \tag{151}$$

This is what we call a *homotopism* (or, *homotopy*) from (X, μ) to (X', μ').

7.3.2 Homomorphisms

When ϕ_i are all equal we obtain the definition of a *homomorphism* from (X,μ) to (X',μ'). Thus, a homomorphism $(X,\mu)\longrightarrow(X',\mu')$ is a mapping $\phi\colon X\longrightarrow X'$ such that

$$\mu'\big(\phi(x_1),\dots,\phi(x_n)\big)=\phi\big(\mu(x_1,\dots,x_n)\big). \tag{152}$$

Exercise 93 *Show that a mapping $\phi\colon X\longrightarrow X'$ is a homomorphism of n-ary structures if and only if the graph Γ_ϕ is a substructure of the product structure on $X\times X'$.*

Exercise 94 *Given three n-ary structures (X,μ), (X',μ'), and (X'',μ''), and substructures E of the product structure on $X\times X'$, and F of the product structure on $X'\times X''$, show that $E\circ F$ is a substructure of the product structure on $X\times X''$.*

7.3.3 Correspondences between n-ary structures

Exercises 93 and 94 indicate that substructures of the product structure on $X\times X'$ can be composed like homotopisms and homomorphisms. We shall refer to them as *correspondences* between (X,μ) and (X',μ').

7.3.4 Isotopisms and isomorphisms

Invertible homotopisms are called *isotopisms* (or *isotopies*), while invertible homomorphisms are called *isomorphisms* of n-ary structures.

Exercise 95 *Suppose that $E\subseteq X\times X'$ is an invertible correspondence, i.e., there exists a correspondence $F\subseteq X'\times X$ such that*

$$E\circ F=\Delta_X \qquad \text{and} \qquad F\circ E=\Delta_{X'}.$$

Show that $E=\Gamma_f$ and $F=\Gamma_{f^{-1}}$ for an isomorphism $f\colon(X,\mu)\longrightarrow(X',\mu)$.

7.3.5

Thus, invertible correspondences are necessarily the graphs of isomorphisms or, since we identify mappings between sets with their graphs, we can say that any invertible correspondence is an isomorphism.

Exercise 96 *Prove that any quasigroup, $(Q, \cdot)$, is isotopic to a loop. (Hint: Find two bijections, f_1 and f_2, of set Q onto itself such that Q equipped with the operation*

$$(q_1, q_2) \longmapsto q_1 \circ q_2 := (f_1)^{-1}(q_1) \cdot (f_2)^{-1}(q_2)$$

is a loop.)

7.3.6 Example: Steiner systems

A set $(X, \triangleright)$ equipped with a totally symmetric ternary relation satisfying the property that, for any distict $x, y \in X$, there exists a unique $z \in X$, which is distinct from both x and y, such that

$$\triangleright(x, y, z), \tag{153}$$

is called a *Steiner triple system*. For any Steiner system, there is an associated quasigroup operation on X,

$$x \cdot y := \begin{cases} \text{the unique } z \text{ such that } \triangleright(x,y,z) & \text{if } x \neq y \\ x & \text{if } x = y \end{cases}.$$

Exercise 97 *Prove that any totally symmetric quasigroup $(Q, \cdot)$, in which every element is an idempotent is associated with a Steiner triple system.*

7.3.7

There is a unique Steiner triple system structure on a set of cardinality 3. If we denote the elements of this set by $\{0, 1, 2\}$, then the associated operation is, using the integer arithmetic modulo 3,

$$(x, y) \longmapsto x \cdot y := -x - y.$$

The corrsponding quasigroup is isotopic but not isomorphic to the group $(\{0, 1, 2\}, +)$, where $+$ denotes addition modulo 3, via the isotopism

$$(\mathrm{id}, \mathrm{id}, -\mathrm{id}).$$

Exercise 98 *Prove that any self-bijection $f \in \mathrm{Bij}\{0, 1, 2\}$ is an automorphism of the quasigroup $(\{0, 1, 2\}, \cdot)$ associated with the unique Steiner triple system on $\{0, 1, 2\}$.*

7.3.8 Isotopisms from a semigroup to a structure with identity

Let $\phi = (f', f'', f)$ be an isotopism from a semigroup $(S, \circ)$ to a binary structure $(X, \cdot)$ with an identity element e.

Denote the inverse mapping $f^{-1}\colon X \longrightarrow S$ by g. The identities

$$f((s \circ t) \circ u) = f'(s \circ t) \cdot f''(u) = f'g\big(f'(s) \cdot f''(t)\big) \cdot f''(u)$$

and

$$f(s \circ (t \circ u)) = f'(s) \cdot f''(t \circ u) = f'(s) \cdot f''g\big(f'(t)) \cdot f''(u)\big),$$

combined with the identity $(s \circ t) \circ u = s \circ (t \circ u)$, imply that

$$f'g\big(f'(s) \cdot f''(t)\big) \cdot f''(u) \;=\; f'(s) \cdot f''g\big(f'(t)) \cdot f''(u)\big). \tag{154}$$

If we adopt the simplified notation by omitting parentheses around the arguments where possible, identity (154) becomes

$$f'g(f's \cdot f''t) \cdot f''u \;=\; f's \cdot f''g(f't \cdot f''u) \qquad (s, t, u \in S). \tag{155}$$

Exercise 99 *Under hypothesis that $(X, \cdot)$ has an identity element, deduce from identity* (155) *the following three identities*

$$f'gf''t \cdot f''u \;=\; f''g(f't \cdot f''u) \tag{156}$$

$$f'g(f's \cdot f''t) \;=\; f's \cdot f''gf't \tag{157}$$

$$f'gf'' \;=\; f''gf' \tag{158}$$

where s, t and u denote arbitrary elements of S.

Exercise 100 *Deduce from identities* (156)–(158) *the following two identities*

$$f''gx \cdot y \;=\; f''g(x \cdot y) \tag{159}$$

$$f'g(x \cdot y) \;=\; x \cdot f'gy \tag{160}$$

where x and y denote arbitrary elements of X.

7.3.9

Let

$$\bar{\phi} := f'gf'' = f''gf'.$$

For any s and t in S, we have

$$\begin{aligned}\bar{\phi}(s \circ t) &= \bar{\phi}g(f's \cdot f''t) = f'gf''g(f's \cdot f''t) \\ &= f'g(f''gf's \cdot f''t) = f''gf's \cdot f'gf''t \\ &= \bar{\phi}s \cdot \bar{\phi}t.\end{aligned}$$

The third equality follows from identity (159), the fourth equality follows from identity (160).

7.3.10

We proved above that the mapping

$$\phi = (f', f'', f) \longmapsto \bar{\phi} := f'f^{-1}f''$$

is a *retraction* of the set of isotopisms ϕ from a semigroup $(S, \circ)$ to a binary structure with identity $(X, \cdot)$ onto the set of isomorphisms from $(S, \circ)$ to $(X, \cdot)$.

7.3.11

In particular, we discovered that a semigroup isotopic to a structure with identity has an identity itself. In particular, it is a monoid. Vice-versa, a structure with identity isotopic to a semigroup is associative itself. In particular, it is a monoid.

7.3.12 Autotopisms and automorphisms

Isotopisms whose source and target coincide are called *autotopisms*. Similarly, isomorphisms with the source and the target coincide are called *automorphisms*.

Autotopisms of (X, μ) form a group (cf. Exercise 92) which we will denote $A(X, \mu)$. The latter contains two subgroups: the group of *automorphisms*, $\mathrm{Aut}(X, \mu)$, and the group of *principal* autotopisms, $A_0(X, \mu)$, i.e., autotopisms of the form:

$$(\phi_1, \ldots, \phi_n, \mathrm{id}_X). \tag{161}$$

Exercise 101 *Prove that any isotopism*

$$(X, \mu) \xrightarrow{\phi=(\phi_1,\ldots,\phi_{n+1})} (Y, \nu)$$

canonically factorizes as the composition of a principal autotopism and an isomorphism:

$$\begin{tikzcd}
(X, \mu) \arrow[rr, "\phi=(\phi_1,\ldots,\phi_{n+1})"] \arrow[dr, "(\dot{\psi}_1,\ldots,\psi_n,\mathrm{id}_X)"'] & & (Y, \nu) \\
& (X, \mu') \arrow[ur, "\phi_{n+1}"'] &
\end{tikzcd}$$

for some n-ary operation μ' on X. (Hint: First find μ'.)

Exercise 102 *Prove that the group of principal autotopisms, $A_0(X, \mu)$, is a normal subgroup of the group of all autotopisms, $A(X, \mu)$.*

Exercise 103 *Let $(X, \cdot)$ be a binary structure. Consider a binary relation on set X:*

$$x \sim y \quad \textit{if} \quad \phi(x) = \phi(y) \textit{ for any homomorphism } \phi \textit{ into any semigroup.} \tag{162}$$

Show that $\sim$ is a congruence on $(X, \cdot)$ and that, for any homomorphism $\phi\colon X \longrightarrow S$ into a semigroup S, there exists a unique *homomorphism $\tilde{\phi}\colon X/_\sim \longrightarrow S$ such that $\phi = \tilde{\phi} \circ \pi$ where $\pi\colon X \longrightarrow X/_\sim$ is the canonical epimorphism.*

7.3.13 Homomorphisms and antihomomorphisms of binary structures

In the case of binary structures, a homomorphism from $(G, \cdot)$ to $(G', \cdot)$ is a map $\phi\colon G \longrightarrow G'$ such that

$$\phi(gh) = \phi(g)\phi(h) \tag{163}$$

for any $g, h \in G$.

If a map ϕ satisfies instead the identity

$$\phi(gh) = \phi(h)\phi(g) \qquad (g, h \in G), \tag{164}$$

then we say that ϕ is an *antihomomorphism*.

7.3.14

Composition of a homomorphism with an antihomomorphism is an antihomomorphism. Composition of two antihomomorphisms is a homomorphism.

7.3.15 The opposite binary structure

For any binary structure, $(G, \cdot)$ we define the *opposite* binary structure, $(G, \cdot)^{op} = (G^{op}, \cdot^{op})$, by setting G^{op} to be the set G whose elements, however, will be denoted g^{op} in order to clearly indicate which structure are we considering, and multiplication given by

$$g^{op}h^{op} := (hg)^{op}. \tag{165}$$

Then

$$(\ )^{op}_G \colon (G, \cdot) \longrightarrow (G^{op}, \cdot^{op}), \qquad g \longmapsto g^{op}, \tag{166}$$

can be thought of as a canonical *anti*isomorphism of $(G, \cdot)$ onto $(G^{op}, \cdot^{op})$.

7.3.16

One has $(G, \cdot)^{op} = (G, \cdot)$ if and only if $(G, \cdot)$ is commutative.

7.3.17

Note that $((G, \cdot)^{op})^{op} = (G, \cdot)$, and

$$(\ )^{op}_{G^{op}} \circ (\ )^{op}_G = id_G. \tag{167}$$

7.3.18 Functoriality of the opposite structure

Any homomorphism $\phi \colon G \longrightarrow G'$ induces a homomorphism of the corresponding opposite structures, $\phi^{op} \colon G^{op} \longrightarrow (G')^{op}$,

$$\phi^{op} := (\ )^{op}_{G'} \circ \phi \circ (\ )^{op}_{G^{op}}. \tag{168}$$

7.3.19

If $\phi\colon G \longrightarrow G'$ is an antihomomorphism, then both

$$\phi \circ (\ )^{op}_{G^{op}}\colon G^{op} \longrightarrow G'$$

and

$$(\ )^{op}_{G'} \circ \phi\colon G \longrightarrow (G')^{op}$$

are homomorphisms, and vice-versa.

