5 Monoids and Groups

5.1 Operators and their properties

We consider a set V. A *binary operator on* V is a function of type $V \times V \to V$, so such a function maps pairs of elements of V to elements of V. Very often, applications of a binary operator are written in *infix-notation*, that is, the function's name is written *in between* the arguments.

In this chapter we use $*$ to denote any operator on a set V. Using infix-notation, we write the application of $*$ to pair $(x, y) \in V \times V$ as $x * y$ (instead of the more standard *prefix-notation* $*(x, y)$).

Sometimes binary operators have special properties, which deserve to be named.

5.1 Definition. Let $*$ be a binary operator on a set V. Then $*$ is called:

- *idempotent*, if for all $x \in V$ we have: $x * x = x$;
- *commutative*, if for all $x, y \in V$ we have: $x * y = y * x$;
- *associative*, if for all $x, y, z \in V$ we have: $(x * y) * z = x * (y * z)$;

□

5.2 Examples.

(a) On $\mathbb{N}$ addition, $+$, and multiplication, $*$, are binary operators; both are commutative and associative but not idempotent.

(b) On $\mathbb{Z}$ addition, $+$, and subtraction, $-$, are binary operators. Subtraction is neither idempotent, nor commutative, nor associative.

(c) On $\mathbb{Z}$ maximum, max, and minimum, min, are binary operators; both are idempotent, commutative, and associative.

(d) On the set of finite lists concatenation, $+\!\!+$, is a binary operator; it is neither idempotent nor commutative but it is associative.

(e) On the set of all relations relation composition, $;$, is an associative binary operator; as a special case, so is function composition, $\circ$, on the set of all functions.

□

For an associative operator $*$, the expressions $(x * y) * z$ and $x * (y * z)$ are equal and, therefore, we may safely omit the parentheses and write $x * y * z$ instead. Thus we do not only save a little writing, we also avoid the choice between two forms that are equivalent. Therefore, particularly with associative operators it pays to use infix-notation. With prefix-notation no parentheses can be omitted and we are always forced to decide whether to write $*(x, *(y, z))$ or $*(*(x, y), z)$: a rather irrelevant choice!

More important than the possibility to omit parentheses, however, is that associativity offers a *manipulative* opportunity in proofs: if we have a formula of the shape $(x * y) * z$ and if $*$ is associative then we may reposition the parentheses and obtain $x * (y * z)$ (and vice versa). So, even if we have omitted the parentheses we better stay aware of their (hidden) presence and of the opportunity to reposition them. We will see examples of this.

5.3 Definition. Let $*$ be a binary operator on a set V. An element $I \in V$ is called $*$'s *identity (element)* if it satisfies, for all $x \in V$:

$$x * I = x \ \wedge \ I * x = x \ .$$

□

Not every binary operator has an identity element but every operator has *at most one* identity element; that is, if it exists an operator's identity element is unique.

5.4 Lemma. Let I and J both be identity elements of binary operator $*$ on a set V. Then $I = J$.

Proof. By calculation:

$$\begin{array}{ll} & I \\ = & \quad \{\ J \text{ is identity element, with } x := I\ \} \\ & I * J \\ = & \quad \{\ I \text{ is identity element, with } x := J\ \} \\ & J \ . \end{array}$$

□

5.5 Examples.

(a) On $\mathbb{N}$ and $\mathbb{Z}$ the identity element of $+$ is 0, and the identity of $*$ is 1.

(b) On $\mathbb{N}^+$ operator $+$ has no identity element.

(c) On $\mathbb{Z}$ operator $-$ has no identity element.

(d) On $\mathbb{Z}$ operators max and min have no identity elements; on $\mathbb{N}$, however, the identity element of max is 0 whereas min still has no identity element.

(e) On the set of finite lists the identity element of $+\!\!+$ is $[\,]$ – the *empty* list –.

(f) The identity element of both relation composition and function composition is the identity relation/function, I.

□

Sometimes we are interested in the relation between two (or even more) binary operators. Although we do not elaborate this in this text, we mention one property that already has been used extensively in previous chapters.