This allows us to view antihomomorphisms as homomorphisms, except that the source, or the target, has to be replaced by the opposite structure.

7.4 Morphisms between ν-structures

7.4.1 Homomorphisms between ν-structures

A homomorphism between ν-structures (X, M) and (X', M') is a mapping $f\colon X \longrightarrow X'$ that is compatible with *all* operations, i.e., for each $i \in I$, the identity

$$\mu'_j\Big(f(x_1), \dots, f(x_{\nu(j)})\Big) \;=\; f\Big(\mu_j(x_1, \dots, x_{\nu(j)})\Big) \qquad (x_1, \dots, x_{\nu(j)}) \tag{169}$$

holds.

7.4.2

It follows from Exercise 93 that a mapping $f\colon X \longrightarrow X'$ is a homomorphism if and only if its graph Γ_f is a substracture of the product structure on $X \times X'$.

7.4.3 Correspondences between ν-ary structures

Subsets of $X \times X'$ which are substructures of the product of structures (X, M) and (X', M') will be referred to as *correspondences* between (X, M) and (X', M').

Composition of such correspondences is again a correspondence between ν-ary stuctures. An invertible correspondence is automatically a homomorphism.

7.4.4

In the case of sets, i.e., ν-ary structures with ν being the inclusion of the empty set into $\mathbf{N}$, we obtain the original definition of a correspondence on sets, cf. Section 2.4.6

8 Group Theory

8.1 $*$-semigroups

8.1.1

Any semigroup G is antiisomorphic to G^{op}, cf. (166). Some semigroups are also *isomorphic* to their opposites or, what is the same, antiisomorphic to themselves.

This happens, for example, when G admits an *antiinvolution*, i.e. an antiisomorphism $*\colon G \longrightarrow G$ such that

$$*(*g)) = g \qquad (g \in G).$$

Such semigroups are called $*$-semigroups. They form an important class of $*$-semigroups.

8.1.2

Every group is equipped with a canonical antiinvolution that sends an element to its inverse,

$$g \longmapsto g^{-1}.$$

8.2 Cyclic groups

8.2.1 The order of an element

The smallest positive integer n such that $g^n = e$ is denoted $|g|$ and called the *order* of an element g of a group G. If no such integer exists we say that g is an element of *infinite order*.

Exercise 104 *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism. Show that, for any element $g \in G$, the order of $\phi(g)$ divides the order of g.*

Exercise 105 *Prove that any subgroup of a cyclic group is cyclic.*

Exercise 106 *Let C be a cyclic group of order n. Prove that for any positive divisor d of n, there exists a unique subgroup $D \subseteq C$ of that order.*

For any two such sungroups D and E, show that $D \subseteq E$ if and only if $|D|$ divides $|E|$.

Exercise 107 *For any elements a and b in a group G, their* commutator *is defined as*

$$[a,b] := aba^{-1}b^{-1}. \tag{170}$$

Let

$$[G,G] := \{g \in G \mid g = [a_1,b_1]\cdots[a_r,b_r] \text{ for some } a_1,b_1,\ldots,a_r,b_r \in G\}. \tag{171}$$

Show that $[G,G]$ is a normal subgroup (this subgroup is called the commutator subgroup *of G). Show that the factor-group $G/[G,G]$ is abelian, and that every homomorphism $\phi\colon G \longrightarrow A$ into an abelian group factorizes through $G/[G,G]$.*

Exercise 108 *Let G be a group such that $g^2 = e$ for each $g \in G$. Show that G is abelian.*

Exercise 109 *Let G be a group such that $G/Z(G)$ is cyclic. Show that G is abelian. (Hint. Let $g \in G$ be an element that is sent by the canonical factor-map $G \twoheadrightarrow G/Z(G)$ to a generator of $G/Z(G)$. Show that $G = Z(G)\langle g\rangle$ and use this fact.)*

Exercise 110 *Let G be a nonabelian group of order 8. Show that there exists an element $a \in G$ of order 4 and show that, for any element $b \in G \setminus \langle a\rangle$, one has $bab^{-1} = a^{-1}$.*

If every element of $G \setminus \langle a\rangle$ is of order 2, the group is called the dihedral group *of order 8 and denoted D_8 or, in older notation, D_4. It is isomorphic to the group of symmetries of the square.*

If, on the other hand, $G \setminus \langle a\rangle$ contains an element of order 4, then show that it is isomorphic to the multiplicative group of quaternions:

$$Q := \{\pm 1, \pm i, \pm j, \pm k\} \tag{172}$$

where i, j, k are the imaginary quaternions. Because of this isomorphism, the unique up to isomorphism group of order 8 with a pair of noncommuting elements of order 4 is called the quaternion *group and is denoted Q.*

Exercise 111 *For both D_8 and Q, do the following.*

Let a be any element of order 4 and b be any element of $G \setminus \langle a \rangle$. Show that the cyclic subgroup, $\langle a \rangle$, is normal, and every element $g \in G$ has a representation,

$$g = a^i b^j, \tag{173}$$

for unique $i \in \mathbf{Z}/4\mathbf{Z}$ and $j \in \mathbf{Z}/2\mathbf{Z}$, in the dihedral case, and $j \in \mathbf{Z}/4\mathbf{Z}$, in the quaternion case.

Write down all elements, (173), of order 2 in G.

Find all subgroups of G and draw a diagram that displays which subgroup is contained in which one. (Do not forget about the trivial subgroups: $\{e\}$ and G).

Find the center, $Z(G)$, of G and its commutator subgroup, $[G, G]$.

Exercise 112 *Determine the structure of the group of automorphisms of cyclic groups of order 2, 4, 8, 16. Formulate a general hypothesis regarding the group of automorphisms of a cyclic group of order 2^n (and prove it, if you can).*

Exercise 113 *Determine the structure of the group of automorphisms of cyclic groups of order 3, 9, 27. Formulate a general hypothesis regarding the group of automorphisms of a cyclic group of order 3^n (and prove it, if you can).*

8.3 Group extensions

8.3.1

Definition 8.1 *A pair of group homomorphisms*

$$\mathscr{E} \ : \qquad G \xleftarrow{\ \pi\ } E \xleftarrow{\ \iota\ } N \tag{174}$$

is called an extension of G by N *if π is an epimorphism, ι is a monomorphism, and* $\operatorname{Ker} \pi = \operatorname{Im} \iota$.

8.3.2 Notation

When dealing with group extensions usually a special notation is employed:

$$\begin{tikzcd} G & E \arrow[l, two heads, "\pi"'] & N \arrow[l, tail, "\iota"'] \end{tikzcd}$$

or

$$\begin{tikzcd} 1 & G \arrow[l] & E \arrow[l, two heads, "\pi"'] & N \arrow[l, tail, "\iota"'] & 1 \arrow[l] \end{tikzcd}$$

Here 1 stands for the trivial, one-element group.

8.3.3 Terminology

By extension, we call the group in the middle, E, an extension of G by N. Group N is called the *kernel* of the extension.

8.3.4 Restriction of an extension to a subgroup

Exercise 114 *If H is a subgroup of G, show that $F := \pi^{-1}(H)$ is a subgroup of E.*

We speak in this case of

$$\begin{tikzcd} H & F \arrow[l, two heads, "\pi_{|F}"'] & N \arrow[l, tail, "\iota"'] \end{tikzcd}$$

as the *restriction* of extension $\mathscr{E}$ to H.

$$\begin{tikzcd} G & E \arrow[l, two heads, "\pi"'] & N \arrow[l, tail, "\iota"'] \end{tikzcd}$$

8.3.5

Exercise 115 *If G and N are finite, show that*

$$|E| = |G|\,|N|.$$

8.3.6 Split extensions

An extension $\mathscr{E}$ is said to be *split* if there exists a homomorphism $\sigma\colon G\longrightarrow E$ such that $\pi \circ \sigma = \mathrm{id}_G$. Such a homomorphism is called a *splitting* of extension $\mathscr{E}$.

Exercise 116 *Show that a group extension,* (174), *is split if and only if there exists a subgroup $G' \subseteq E$ such that $\pi_{|G'}$ is an isomorphism between G' and G.*

The following theorem is one of the fundamental results of Finite Group Theory.

Theorem 8.2 (Schur–Zassenhaus) *If G and N are finite groups and their orders are relatively prime, then any extension of G by N is split.* □

8.3.7 Morphisms of extensions

A morphism of an extension $\mathscr{E}$ into an extension $\mathscr{E}'$ consists of three group homomorphisms $f_0\colon G\longrightarrow G'$, $f_1\colon E\longrightarrow E'$ and $f_2\colon N\longrightarrow N'$ such that the squares in the following diagram

$$\begin{tikzcd}
\mathscr{E}\ : & G \arrow[d, dashed, "f_0"] & E \arrow[l, two heads, "\pi"'] \arrow[d, dashed, "f_1"] & N \arrow[l, tail, "\iota"'] \arrow[d, dashed, "f_2"] \\
\mathscr{E}'\ : & G' & E' \arrow[l, two heads, "\pi'"'] & N' \arrow[l, tail, "\iota'"']
\end{tikzcd}$$

commute.

8.3.8 Trivial extensions

An extension $\mathscr{E}$ is said to be trivial if it is isomorphic to the extension

$$G \xleftarrow{p_2} N\times G \xleftarrow{i_1} N \tag{175}$$

where $p_2\colon N\times G\longrightarrow G$ is the projection onto the second factor, and

$$i_1\colon N\longrightarrow N\times G, \qquad n \longmapsto (n,e)$$

is the inclusion of the first factor, N, into $G\times N$.

8.3.9 Central extensions

If the kernel, N, of extension $\mathscr{E}$ is contained in the center of E, then we say that the extension is *central*.

A central extension is split if and only if it is trivial.

8.3.10

Central extensions play a fundamental role in modern Mathematics and Mathematical Physics.

8.4 Solvable groups

8.4.1 Classes of groups closed under extensions

Definition 8.3 *We say that some class $\mathscr{C}$ of groups is* closed under extensions *if in any extension,* (174)*, where G and N belong to class $\mathscr{C}$, also the middle group, E, belongs to $\mathscr{C}$.*

8.4.2 Classes of groups closed under extensions

The class of finite groups is obviously closed under extensions. A less obvious example is provided by so called torsion groups.

Definition 8.4 *We say that a group G is a* torsion group *if every element $g \in G$ has a finite order.*

Exercise 117 *Show that the class of torsion groups is closed under extensions.*

8.4.3

The class of abelian groups is obviously *not* closed under extensions. We shall explicitly construct the smallest class closed under extensions which contains the class of abelian groups. Denote the latter class by $\mathscr{S}_0$. Groups E that are extensions of an abelian group G by an abelian group N will form the larger class that will be denoted $\mathscr{S}_1$. Groups E that are extensions of an abelian group G by a group N of class $\mathscr{S}_1$ will form even the larger class that will be denoted $\mathscr{S}_2$, and so on: groups E that are extensions of an abelian group G by a group N of class $\mathscr{S}_l$ will form the class denoted $\mathscr{S}_{l+1}$.

Definition 8.5 *We say that a group G is* solvable *if it is of class $\mathscr{S}_l$ for some $l \geq 0$.*

Exercise 118 *Show that class $\mathscr{S}_1$ defined above coincides with the class of groups E whose commutator subgroup $[E, E]$ is abelian.*

8.4.4 Derived series

For any group G, define inductively the sequence of subgroups

$$G^{(0)} := G, \qquad \text{and} \qquad G^{(l+1)} := [G^{(l)}, G^{(l)}]. \tag{176}$$

Exercise 119 *Prove, by induction on l, that any subgroup F of a group E of class $\mathscr{S}_l$ is of class $\mathscr{S}_l$ itself.*

Exercise 120 *Prove, by induction on l, that class $\mathscr{S}_l$ defined above coincides with the class of groups E such that $E^{(l+1)} = 1$ or, equivalently, such that $E^{(l)}$ is abelian. (Hint. Use Exercise 119 and note that $[E,E]^{(l)} = E^{(l+1)}$.)*

8.4.5

It follows that the class of solvable groups coincides with the class of groups for which the *derived series* terminates after finitely many terms in the trivial group

$$E = E^{(0)} \triangleright E^{(1)} \triangleright \cdots \triangleright E^{(l+1)} = 1. \tag{177}$$

9 Actions

9.1 Vocabulary

9.1.1

Definition 9.1 *We say that a semigroup G* acts *on a set X if a map*

$$G \times X \longrightarrow X, \qquad (g,x) \longmapsto gx \tag{178}$$

is given such that

$$(gh)x = g(hx) \tag{179}$$

for all $g,h \in G$ and $x \in G$. The map, (178)*, satisfying* (179) *is called an* action *of G on X and a set equipped with such an action is referred to as a G*-set*.*

9.1.2

A G-action on X induces a homomorphism into the monoid of self-maps, $\mathrm{Map}(X,X)$,

$$\lambda\colon (G,\cdot)\longrightarrow(\mathrm{Map}(X,X),\circ), \qquad g\longmapsto \lambda_g, \tag{180}$$

where

$$\lambda_g(x) := gx. \tag{181}$$

And vice-versa, any homomorphism of G into $\mathrm{Map}(X,X)$. defines a G-action on X:

$$(g,x)\longmapsto \lambda_g(x). \tag{182}$$

9.1.3 Equivariant maps

Given two G-sets, X and Y, a map $f\colon X\longrightarrow Y$ is said to be *equivariant* (or, G-equivariant, for added clarity), if

$$f(gx) = gf(x) \tag{183}$$

for any $g\in G$ and $x\in X$.

Equivariant maps play the role of morphisms in the world of G-sets when G is fixed.

9.1.4 Orbits

For any element $x\in X$, the subset of X

$$Gx := \{gx \mid g\in G\} \tag{184}$$

is called the *orbit* of x.

9.1.5 Stabilizers

For any element $x\in X$, the subset of G

$$G_x := \{g\in G \mid gx = x\} \tag{185}$$

is called the *stabilizer* of x, or the *isotropy* semigroup of x.

The stabilizer of any element $x\in X$ is indeed a semigroup. The stabilizer is also sometimes denoted $\mathrm{stab}_G(x)$. Remember to never confuse G_x with Gx!

9.1.6 Invariant subsets

A subset $A \subseteq X$ of a G-set is said to be *invariant* (under the action of G) if $gx \in A$ for every $x \in X'$. More natural would be to call such subsets G-subsets.

9.1.7 Fixed points

An element x of a G-set is called a *fixed point* (of the action) if

$$gx = x \qquad \text{for every } g \in G. \tag{186}$$

9.1.8 Right actions

What we have defined in Definition 9.1, was, properly speaking, a *left* action of a semigroup G on a set X. There is als a related notion of *right action*.

Definition 9.2 *We say that a semigroup G* acts *on a set X* on the right *if a map*

$$X \times G \longrightarrow X, \qquad (x, g) \longmapsto xg \tag{187}$$

is given such that

$$x(gh) = (xg)h \tag{188}$$

for all $g, h \in G$ and $x \in G$. The map, (178), *satisfying* (179) *is called a* right action *of G on X and a set equipped with such an action is referred to as a* right G-set.

9.1.9 An example: the left and the right regular actions

For any semigroup G, the multiplication map

$$G \times G \longrightarrow G$$

can be thought as a left action of G on itself as well as a right action of G on itself. In the first case, we call it the *left multiplication* action, or the *left regular action* of G. In the second case, we refer to it as the *right multiplication* action, or the *right regular action* of G.

9.1.10

A right G-action on X induces an *anti*homomorphism into the monoid of self-maps, $\mathrm{Map}(X, X)$,

$$\rho\colon (G, \cdot) \longrightarrow (\mathrm{Map}(X, X), \circ), \qquad g \longmapsto \rho_g, \tag{189}$$

where

$$\rho_g(x) := xg. \tag{190}$$

And vice-versa, any anti-homomorphism of G into $\mathrm{Map}(X, X)$. defines a G-action on X:

$$(x, g) \longmapsto \rho_g(x). \tag{191}$$

9.1.11

A right action of G is the same as the left action of G^{op}:

$$(g^{op})x := xg \qquad (g \in G, x \in X).$$

If G is a $*$-semigroup, any right action of G can be converted into a left action with help of the antiinvolution:

$$gx := x(*g)$$

For example, in the case of a group,

$$(G, X) \longrightarrow X, \qquad x \longmapsto xg^{-1},$$

is a (left) action.

9.1.12 Induced actions

An action on a set X may induce a number of related actions. An example is provided by the natural action on the set of all subsets, $\mathscr{P}(X)$ of X,

$$(g, A) \longmapsto gA := \{ga \mid a \in A\} \qquad (A \subseteq X). \tag{192}$$

Note that, invariants subsets of X are precisely the fixed points of this action.

9.1.13

If S is any set and X is a G-set, then G acts naturally on the set of all maps from S to X: a map $F\colon S\longrightarrow X$ is sent under $g\in G$ to the map

$$(gF)(s) := gF(s) \qquad (s\in S). \tag{193}$$

9.1.14

Similarly, the formula

$$(Fg)(x) := F(gx) \qquad (x\in X) \tag{194}$$

defines a natural *right* action on the set of all maps from G to S.

9.1.15 Restriction of an action to an invariant subset

Given an invariant subset $A\subseteq X$ one can *restrict* the action to A to make A into a G-set.

9.1.16 Product of G-sets

Given two G-sets X and Y, there is a natural action of G on $X{\times}Y$:

$$g(x,y) := (gx,gy) \qquad (g\in G,\ x\in X,\ y\in Y). \tag{195}$$

and similarly for the general case of the product of any family of G-sets.

9.1.17 Equivariant relations

Given G-sets $X_1,\dots,X_n$, we say that an n-ary relation $(X_1,\dots,X_n,\mathscr{R})$ is *equivariant* if, for any $x_1\in X_1,\dots,x_n\in X_n$, and $g\in G$, one has

$$\mathscr{R}(x_1,\dots,x_n) \quad \text{implies} \quad \mathscr{R}(gx_1,\dots,gx_n). \tag{196}$$

9.1.18 Quotient G-sets

If G-subsets of a G-set X are just invariant subsets, then the G-quotients of X are the quotients $X/_{\sim}$ by equivariant equivalence relations. Note that the equivalence class $[gx]$ in this case depends only on the equivalence class $[x]$. In particular, the formula

$$g[x] := [gx]$$

defines an induced action of G on $X/_\sim$.

9.2 Group actions

9.2.1

When a group G acts on a set X, then any $\lambda_g\colon X \longrightarrow X$ is a bijection since

$$\lambda_e = \mathrm{id}_X \quad \text{and therefore} \quad (\lambda_g)^{-1} = \lambda_{g^{-1}}$$

for any $g \in G$. Hence, a G-action is the same as a homomorphism from G into the group $\operatorname{Bij} X$ of self-bijections, otherwise known as *permutations* of X:

$$\lambda\colon G \longrightarrow \operatorname{Bij} X. \tag{197}$$

9.2.2 Orbital decomposition of a G-set

Exercise 121 *Let G be a group acting on a set X. Show that any two orbits $\mathscr{O}$ and $\mathscr{O}'$ are either equal or disjoint.*

In particular, orbits of any group action on X form a partition of X which must correspond to some equivariant equivalence on X. The quotient is denoted X/G in this case. It is the *largest* quotient G-set of X on which G acts trivially.

The set, X/G, is often called the *space of orbits* of the G-action, or the *quotient of X by the action of G*.

9.2.3 The adjoint action

Besides the left and right multiplication actions, group G acts on G also by *conjugation*,

$$(g, x) \longmapsto {}^g x := gxg^{-1} \qquad (g, x \in G). \tag{198}$$

For any $g \in G$, the map

$$\mathrm{ad}_g\colon x \longmapsto {}^g x \qquad (x \in G) \tag{199}$$

is an automorphism of group G. Such automorphisms are called *inner*.

9.2.4

In literature very often one encounters notation $x^g := g^{-1}xg$. Note that,

$$(x, g) \longmapsto x^g$$

is a *right* action.

Exercise 122 *Let* $\alpha \in \operatorname{Aut} G$ *be any automorphism of group* G*. Show that the group of inner automorpisms,*

$$\operatorname{Inn} G := \{\operatorname{ad}_g \mid g \in G\}, \tag{200}$$

is a normal subgroup of $\operatorname{Aut} G$*. (Hint: prove that*

$$\alpha \circ \operatorname{ad}_g \circ \alpha^{-1} = \operatorname{ad}_{\alpha(g)} \tag{201}$$

for any $g \in G$*.)*

9.2.5 Outer automorphisms

The quotient group

$$\operatorname{Out} G := \operatorname{Aut} G / \operatorname{Inn} G \tag{202}$$

is called the group of *outer* automorphisms of G and denoted $\operatorname{Out} G$. Note that "outer automorphisms" are *not* automorphisms of group G but the cosets in $\operatorname{Aut} G$ of the subgroup of inner automorphisms $\operatorname{Inn} G$.

9.2.6 Conjugacy classes

The orbit of an element $x \in G$ under the adjoint action is called the *conjugacy class* of G.

9.2.7 Centralizers

For any element $a \in G$, the stabilizer of a under the adjoint action of G coincides with the so called centralizer of a,

$$C_G(a) := \{g \in G \mid ga = ag\}. \tag{203}$$

If $A \subseteq G$ is a subset, then its centralizer is the intersection of centralizers of all of its elements,

$$C_G(A) := \bigcap_{a \in A} C_G(a). \tag{204}$$

Exercise 123 *Show that, for any subset A of G, its centralizer $C_G(A)$ is a subgroup of G. Express $C_G({}^gA)$ in terms of $C_G(A)$ and $g \in G$.*

9.2.8 Normalizers

If $A \subseteq G$ is a subset, then its *normalizer*,

$$N_G(A) := \{g \in G \mid {}^gA = A\} \tag{205}$$

is the stabilizer of A with respect to the action on $\mathscr{P}(G)$ induced by the adjoint action.

Exercise 124 *Show that, for any subset A of G, its normalizer $N_G(A)$ is a subgroup of G. Express $N_G({}^gA)$ in terms of $N_G(A)$ and $g \in G$.*

Exercise 125 *Let G be a group acting on a set X and. Show that, for any $x \in X$, the stabilizer, G_x is a subgroup of G, and that*

$$G_{gx} = {}^gG_x. \tag{206}$$

9.2.9

Exercise 126 *Consider the action of a group G on itself by left multiplication. For any subgroup $H \subseteq G$, show that*

$$x \sim_H y \qquad \text{if} \qquad y^{-1}x \in H \tag{207}$$

is an equivariant equivalence on G-set G.

Vice-versa, prove that any *equivariant equivalence on G is of the form,* (207), *for some subgroup H. (Hint: Find the candidate for H first.)*

Note that the the G-quotient, $G/_{\sim_H}$, is just the set of the left cosets, G/H.

Exercise 127 *Let G be a group and X be any G-set. Show that for any $x \in X$, the map*

$$G/H \longrightarrow Gx, \qquad gH \longmapsto gx, \tag{208}$$

where $H = G_x$, is an isomorphism of G-sets.

In particular, if the orbit of an element $x \in X$ is finite, then its cardinality equals the index of the stabilizer of x in G,

$$|Gx| = |G : G_x|. \tag{209}$$

9.2.10

By combining (209) with Exercise 121 we obtain the following observation.

Observation 9.3 *For any finite G-set X, one has the following identity*

$$|X| = \sum_{\mathscr{O}} |G : G_x|, \tag{210}$$

where the summation extends over all distinct orbits $\mathscr{O} \subseteq X$ and G_x denotes the stabilizer of any single element $x \in \mathscr{O}$.

Exercise 128 *Let H and K be two subgroups of G. Restrict the action of G by left multiplication on G/K to H. Show that the map*

$$H \longrightarrow HK/K, \qquad h \longmapsto hK, \tag{211}$$

induces an isomorphism of H-sets

$$H/H \cap K \simeq HK/K \tag{212}$$

where $HK/K \subseteq G/K$ denotes the subset

$$HK/K := \{hK \in G/K \mid h \in H\}. \tag{213}$$

Exercise 129 *Let H and K be two finite subgroups of G. Show that*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}. \tag{214}$$

Exercise 130 *Let H and K be two subgroups of G. Restrict the action of G by left multiplication on G/K to H. Show that*

$$\operatorname{stab}_H(gK) = H \cap {}^{g}K. \tag{215}$$

Exercise 131 *Let H a subgroup of G. Show that $H = gH$ is a fixed point of the H-action on G/H if and only if $g \in N_G(H)$. In other words,*

$$\operatorname{Fix}_H(G/H) = N_G(H)/H, \tag{216}$$

and thus the number of fixed points of the H-action on G/H equals the index of H in its normalizer, $N_G(H)$,

$$|\operatorname{Fix}_H(G/H)| = |N_G(H) : H|. \tag{217}$$

Exercise 132 *Let H be a subgroup of G. Consider the set of all the conjugate subgroups,*

$$X := \{{}^{g}H \mid g \in G\} \tag{218}$$

Show that

$$|X| = |G : N_G(H)|. \tag{219}$$

Group G acts on X by conjugation.

$$\mathrm{stab}_G({}^{g}H) = {}^{g}N_G(H). \tag{220}$$

9.2.11 Restriction of an action to a subgroup

A G-set X can be viewed as an H-set for any subgriup H of G by restrictiong the action to elements $h \in H$. In this case its orbit structure is different. Any G-orbit $\mathscr{O} = Gx$ is naturally H-invariant but H may not act on $\mathscr{O}$ transitively.

9.2.12

Subgroup H acts on Gx transitively if and only if

$$G = H \cdot \mathrm{stab}_G(x). \tag{221}$$

Note that in this case also $G = {}^{g}H \cdot \mathrm{stab}_G(x)$ for any $g \in G$.

Exercise 133 *Deduce that that the conjugacy class of $a \in G$ in G equals the conjugacy class of a with respect to H if and only if*

$$G = HC_G(a) \tag{222}$$

9.2.13 Frattini's Argument

Exercise 134 *By looking at the action on the power set $\mathscr{P}(G)$ which is induced by the adjoint action of G, we deduce that the set of G-conjugates of a subset $S \subseteq G$ coincides with the set of H-conjugates,*

$$ {}^{G}S = {}^{H}S, \tag{223}$$

if and only if

$$G = HN_G(S). \tag{224}$$

(Note that both ${}^{G}S$ and ${}^{H}S$ are subsets of $\mathscr{P}(G)$, not of G. In other words, they are families *of subsets of G.)*

The above observation is frequently used in Group Theory and it is known under the name of *Frattini's Argument*.

9.3 p-groups

9.3.1

Proposition 9.4 *Let G be a group of order p^n, where p is a prime, and X be a finite G-set. Then*

$$|X| = |\operatorname{Fix}_G(X)| \mod p. \tag{225}$$

Proof. By (210), one has

$$|X| = \sum_{|\mathscr{O}|=1} |G : G_x| + \sum_{|\mathscr{O}|>1} |G : G_x| = |\operatorname{Fix}_G(X)| + \sum_{|\mathscr{O}|>1} |G : G_x|. \tag{226}$$

Each $|\mathscr{O}| = |G : G_x|$ is, by Lagrange's Teorem, a divisor of $|G| = p^n$, and thus is a power of p itself. If $|\mathscr{O}| > 1$, then $|\mathscr{O}|$ is divisible by p. Hence the right-hand-side of (226) is the sum of $|\operatorname{Fix}_G(X)|$ and a natural number divisible by p. □

9.3.2 Cauchy's Theorem

Theorem 9.5 (Cauchy's Theorem) *If a prime p divides the order of a finite group G, then*

$$\{g \in G \mid |g| = p\} = -1 \mod p. \tag{227}$$

In particular, there exists an element of G of order p.

Proof. Consider the action of group $\mathbf{Z}/p\mathbf{Z}$ by cyclic permutations of the factors in G^p:

$$\lambda_i \colon (g_1, \ldots, g_p) \longmapsto (g_{p-i+1}, \ldots, g_p, g_1 \ldots, g_{p-i}), \qquad (i \in \mathbf{Z}/p\mathbf{Z}).$$

Exercise 135 *Show that the subset*

$$X := \{(g_1, \ldots, g_p) \mid g_1 \cdots g_p = e\} \tag{228}$$

is invariant under the action of $\mathbf{Z}/p\mathbf{Z}$.

The map

$$(g_1,\ldots,g_{p-1}) \longmapsto (g_1,\ldots,g_{p-1},(g_1\cdots g_{p-1})^{-}1),$$

provides a bijection from G^{p-1} onto X, hence

$$|X| = |G^{p-1}| = |G|^{p-1}$$

is divisible by p.

A p-tuple $(g_1,\ldots,g_p)$ is a fixed point of the $\mathbf{Z}/p\mathbf{Z}$-action on X if and only if $g_1,\ldots,g_p$ is of the form $(g,\ldots,g)$ and $g^p = e$. In other words, the map

$$g \longmapsto (g,\ldots,g)$$

identifies the set

$$\{g \in G \mid g^p = e\} = \{e\} \sqcup \{g \in G \mid |g| = p\}$$

with the set of fixed points

$$\mathrm{Fix}_{\mathbf{Z}p\mathbf{Z}}(X),$$

and the number of elements in the latter is, in view of Proposition 9.4, and a remark in the previous paragraph, divisible by p. □

9.3.3

A group G is said to be a *p-group* (for a prime p), if the order of every element $g \in G$ is a power of p.

Corollary 9.6 *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Exercise 136 *Prove Corollary 9.6.*

Exercise 137 *Prove that the center, $Z(G)$, of any finite p-group G is nontrivial, i.e., $Z(G) \neq \{e\}$. (Hint: consider the adjoint action of G.*

Exercise 138 *Let H be a proper subgroup of a finite p-group G. Prove that there exists an intermediate subgroup $H \subsetneq H' \subseteq G$ such that $H \lhd H'$. (Hint: consider the adjoint action of G.*

Exercise 138 leads to a number of facts about the structure of a finite p-group.

9.3.4 Maximal subgroups

A proper subgroup $M \subset G$ is said to be *maximal* if any M is not contained in any proper subgroup of G.

Exercise 139 *Let H be a subgroup of prime index in a group G. Show that H is maximal.*

Exercise 140 *Let H be a subgroup of index 2 in a group G. Show that H is normal.*

9.3.5 An example

Consider the group of permutations of a 3-element set, Σ_3. All of its proper subgroups are cyclic:

$$\langle(1\,2\,3)\rangle, \qquad \langle(1\,2)\rangle, \qquad \langle(2\,3)\rangle, \qquad \langle(3\,1)\rangle,$$

and of indices 3 and 2, respectively, hence maximal. All three subgroups of index 3 are conjugate to each other, therefore they are not normal.

Group Σ_3 has order $6 = 2 \cdot 3$ and thus is the smallest non-p-group. For, in a p-group all maximal subgroups are normal.

Corollary 9.7 *Any maximal subgroup M of a finite p-group is normal.* □

This is an immediate corollary of Exercise 138.

Lemma 9.8 *Let H be a subgroup of index greater than p in a p-group G. Then there exists an intermediate subgroup*

$$H \subsetneq H' \subsetneq G. \tag{229}$$

Proof. Let H' be a subgroup of G such that $H \lhd H'$. If H is not normal in G, then H' is the desired group.

If H is normal, then, in view of Cauchy's Theorem, there exists a cyclic subgrup C of order p in G/H. Let H' be a preimage of C in G under the canonical quotient map $\pi\colon G \longrightarrow G/H$, cf. 8.3.4. Its order is $|H|\,|C|$, cf. Exercise 115, and

$$|H'| = |H|\,|C| = |H| \cdot p < |H|\,|G/H|$$

since $|G/H| = |G : H| > p$ by hypothesis. □

As an immediate corollary, we obtain that any flag of subgroups in a group of order p can be extended to a maximal flag of subgroups of orders dividing the order of G:

$$1 < p < p^2 < \cdots .$$

Corollary 9.9 *Any flag of subgroups*

$$H_{p^{i_1}} \subset \cdots \subset H_{p^{i_r}} \tag{230}$$

in a p-group G of order p^n, where $H_{p^{i_k}}$ has order p^{i_k}, is contained in some maximal flag

$$1 \subset \cdots \subset H_{p^i} \subset \cdots \subset G \tag{231}$$

where H_{p^i} has order p^i, $i = 0, 1, \ldots, n$. □

9.4 p-subgroups of finite groups

9.4.1

Exercise 141 *a Let P be a p-subgroup of a group G. Show that p divides either the index of P in its normalizer,*

$$|N_G(P) : P|,$$

or the number of subgroups in G which are conjugate to P is congruent to 1 modulo p,

$$|\{{}^gP \mid g \in G\}| = 1 \mod p. \tag{232}$$

Hint: prove that

$$|G : P| = |N_G(P) : P| \mod p. \tag{233}$$

9.4.2

Definition 9.10 *A maximal p-subgroup P of a finite group G is called a* Sylow p-subgroup.

9.4.3

Let P be a Sylow p-subgroup and let $|P| = p^l$. If $|N_G(P) : P|$ were divisible by p, then the quotient group $N_G(P)/P$ would contain an element a of order p. This follows from Cauchy's Theorem, cf. 9.5.

In that case, $N_G(P)$ would contain a subgroup, P', containing P and of order p^{l+1}. Indeed, the preimage $\pi^{-1}(\langle a \rangle)$ under the canonical epimorphism

$$\pi \colon N_G(P) \twoheadrightarrow N_G(P)/P$$

would be such a group. That would contradict the maximality of P.

Thus, $|N(P) : P|$ is not divisible by p. By combining this with Exercise 141, we deduce that the number of conjugates of any Sylow p-subgroup equals 1 modulo p, cf. (232).

9.4.4

By combining the result of Section 9.4.3 with (233), we deduce that the index, $|G : P|$, is not divisible by p. In other words, the order of a maximal p-subgroup in G coicides with the maximum power p^e of p which divides $|G|$.

If we represent $|G|$ as the product of p^e and an integer m not divisible by p, then we obtain that the number of conjugates of a Sylow p-subgroup,

$$|G : N_G(P)|$$

divides

$$m = |G : P|.$$

.

9.4.5

Let Q be any p-subgroup. It acts on G/P by left multiplication. By combining the result of Section 9.4.3 with conguence (233) and Proposition 9.4, we deduce that

$$|\operatorname{Fix}_Q(G/P)| = 1 \mod p. \tag{234}$$

Thus, there exists $g \in G$ such that

$$Q \subseteq \operatorname{stab}_G(gP) = {}^{g}P,$$

cf. (215).

We arrive at the following fundamental result.

Theorem 9.11 *Let G be a group of order $p^e m$ where $p \nmid m$. Then:*

(i) Any p-group Q is contained in some Sylow p-subgroup P and all Sylow p-subgroups have order p^e.

(ii) Any two Sylow p-subgroups are conjugate.

(iii) The number of Sylow p-subgroups, $s_p(G)$, satisfies the following two constraints:

$$s_p(G) \mid m, \tag{235}$$

and

$$s_p(G) = 1 \mod p. \tag{236}$$

9.4.6

Assertions (i), (ii), and (iii), are usually called the *First*, the *Second*, and the *Third Sylow Theorems*.

Exercise 142 *Show that $N_G(N_G(P)) = N_G(P)$ for any Sylow p-subgroup $P \subseteq G$.*

9.4.7 Frattini's Argument (in its original form)

Exercise 143 *Let Q be a Sylow p-subgroup of a normal subgroup $H \lhd G$. Show that*

$$G = HN_G(Q). \tag{237}$$

Exercise 144 *Let P be a Sylow p-subgroup of G and $H \lhd G$ be a normal subgroup. Show that $P \cap H$ is a Sylow subgroup of H.*

9.5 Nilpotent groups

9.6

In Section 8.4 we introduced the class of sovable groups, $\mathscr{S}$, which is the smallest class closed under extensions which contains abelian groups. Now we shall discuss an important subclass $\mathscr{N} \subset \mathscr{S}$ of *nilpotent groups*.

9.6.1

Denote the class of abelian groups by $\mathscr{N}_0$. Groups that are *central* extensions of abelian groups will form the class $\mathscr{N}_1$. Groups that are central extensions of a group of class $\mathscr{N}_1$ will form the class $\mathscr{N}_2$, and so on: groups that are central extensions of a group of class $\mathscr{N}_l$ will form the class denoted $\mathscr{N}_{l+1}$.

Definition 9.12 *A group is said to be* nilpotent *(of level l) if it belongs to class $\mathscr{N}_l$.*

Exercise 145 *Show that, for any group G, the following two conditions are equivalent:*

(a) G is nilpotent of level 1;

(b) $[G,G] \subseteq Z(G)$.

9.6.2 Upper central series

For any group G, define inductively the sequence of subgroups

$$Z_0(G) := 1, \qquad \text{and} \qquad Z_{l+1}(G) := \{g \in G \mid [g,G] \subseteq Z_l(G)\}. \tag{238}$$

9.6.3

It follows directly from the definition that $Z_{l+1}(G)/Z_l(G)$ is contained in the center of $G/Z_l(G)$ and thus $G/Z_l(G)$ is a central extension of $G/Z_{l+1}(G)$ by $Z_{l+1}(G)/Z_l(G)$.

Accordingly, if $Z_{l+1}(G) = G$, then $G/Z_l(G)$ is abelian, i.e., nilpotent of level 0, $G/Z_{l-1}(G)$ is nilpotent of level 1, and so on. In particular, $G = G/Z_0(G)$ is nilpotent of level l.

Exercise 146 *Prove that, for any group G and $l \in \mathbf{N}$, one has*

$$Z_l(G/Z(G)) = Z_{l+1}/Z(G). \tag{239}$$

9.6.4 Lower central series

For any group G, define inductively the sequence of subgroups

$$L_0(G) := G, \qquad \text{and} \qquad L_{l+1}(G) := [L_l(G), G]. \tag{240}$$

9.6.5

It follows directly from the respective definitions that, for any group G, the following three conditions are equivalent:

(a) $Z_{l+1}(G) = G$;

(b) $L_{l+1}(G) = 1$;

(c) $[\ldots[,[g_0, g_1], g_2], \ldots, g_l] = 1$ for any $g_0, g_1, \ldots, g_l \in G$.

By combining this with 9.6.3 and with Exercise 146, we see that any of the above conditions characterizes groups nilpotent of level l.

9.6.6

Exercise 147 *Prove that for any proper subgroup $H \subset G$, one has*

$$N_G(H) \neq H. \tag{241}$$

.

9.6.7

Exercise 148 *Prove that every Sylow subgroup of a finite nilpotent group G is normal in G.*

9.6.8

Exercise 149 *Deduce from Exercise 9.6.7 that a finite group is nilpotent if and only if G is isomorphic to a product of p-groups.*

9.6.9 The Frattini subgroup

For any finite group G we define $\operatorname{Frat} G$ as the intersection of all of its *maximal* (proper) subgroups.

Exercise 150 *Let $G = \langle g \rangle$ be a cyclic group of order*

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

Prove that $\langle g^m \rangle$ is a maximal subgroup of G if and only if m is prime. Use this to prove that $\operatorname{Frat} G = \langle g^{p_1 \cdots p_r} \rangle$. In particular,

$$|\operatorname{Frat} G| = \tfrac{n}{p_1 \cdots p_r} = p_1^{e_1 - 1} \cdots p_r^{e_r - 1}.$$

It follows that $\operatorname{Frat} C_n = 1$ if and only if n is square-free.

Exercise 151 *Prove that* $\operatorname{Frat} G \lhd G$.

Exercise 152 *Prove that, for any subgroup* $H \subseteq G$, *if*

$$(\operatorname{Frat} G)H = G,$$

then

$$H = G.$$

9.6.10

In particular, a subset $X \cup \operatorname{Frat} G$ generates group G if and only if X alone generates G.

Exercise 153 *Prove that the Frattini subgroup of any finite group is nilpotent. (Hint. Prove that every Sylow subgroup of* $\operatorname{Frat} G$ *is normal in* G.*)*

10 Group structure

10.1 Semidirect products

10.1.1

Given an action of a group G on a group N, which is understood to be via automorphisms of N:

$$\varphi\colon G \longrightarrow \operatorname{Aut} N, \tag{242}$$

one can construct the so called *semidirect product* of G and N, denoted $N \rtimes_\varphi G$, which is set $N \times G$ equipped with the multiplication

$$(m, a)(n, b) := (m\varphi_a(n), ab). \tag{243}$$

10.1.2

Note that

$$^{(e,a)}(n, e) = (\varphi_a(n), e).$$

Thus, the action of G on N is realized in the semidirect product, $N \rtimes_\varphi G$, as conjugation of elements of $M \times 1$ by elements of $1 \times G$.

Exercise 154 *Prove that* (243) *is associative; find* $(n, a)^{-1}$.

Exercise 155 *Prove that if in a group* G *there is a normal subgroup* N *and a subgroup* H *such that*

$$G = NH \qquad \text{and} \qquad N \cap H = 1, \tag{244}$$

then G *is isomorphic to the semidirect product* $N \rtimes_{\varphi} H$ *for some* φ. *Find* φ.

In this case we speak of so called *(internal) semidirect product*.

10.1.3 Semidirect products and split extensions

Semidirect product, $N \rtimes_{\varphi} H$, determines a natural extension of H by N, cf. 8.3.8:

$$\begin{tikzcd} H & N \rtimes H \arrow[l, two heads, "p_2"'] & N \arrow[l, tail, "i_1"'] \end{tikzcd} \tag{245}$$

This extension is equipped with a canoical splitting:

$$i_2 \colon H \longrightarrow N \rtimes_{\varphi} H, \qquad h \longmapsto (e, h). \tag{246}$$

Exercise 156 *Prove that any split extension of* H *by* N *is isomorphic to the semidirect product extension,* (245), *for some* $\varphi \colon H \longrightarrow \operatorname{Aut} N$.

10.1.4 Isomorphisms of semidirect products

Let

$$f \colon N \rtimes_{\varphi} H \longrightarrow N' \rtimes_{\varphi'} H' \tag{247}$$

be a homomorphism of semidirect products such that

$$f(H) \subseteq H'$$

and

$$f \text{ identifies } N \text{ with } N'.$$

Denote the restriction of f to H by χ and consider it to be a homomorphism

$$\chi \colon H \longrightarrow H' \tag{248}$$

and, similarly, denote the restriction of f to N by ν and consider it to be an isomorphism

$$\nu \colon N \xrightarrow{\sim} N'. \tag{249}$$

Exercise 157 *Show that the following diagram is commutative*

$$\begin{tikzcd} H \arrow[r, "\varphi"] \arrow[d, "\chi"'] & \operatorname{Aut} N \arrow[d, "\mathrm{ad}_\nu"] \\ H' \arrow[r, "\varphi'"] & \operatorname{Aut} N' \end{tikzcd} \tag{250}$$

where ad_ν *is the isomorphism induced by* ν*:*

$$\mathrm{ad}_\nu\colon \alpha \longmapsto {}^{\nu}\alpha = \nu \circ \alpha \circ \nu^{-1} \qquad (\alpha \in \operatorname{Aut} N). \tag{251}$$

Vice-versa, show that a pair consisting of a homomorphism, (248)*, and an isomorphism,* (249)*, defines a homomorphism* (247) *by setting*

$$f(n,h) := (\nu(n), \chi(h)) \qquad (n \in N;\, h \in H) \tag{252}$$

if diagram (250) *is commutative.*

10.1.5

Above we described a certain class of homomorphisms between semidirect products. In particular, we described all isomorphisms between $N \rtimes_\varphi H$ and $N' \rtimes_{\varphi'} H'$ such that $f(N) = N'$ and $f(H) = H'$.

Exercise 158 *Suppose that any two cyclic subgroups of prime order* p *in* $\operatorname{Aut} N$ *are conjugate. Show that, for any nontrivial homomorphisms of a cyclic group,* C_p*, of order* p *into* $\operatorname{Aut} N$*,*

$$\varphi\colon C_p \longrightarrow \operatorname{Aut} N \qquad \textit{and} \qquad \varphi\colon C_p \longrightarrow \operatorname{Aut} N,$$

the corresponding semidirect products are isomorphic:

$$N \rtimes_\varphi H \simeq N \rtimes_{\varphi'} H.$$

10.1.6

An immediate corollary of Exercise 158 is that if a finite group G equals NC_p where N is normal in G and any two cyclic subgroups of $\operatorname{Aut} N$ of order p are conjugate, then G is either isomorphic to the product $N \times C_p$ (case when φ is trivial), or is a nontrivial semidirect product $N \rtimes C_p$, and all such semidirect products are isomorphic to each other.

10.2 The group of automorphisms of a group

10.2.1

In order to be able to take advantage of Sylow's Theorems in classification of finite groups of small order one needs to understand better the structure of the automorphism group Aut of some frequently encountered groups.

10.2.2 The case of an abelian group

The set of all endomorphisms, End A, of an abelian group $(A,+)$ forms a group under addition. The composition of endomorphisms is distributive with respect to addition, and thus End A is a ring with identity. Its group of invertible elements coincides with the group of automorphisms of A:

$$(\mathrm{End}\, A)^* = \mathrm{Aut}\, A. \tag{253}$$

10.2.3 The case of a cyclic group

In particular, for a cyclic group C_n of order

$$n = p_1^{m_1} \cdots p_r^{m_r},$$

one has a canonical isomorphism

$$\mathrm{End}\, C_n \simeq \mathbf{Z}/n\mathbf{Z}, \tag{254}$$

hence the canonical isomorphism

$$\mathrm{Aut}\, C_n \simeq (\mathbf{Z}/n\mathbf{Z})^* \tag{255}$$

To an element $l \in (\mathbf{Z}/n\mathbf{Z})^*$ corresponds an automorphism of C_n which sends any element $x \in C_n$ to x^l (we are using multiplicative

Since,

$$\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1^{m_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{m_r}\mathbf{Z},$$

one has the isomorphism

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/p_1^{m_1}\mathbf{Z})^* \times \cdots (\mathbf{Z}/p_r^{m_r}\mathbf{Z})^*,$$

i.e., the group of automorphisms of C_n is the product

$$\mathrm{Aut}\, C_n \simeq \mathrm{Aut}\, Cp_1^{m_1} \times \cdots \times \mathrm{Aut}\, Cp_r^{m_r}.$$

Theorem 10.1 *The group of automorphisms of the cyclic group of order p^m is cyclic,*

$$C_{(p-1)p^{m-1}} \simeq C_{p-1} \times C_{p^{m-1}}, \tag{256}$$

if p is odd, and isomorphic to

$$\{\pm 1\} \times C_{2^{m-2}} \tag{257}$$

when $p = 2$ and $m \geq 2$.

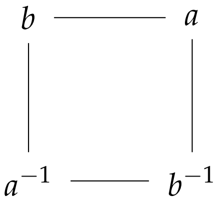
10.2.4

In the following exercises you are asked to determine $\operatorname{Aut} P$ for a few simplest 2-groups P. First, find the order of $\operatorname{Aut} P$, and then construct automorphisms of P which generate a subgroup in $\operatorname{Aut} P$ of the desired order.

Exercise 159 *Show that $\operatorname{Aut}(C_2 \times C_4)$ is the dihedral group, D_8, of order 8. (Hint: Find two elements of order 4 in $A = C_2 \times C_4$ such that*

$$X = \{a, b, a^{-1}, b^{-1}\}$$

is the set of all elements of order 4 in A. Show that the restriction to X of a nontrivial automorphism of A is a nontrivial permutation of X. This defines an embedding of $\operatorname{Aut} A$ into Σ_X. Show that any symmetry of the square



extends to an automorphism of A. Finally, find a permutation of X which does not extend to an automorphism. Deduce from this that $\operatorname{Aut} A \simeq D_8$.

Exercise 160 *Determine the structure of $\operatorname{Aut} D_8$. (Hint. Group D_8 has 5 elements of order 2: one element is central and the remaining four belong two conjugacy classes. 'Organize' those four elements into a square and show that the restriction of any automorphism of D_8 to the non-central elements of order 2* *defines an isomorphism of* $\operatorname{Aut} D_8$ *with the group of symmetries of that 'square'. The latter is isomorphic to* D_8 *but the canonical map*

$$\operatorname{ad}\colon D_8 \longrightarrow \operatorname{Aut} D_8 \tag{258}$$

is not an isomorphism. What is its kernel and its image?)

Exercise 161 *Find the order,* $|\operatorname{Aut} Q|$*, of the group of automorphisms of the quaternion group* Q*. (Hint. Determine the subgroup of* $\operatorname{Aut} Q$ *which consists of automorphisms that fix* i*, and then, for any element* q *of the set of elements of order 4 in* Q*,*

$$\{\pm i, \pm j, \pm k\},$$

construct an automorphism of Q *which sends* i *to* q*.)*

Exercise 162 *Prove that any group* G *of order 56 is either a (not necessarily nontrivial) semidirect product*

$$C_7 \rtimes P_2$$

of a cyclic group of order 7 and a 2-subgroup P_2 *of order 8, or is a nontrivial semidirect product*

$$C_2^3 \rtimes C_7$$

of an elementary abelian 2-group of rank 3 and a cyclic group of order 7.

11 The permutation and the alternating groups

11.1 Cyclic decomposition of a permutation

11.1.1 Support of a permutation

Let $\sigma \in \operatorname{Bij} X$ be a permutation of a set X. Its *support* is the set

$$\operatorname{supp} \sigma := \{x \in X \mid \sigma(x) \neq x\}. \tag{259}$$

Exercise 163 *Show that:*

$$\operatorname{supp}(\rho \circ \sigma) \subseteq \operatorname{supp} \rho \cup \operatorname{supp} \sigma \tag{260}$$

and

$$\operatorname{supp}(\sigma^{-1}) = \operatorname{supp} \sigma. \tag{261}$$

Deduce from this that the set of permutations with finite support

$$\Sigma_X := \{\sigma \in \operatorname{Bij} X \mid \operatorname{supp} \sigma \textit{ is finite}\} \tag{262}$$

is a normal subgroup of $\operatorname{Bij} X$*.*

11.1.2

It is clear that $\operatorname{supp}\sigma$ is the complement in X of the set of fixed points of the action of the cyclic group $\langle\sigma\rangle$ on X,

$$\operatorname{supp}\sigma = X \setminus \operatorname{Fix}_{\langle\sigma\rangle}(X).$$

In particular, the support is a $\langle\sigma\rangle$-invariant subset of X.

11.1.3 Cycles

A permutation λ of a set X is called a *cycle* of *length* l if $\operatorname{supp}\lambda$ is finite and consists of a single orbit group $\langle\lambda\rangle$,

$$\operatorname{supp}\lambda = \{x_j \mid j \in \mathbf{Z}/l\mathbf{Z}\} \quad \text{and} \quad \lambda(x_j) = x_{j+1}, \quad (j \in \mathbf{Z}/l\mathbf{Z}). \tag{263}$$

(Note that since we index elements of $\mathscr{O}$ by elements of ring $\mathbf{Z}/l\mathbf{Z}$ rather than by integers, $l+1=1$.)

11.1.4 Cycle notation

When dealing with cycles it is customary to employ a special notation

$$\lambda = (x_1 \ \ldots \ x_l) \tag{264}$$

(note the absence of commas).

11.1.5

Cycles of length l will be also called l-cycles. Their order equals l. Cycles of order 2 are called *transpositions*.

Exercise 164 *Suppose that set X has at least 4 distinct elements u, v, w, and x. Show that $(u\ v)(w\ x)$ and $(u\ v)(v\ w)$ can be expressed as products of 3-cycles.*

Exercise 165 *Suppose that set X has at least l distinct elements $x_1, \ldots, x_l$ where $l > 3$. Show that the 3-cycle, $(x_1\ x_2\ x_3)$ can be expressed as the product of 2 l-cycles.*

Exercise 166 *Suppose that set X has at least l distinct elements $x_1, \ldots, x_l$. Show that the l-cycle, $(x_1\ \ldots\ x_l)$ can be expressed as the product of $l-1$ transpositions.*

11.1.6

We say that two permutations ρ and σ are *disjoint* if

$$\operatorname{supp}\rho \cap \operatorname{supp}\sigma = \emptyset.$$

Exercise 167 *Show that disjoint permutations commute*

$$\rho\sigma = \sigma\rho.$$

Exercise 168 *Let λ be a cycle of length $l = mn$. Show that λ^m is the product of m (mutually) disjoint cycles of length n,*

$$\sigma^m = \lambda_1 \circ \cdots \circ \lambda_m.$$

Proposition 11.1 *Any permutation with finite support, $\sigma \in \Sigma_X$, is the product,*

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r, \tag{265}$$

of disjoint cycles.

Proof. Let

$$\operatorname{supp}\sigma = \mathscr{O}_1 \cup \cdots \cup \mathscr{O}_r \tag{266}$$

be the decomposition of the support of σ into the disjoint union of orbits of the $\langle\sigma\rangle$-action on X. For each orbit, $\mathscr{O}_i$, let

$$\mathscr{O}_i = \{x_{i1}, \ldots, x_{il_i}\}$$

where

$$\sigma(x_{ij}) = x_{i,j+1} \qquad (j \in \mathbf{Z}/l_i\mathbf{Z}).$$

Let

$$\lambda_i := (x_{i1} \; \ldots \; x_{il_i})$$

be the cycle of length $l_i = |\mathscr{O}_i|$ which cyclically permutes the elements of $\mathscr{O}_i$. Since the orbits $\mathscr{O}_i$ in (266) are disjoint, the corresponding cycles are mutually disjoint, and (265) holds. □

11.1.7

The decomposition of σ into a product of disjoint cycles is unique up to a rearrangement of terms in (265).

Indeed, for any such decomposition, (265), the support of each λ_i is an orbit, call it $\mathscr{O}_i$, of $\langle\sigma\rangle$ on X, and the action of σ on $\mathscr{O}_i$ determines λ_i. Thus, knowledge of decomposition of X into orbits of $\langle\sigma\rangle$-action, and the action of σ on each orbit, determine the decompostion of σ into a product of disjoint cycles uniquely up to the order in which one composes the cycles.

Exercise 169 *Let λ be any cycle of length l. Show that λ^m is a cycle, necessarily of length$l$, if m relatively prime to l.*

11.1.8

The list

$$(l_1, \dots, l_r) \tag{267}$$

is called the *cyclic type* of permutation σ. The order in (267) is unimportant. There are other ways to denote the cyclic type of a permutation, e.g., $2^3 3^2 7$, $2_3 3_2 7$, $2+2+2+3+3+7$, all can denote cyclic type

$$(2,2,2,3,3,7).$$

Exercise 170 *Show that the order of a permutation σ of (cyclic) type* (267) *is the least common multiple of numbers $l_1, \dots, l_r$,*

$$|\sigma| = \operatorname{lcm}(l_1, \dots, l_r).$$

11.1.9

Exercise 171 *Show that two permutations ρ and σ are conjugate to each other if and only if they have the same cyclic type.*

Exercise 172 *Show that for any $\sigma \in \Sigma_X$, its inverse, σ^{-1}, is conjugate to σ in Σ_X.*

11.1.10 Parity of a permutation

For a permutation σ of type (267), its *parity* is defined as

$$\tilde{\sigma} := (l_1 - 1) + \cdots + (l_r - 1) \mod 2. \tag{268}$$

It is an element of $\mathbf{Z}/2Z$. Permutations of parity 0 are called *even*, and those of parity 1 – are called *odd*. Parity is sometimes written multiplicatively as $+1$, for even, and -1, for odd permutations.

11.1.11

It follows from Exercise 166 that an even permutation can be expressed as a product of even number of transpositions, and an odd permutation can be expressed as a product of even number of transpositions.

Exercise 173 *Let $\tau = (x\ y)$ be a transposition, and σ be any permutation with finite support. Show that $\sigma \circ \tau$ has parity $\tilde{\sigma} + 1$. In other words, composition with a transposition reverses the parity. (Hint. Consider separately four cases:*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r, \qquad x \in \operatorname{supp} \lambda_1 \text{ and } y \in \operatorname{supp} \lambda_2, \tag{269}$$

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r, \qquad \{x, y\} \subseteq \operatorname{supp} \lambda_1, \tag{270}$$

$$\operatorname{supp} \sigma \cap \{x, y\} = \{x\}, \tag{271}$$

and

$$\operatorname{supp} \sigma \cap \{x, y\} = \emptyset.) \tag{272}$$

11.1.12

It follows from Exercise 173 and remark 11.1.11 that the product of m transpositions has parity m modulo 2.

Exercise 174 *Prove the above statement by induction on m.*

11.1.13 The alternating group A_X

Denote by A_X the set of all permutations

$$A_X := \{\sigma \in \Sigma_X \mid \tilde{\sigma} = 0\} \tag{273}$$

Exercise 175 *Show that A_X coincides with the set of permutations that can be expressed as a product of an even number of transpositions, and that all permutations that can be expressed as a product of an odd number of transpositions form a single coset of A_X in Σ_X. In particular, A_X is a subgroup of index 2 in Σ_X.*

Exercise 176 *Show that A_X is generated by 3-cycles.*

Exercise 177 *Show that*

$$[\Sigma_X, \Sigma_X] = A_X. \tag{274}$$

11.2 Combinatorics of permutations

11.2.1

For any element a of a group G, we shall denote by $\langle\langle a \rangle\rangle_G$, or by $\langle\langle a \rangle\rangle$ — if G is clear from the context, the smallest normal subgroup of G which contains a.

Exercise 178 *Show that $\langle\langle a \rangle\rangle$ coincides with the subgroup generated by the conjugacy class of a*

$$\langle\langle a \rangle\rangle = \left\langle {}^G a \right\rangle. \tag{275}$$

11.2.2

It follows from Proposition 11.1 combined with Exercise 166 that

$$\langle\langle \tau \rangle\rangle = \Sigma_X \tag{276}$$

for any transposition τ.

Exercise 179 *Show that*

$$\langle\langle \lambda \rangle\rangle = A_X \tag{277}$$

where λ is any 3-cycle. (Hint. Use Exercise 164.)

11.2.3

Suppose that $\sigma \in \Sigma_X$ is a product of disjoint cycles (265), and λ_1 has an *odd* length. The permutation,

$$\sigma' := \lambda_1 \circ \lambda_2^{-1} \circ \cdots \circ \lambda_r^{-1}$$

has the same cyclic type and thus is conjugate to σ. Note that

$$\sigma \circ \sigma' = \lambda_1^2$$

and since the order of λ_1 is odd, is a cycle of the same length. In view of Exercise 169, the subgroup $\langle\langle \sigma \rangle\rangle$ of Σ_X contains $\langle\langle \lambda \rangle\rangle$ where λ is a cycle of an odd length.

By combining this with Exercise 165, we deduce that

$$\langle\langle \lambda \rangle\rangle \subseteq \langle\langle \sigma \rangle\rangle \tag{278}$$

for some 3-cycle λ and, in view of (277),

$$A_X \subseteq \langle\langle \sigma \rangle\rangle. \tag{279}$$

.

11.2.4

Suppose that the order of $\sigma \in \Sigma_X$ equals $2^e m$ where $m > 1$ is odd. Then, σ^{2^e} having order m, is a product of disjoint cycles of odd length. By previous argument, 11.2.3,

$$A_X \subseteq \langle\langle \sigma^m \rangle\rangle \subseteq \langle\langle \sigma \rangle\rangle.$$

11.2.5

Suppose that the order of $\sigma \in \Sigma_X$ equals 2^e where $e > 0$. Then, $\sigma^{2^{e-1}}$ has order 2.

Exercise 180 *Show that a permutation $\sigma \in \Sigma_X$ of order 2 is a product of disjoint transpositions*

$$\sigma = \tau_1 \circ \cdots \circ \tau_r. \tag{280}$$

11.2.6

If σ is a single transposition then $\langle\langle\tau\rangle\rangle = \Sigma_X$, cf. (276). If σ is a product of at least 2 disjoint transpositions,

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r,$$

where $\tau_1 = (u\ v)$ and $\tau_2 = (w\ x)$, then

$$\sigma' = (u\ w)(v\ x) \circ \tau_3 \circ \cdots \circ \tau_r,$$

has the same cyclic type as σ and is thus conjugate to σ, and $\sigma \circ \sigma'$ is the product of 2 disjoint cycles,

$$\sigma \circ \sigma' = (u\ x)(v\ w).$$

11.2.7

If X has at least 5 elements, u, v, w, x, and y, then the subgroup $\langle\langle(u\ x)(v\ w)\rangle\rangle$ contains the 3-cycle

$$(u\ x)(v\ w) \circ (x\ y)(v\ w) = (u\ x\ y)$$

and hence contains $\langle\langle(u\ x\ y)\rangle\rangle = A_X$.

11.2.8

By combining everything together, we conclude that, for any non-identity permutation $\sigma \in \Sigma_X$, the smallest normal subgroup $\langle\langle\sigma\rangle\rangle$ which contains σ contains A_X – provided X has at least 5 elements. When $|X| = 4$ this is false: The subgroup

$$\langle\langle(u\ x)(v\ w)\rangle\rangle$$

in this case has order 4 and is normal in Σ_X and is strictly contained in A_X.

11.2.9

When σ is even, then $\langle\langle\sigma\rangle\rangle \subseteq A_X$, hence

$$\langle\langle\sigma\rangle\rangle = A_X \tag{281}$$

in this case.

11.2.10

When σ is odd, then $\sigma \notin A_X$, hence $\langle\!\langle \sigma \rangle\!\rangle$ is strictly bigger than A_X. Since $\Sigma_X : A_X| = 2$, Langrange's Theorem implies that

$$\langle\!\langle \sigma \rangle\!\rangle = \Sigma_X \tag{282}$$

in this case.

Thus we proved the following theorem.

Theorem 11.2 *For any set X of cardinality different from 4, the group of permutations withh finite support, Σ_X, has a unique nontrivial normal subgroup, namely A_X.*

11.2.11

The above theorem implies that no nontrivial normal subgroup H of A_X can be normal in Σ_X. Since $N_{\Sigma_X}(H) = A_X$ and $|\Sigma_X : A_X| = 2$, any such subgroup would have only 2 conjugacy classes in Σ_X,

$$H \qquad \text{and} \qquad {}^{\rho}H$$

where ρ is any odd permutation.

Below we shall demonstrate, however, that A_X has no nontrivial normal subgroups if X has at least 5 elements.

11.2.12

When h is an element of a subgroup H of G, then $\langle\!\langle h \rangle\!\rangle_H$ usually differs from $\langle\!\langle h \rangle\!\rangle_G$. For example,

$$\langle\!\langle (1\ 2) \rangle\!\rangle_{\Sigma_n} = \Sigma_n \qquad (n \geq 2).$$

The two subgroups coincide, however, when ${}^{H}h = {}^{G}h$. This happens often for elements of $H = A_X$ viewed as a subgroup in $G = \Sigma_X$.

Exercise 181 *Show that, for $\sigma \in A_X$,*

$${}^{A_X}\sigma = {}^{\Sigma_X}\sigma \tag{283}$$

if and only if there exists $\rho \in \Sigma_X \setminus A_X$ such that

$$\rho\sigma = \sigma\rho.$$

Exercise 182 *Show that* (283) *holds, for $\sigma \in A_X$, if*

$$\operatorname{supp}\sigma \neq X.$$

In particular,

$$\langle\langle\sigma\rangle\rangle_{A_X} = \langle\langle\sigma\rangle\rangle_{\Sigma_X} = A_X \tag{284}$$

in this case.

Exercise 183 *Show that* (283) *holds, for $\sigma \in A_X$, if σ is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r$$

with at least one cycle having even length. In particular, (284) *holds in this case as well.*

Exercise 184 *Show that* (283) *holds, for $\sigma \in A_X$, if σ is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r$$

with λ_1 and λ_2 being cycles of the same odd length l:

$$\lambda_1 = (u_1 \ \ldots \ u_l)$$

and

$$\lambda_2 = (v_1 \ \ldots \ v_l)$$

In particular, (284) *holds in this case as well.*

11.2.13

The above exercises demonstrate that the conjugacy classes in A_X and in Σ_X coincide for many even permutations. In particular, the normal subgroups they generate are all equal to A_X. For some even permutations however, ${}^{A_X}\sigma$ is indeed different from ${}^{\Sigma_X}\sigma$, and we need another method to show that $\langle\langle\sigma\rangle\rangle_{A_X} = A_X$ also in this case.

11.2.14

Suppose that $h \in H \subseteq G$, then

$$[a, h] = aha^{-1}h^{-1} \in \langle\langle h \rangle\rangle_H$$

for any a H. In particular,

$$\langle\langle [a, h] \rangle\rangle_H \subseteq \langle\langle h \rangle\rangle_H. \tag{285}$$

Exercise 185 *Calculate*

$$[(1\,2\,3), (1\ \ldots\ l)] \qquad (l \geq 2).$$

Use your calculation combined with remark 11.2.14 to show that (284) *holds if $\sigma \in A_X$ is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r$$

with at least one cycle having length greater or equal 4.

11.2.15

The above sequence of remarks and exercises shows that

$$\langle\langle \sigma \rangle\rangle_{A_X} = \langle\langle \sigma \rangle\rangle_{\Sigma_X} = A_X$$

for any even permutation $\sigma \neq \mathrm{id}_X$ in A_X.

We have proved the following important theorem.

Theorem 11.3 *The alternating group A_X has no nontrivial normal subgroups if set X has at least 5 elements.*

11.2.16

Note that A_X has non nontrivial normal subgroups also when X has fewer than 4 elements, so Theorem 11.3 excludes only the case $|X| = 4$. In that case A_X contains unique nontrivial normal subgroup, namely its Sylow 2-subgroup

$$\langle\langle \sigma \rangle\rangle_{A_X}$$

where σ is any element of order 2 in A_X.

11.3 Simple groups

11.3.1

Definition 11.4 *A simple group is a group with no nontrivial normal subgroups.*

11.3.2

An abelian simple group A has no nontrivial subgroups since every subgroup in an abelian group is normal. Such a group is cyclic of prime order. Indeed, if $g \in A \setminus 1 = \{a \in A \mid a \neq 1\}$ does not generate A, then $1 \neq \langle g \rangle \neq A$ is a nontrivial subgroup.

11.3.3

The center of a non-abelian simple group G is trivial

$$Z(G) = 1$$

and the commutator subgroup is the whole G

$$[G, G] = G. \tag{286}$$

Definition 11.5 *Groups satisfying* (286) *are called* perfect.

11.3.4

Since the kernel of any homomorphism $f \colon G \longrightarrow G'$ is normal, a nontrivial homomorphism from a simple group into any group is always injective.

11.3.5

Since $Z(P) \neq 1$ and $[P, P \neq P$ for any nonabelian p-group P, a p-group is simple if and only if it is cyclic of order p.

Exercise 186 *Show that any group of order* 42 *has a normal subgroup of order* 7.

Exercise 187 *Show that any group of order* 30 *has a normal subgroup of order* 3 *or* 5.

Theorem 11.6 *If a simple group G acts nontrivially on a set X of cardinality l, then $|G| \leq l!$.*

Proof. If G acts nontrivially on X, then there exists at least one element $x \in X$ which is not fixed by G. In this case, the G-action of G on the orbit, $\mathscr{O} = Gx$, of x defines a nontrivial homomorphism

$$G \longrightarrow \Sigma_{\mathscr{O}}.$$

By remark 11.3.4 this embeds G into the permutation group, $\Sigma_{\mathscr{O}}$. Thus, $|G| \leq |\Sigma_{\mathscr{O}}| = l!$. □

Corollary 11.7 *A simple group G of order less than $l!$ has no subgroup of index less or equal l.*

Proof. For any subgroup H of G the latter acts transitively on the set of left cosets G/H, cf. Exercise 126. If $H \neq G$, then G acts nontrivially on $X = G/H$ and the latter has cardinality $l = |G : H|$. □

11.3.6 Example: no group of order 24 is simple.

Sylow subgroups of a group G of order 24 have orders 8 and 3. The index in G of any Sylow 2-group is 3 and $3! = 6 < 24 = |G|$. By Corollary 11.7, G cannot be simple.

Exercise 188 *Show that no group of order 36 is simple.*

Theorem 11.8 *A simple group of order 60 has 5 Sylow 2-subgroups, and is canonically isomorphic to $A_{\mathrm{Syl}_2 G}$. In particular, there is only one simple group of order 60 up to an isomorphism.*

Proof. By the Third Sylow Theorem, the number $s_5(G) = |\mathrm{Syl}_5 G|$ divides $60/5 = 12$ and is congruent to 1 modulo 5. This leaves only two possibilities:

$$s_5(G) = 6 \quad \text{or} \quad 1.$$

In the case $s_5(G) = 1$, group G would have a normal subgroup of order 5, contradicting the simplicity hypothesis. Thus, $s_5(G) = 6$, and there are exactly $6 \cdot (5 - 1) = 24$ elements of order 5.

By the aforementioned Third Sylow Theorem, the number of Sylow 3-subgroups, $s_3(G)$, divides $60/3 = 20$ and is congruent to 1 modulo 3. This leaves only two possibilities:

$$s_3(G) = 10 \quad \text{or} \quad 1.$$

Again, $s_3(G) = 1$ would contradict the simplicity hypothesis. Thus, $s_3(G) = 10$, and there are exactly $10 \cdot (3-1) = 20$ elements of order 5.

All the elements of all the Sylow 2-subgroups are contained in the set

$$\{g \in G \mid g^3 \neq 1 \text{ and } g^5 \neq 1\}$$

which has $60 - (24 + 20 + 1) = 15$ elements.

The number off Sylow 2-subgroups, $s_2(G)$, divides $60/4 = 15$. If $s_2(G) = 3$, then G would act nontrivially on a set of cardinality 3, and $3! = 6 < 60 = |G|$. In view of Theorem 11.6 that is impossible.

If $s_2(G) = 15$, then at least two Sylow 2-subgroups, P and Q, must have a nontrivial element:

$$a \in P \cap Q.$$

Consider the centralizer, $C_G(a)$. Its order is divisible by $|P| = 4$ and greater or equal $|P \cup Q| = 6$. At the same time, is a divisor of $|G| = 60$. This leaves three possibilities:

$$12 = 3 \cdot 4, \qquad 20 = 5 \cdot 4, \qquad \text{or} \qquad 60 = 15 \cdot 4.$$

In the last case a would belong to the center of G and the center is trivial since G is obviously nonabelian.

In the second case, the index of $C_G(a)$ in G would be 3 and we know that G has no subgroups of order l such that $l! < |G|$.

The only possibility left is thus $|C_G(a)| = 5$.

The action of G on the set of left cosets, $X = G/C_G(a)$, then identifies G with a subgroup of index 2 in Σ_X, and there is only one such subgroup: A_X.

We proved that G is isomorphic to A_5. But this contradicts our assumption that $s_2(G) = 15$ since $s_2(A_5) = 5!$.

This proves that $s_2(G) = 5$ after all, and the transitive action of G on $\mathrm{Syl}_5(G)$ defines a canonical embedding of G onto $A_{\mathrm{Syl}_5(G)}$. □

11.3.7

It follows from Exercises 162, 186, 187, and 188, in combination with Section 11.3.6, that no nonabelian group of order less than 60 is simple. Thus, the alternating group on a 5-element set is the smallest nonabelian simple group.

11.3.8

The next nonabelian simple group has order 168. It is isomorphic to the group

$$\operatorname{Aut} C_3^2 = \mathrm{GL}_3(\mathbf{F}_2)$$

which is the group of collineations of the Fano plane: the smallest projective plane which has 7 points and 7 lines.

11.4 Linear groups

11.4.1 General linear group

Let F be a field. The group of automorphisms of the n-dimensional vector space F^n is identified with the group, $\mathrm{GL}_n(F)$, of invertible $n \times n$-matrices with entries in F: just associate to an automorphism its matrix in the standard basis of F^n. Group $\mathrm{GL}_n(F)$ is called the *general linear group* of F (of rank n).

11.4.2 General projective group

The center, $Z(\mathrm{GL}_n(F))$, consists of diagonal matrices

$$\begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \qquad (\lambda \in F^*) \tag{287}$$

where F^* denotes the multiplicative group of F. Note that $F^* = \mathrm{GL}_1(F)$.

The quotient by the center, $\mathrm{GL}_n(F)/Z(\mathrm{GL}_n(F))$, is called the *general projective group*. It is a subgroup of the group of all collineations of a projective $n-1$-dimensional space which is *coordinatized* by field F.

11.4.3 Special linear group

The general linear group is equipped with the canonical homomorphism

$$\det\colon \mathrm{GL}_n(F)\longrightarrow F^* \tag{288}$$

which is called the *determinant*. Its definition and properties are the subject of an introductory Linear Algebra course.

The kernel of (288) is denoted $\mathrm{SL}_n(F)$ and called the *special linear group*.

11.4.4 Special projective groups

The center of $\mathrm{SL}_n(F)$ consists of diagonal matrices (287) with λ being the roots of 1 of degree n. This group is always finite. In fact, it has no more than n elements since all such roots are zeros of the polynomial

$$X^n - 1$$

and any polynomial of degree n has at most n distinct roots.

The quotient by the center, $\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$, is called the *special projective group*.

11.4.5

Note that over a 2-element field $\mathbf{F}_2$, one has

$$\mathrm{GL}_n(F_2) = \mathrm{GL}_n(F_2) = \mathrm{SL}_n(\mathbf{F}_2) = textupPSL_n(\mathbf{F}_2).$$

Theorem 11.9 *With the exception of $textupPSL_2(\mathbf{F}_2)$ and $textupPSL_2(\mathbf{F}_3)$, which have orders 6 and 12, respectively, the special linear group of rank $n > 1$ of any field F, is simple.* □

12 Classification of groups of small order

12.1 Groups of order 12

12.1.1

Sylow subgroups of a group G of order $12 = 2^2 \cdot 3$ have orders 4 and 3. Sylow 2-subgroups are either cyclic, C_4, or elementary abelian, $C_2^2 = C_2{\times}C_2$.

12.1.2 Case I: G has a normal subgroup of order 3

In this case, G is a semidirect product of C_3 and its Sylow 2-subgroup P_2.

If $P_2 \lhd G$, then G is abelian and either is cyclic,

$$G \simeq C_3 \times C_4 \simeq C_{12},$$

or is isomorphic to the product of two cyclic groups,

$$G \simeq C_3 \times C_2 \times C_2 \simeq C_6 \times C_2.$$

Otherwise, the adjoint action of P_2 on $P_3 = C_3$ defines a nontrivial homomorphism

$$P_2 \longrightarrow \operatorname{Aut} C_3 = \{\pm 1\}. \tag{289}$$

12.1.3 Subcase: P_2 is elementary abelian

There is only one such homomorphism when $P_2 = C_4$. In this case,

$$G \simeq C_3 \rtimes C_4 = \langle a, b \mid a^4 = b^3 = aba^{-1}b = 1 \rangle \tag{290}$$

What you see on the righ-hand side of (290) is the often used in Group Theory notation giving a so called *presentation* of the group in terms of some set of generators (here, $\{a, b\}$), and defining relations (three in our case, $a^4 = 1$, $b^3 = 1$, and $aba^{-1} = b^{-1}$).

12.1.4 Subcase: P_2 is elementary abelian

When $P_2 = C_2^2$, there are three nontrivial homomorphisms (289): if $\{u, v, w\}$ denotes the set of elements of order 2 in C_2^2, then one element is sent to 1 and the remaining two are sent to -1. In either case,

$$G \simeq (C_3 \rtimes C_2) \times C_2 = \Sigma_3 \times C_2$$

where the factor C_2 is the subgroup of C_2^2 generated by the element of $\{u, v, w\}$ which acts trivially on C_3.

12.1.5 Case II: P_3 is not normal

In this case there are 4 cyclic subgroups of order 3, and 8 elements of order 3. This leaves room for only 3 elements $g \in G$ such that $g^3 \neq 1$. Since $P \setminus 1$, for any Sylow 2-subgroup has exactly 3 such elements, we conclude that there is only one Sylow 2-subgroup in G. In other words, $P_2 \lhd G$, and therefore

$$G = P_2 \rtimes C_3.$$

The adjoint action of C_3 on P_2 defines a nontrivial homomorphism

$$C_3 \longrightarrow \operatorname{Aut} P_2. \tag{291}$$

Since $\operatorname{Aut} C_4 = \{\pm 1\}$, there is no such homomorphism if P_2 is cyclic.

On the other hand, there are two such homomorphisms if P_2 is elementary abelian C_2^2, since $\operatorname{Aut} C_2^2 = \Sigma_X$ where X is the set of elements of order 2 in C_2^2. The corresponding semidirect products

$$C_2^2 \rtimes C_3$$

are isomorphic: this follows from Exercise 158. Thus, there is only one group, up to isomorphism, of order 12 without a normal subgroup of order 3.

Note that the action of G on the set, $\operatorname{Syl}_3 G$, of Sylow 3-subgroups defines a homomorphism

$$G \longrightarrow \Sigma_{\operatorname{Syl}_3 G}. \tag{292}$$

Let K denote its kernel and $\bar{G} \simeq G/K$ denote its image. Since $\bar{G}$ acts transitively on $\operatorname{Syl}_3 G$, number $4 = |\operatorname{Syl}_3 G|$ divides $|G|$ and the latter divides $12 = |G|$. This leaves only two possibilities for $|\bar{G}|$: either 4 or 12. In the former case, K would be a normal subgroup of order $12/4 = 3$, and that would contrardict the fact that G has no such subgroup. Thus, $|\bar{G}| = 12$ and $K = 1$. In other words, homomorphism (292) identifies G with a subgroup of $\Sigma_{\operatorname{Syl}_3 G}$ of index 2.

The permutation group, Σ_X, of a finite set X has only one subgroup of index 2, namely the alternating group A_X. Thus we proved that

a group of order 12 with no normal subgroup of order 3 is canonically isomorphic to $A_{\operatorname{Syl}_3 G}$. (293)

12.1.6

To sum up, there are exactly 5 groups of order 12 up to isomorphism, two of them are abelian, the rest are nonabelian:

$$C_3 \rtimes C_4, \qquad \Sigma_3 \times C_2 \qquad \text{and} \qquad A_4. \tag{294}$$

Exercise 189 *Show that $textupPSL_2(\mathbf{F}_3)$ is isomorphic to the alternating group, A_4. Provide two different proofs: one, group-theoretic, by finding a normal subgroup in $textupPSL_2(\mathbf{F}_3)$ of order 4, or by finding at least two different subgroups of order 3, and then using Case II of the above classification of groups of order 12; another one, using methods of elementary Linear Algebra, by proving that $textupPSL_2(\mathbf{F}_3)$ acts faithfully on the set of lines in the 2-dimensional vector space $\mathbf{F}_3^2$ which pass through the origin.*