5.6 Definition. Let $*$ and $+$ (say) be binary operators on a set V. Then we say that $*$ *distributes (from the left) over* $+$ if, for all $x, y, z \in V$:

$$x * (y + z) \;=\; (x * y) + (x * z) \quad .$$

Similarly, $*$ *distributes (from the right) over* $+$ if, for all $x, y, z \in V$:

$$(y + z) * x \;=\; (y * x) + (z * x) \quad .$$

Of course, if $*$ is commutative the distinction between "left" and "right" disappears and we just say "distributes over". (This is the case for almost all examples we have seen, with relation composition as the most notable exception.)
□

5.7 Examples.

(a) On $\mathbb{N}$ and $\mathbb{Z}$ multiplication, $*$, distributes over addition, $+$, but addition does not distribute over multiplication.

(b) On $\mathbb{Z}$ operator max distributes over min and min distributes over max.

(c) On $\mathbb{Z}$ operator $+$ distributes over both max and min.

(d) On $\mathbb{N}$ operator $*$ distributes over both max and min, whereas this is not true on $\mathbb{Z}$.

(e) Set union, $\cup$, distributes over set intersection, $\cap$, and vice versa.

(f) Relation composition, $;$, distributes, from the left and from the right, over union of relations, $\cup$. (Recall that composition is not commutative.)

□

5.2 Semigroups and monoids

So-called *algebraic structures* are sets with operators having particular properties. The simplest such structure is called a *semigroup*, which is just a set with an associative operator.

5.8 Definition. Let $*$ be a binary operator on a set V. The pair $(V, *)$ is a *semigroup* if $*$ is associative.
□

If the operator in a semigroup has an identity element the structure already becomes a little more interesting.

5.9 Definition. A *monoid* is a triple $(V, *, I)$, where $*$ is an associative binary operator on set V, so $(V, *)$ is a semigroup, and I, $I \in V$, is the identity element of $*$.
□

5.10 Examples.

(a) $(\mathbb{N}, +, 0)$ is a monoid, whereas $(\mathbb{N}^+, +)$ is a semigroup but not a monoid.

(b) both $(\mathbb{N}, *, 1)$ and $(\mathbb{N}^+, *, 1)$ are monoids.

(c) Let $\mathcal{L}_*$ denote the set of all finite lists, and let $\mathcal{L}_+$ denote the set of all non-empty finite lists. Then $(\mathcal{L}_*, +\!\!+, [\,])$ is a monoid, whereas $(\mathcal{L}_+, +\!\!+)$ only is a semigroup.

(d) All relations on a set with operator ; and identity relation I form a monoid. Similarly, all functions on a set, with function composition and the identity function form a monoid too.

□

5.11 Definition. Let $(V, *, I)$ be a monoid. For all $x \in V$ and for all $n \in \mathbb{N}$ we define x^n recursively, as follows:

$$x^0 = I \;\wedge\; x^{n+1} = x * x^n \quad .$$

□

5.12 Lemma. Let $(V, *, I)$ be a monoid. For every $x \in V$ and for all $m, n \in \mathbb{N}$ we have: $x^{m+n} = x^m * x^n$.

Proof. The proof of this lemma was already given in the proof of Lemma 1.31 in the chapter on relations. In fact Lemma 1.31 is a special case of the current lemma for the monoid consisting of all relations on a set U and the monoid operation ';'. Since the proof of Lemma 1.31 only uses the monoid properties (identity and associativity) of ';', the same proofs holds for arbitrary monoids. □

5.13 Definition. Let $(V, *, I)$ be a monoid. For every $x \in V$ an element $y \in V$ is called an *inverse* of x (with respect to $*$) if and only if: $x * y = I \;\wedge\; y * x = I$.
□

An element of a monoid does not necessarily have inverses, but if it has an inverse, it is unique. This is stated by the following lemma.

5.14 Lemma. Let $(V, *, I)$ be a monoid. Let $x, y, z \in V$ satisfy:

$$y * x = I \;\wedge\; x * z = I \quad .$$

Then $y = z$.

Proof. By calculation:

$$
\begin{array}{ll}
 & y \\
= & \quad \{\ I \text{ is identity of } *\ \} \\
 & y * I \\
= & \quad \{\ x * z = I\ \} \\
 & y * (x * z) \\
= & \quad \{\ *\ \text{is associative}\ \} \\
 & (y * x) * z \\
= & \quad \{\ y * x = I\ \} \\
 & I * z \\
= & \quad \{\ I \text{ is identity of } *\ \} \\
 & z \quad .
\end{array}
$$

□

Notice that in the proof of this lemma we have only used $x * z = I\ -z$ is a *right-inverse* of $x-$ and $y * x = I\ -y$ is a *left-inverse* of $x-$, so, actually, we have proved that all left-inverses are equal to all right-inverses.

5.3 Groups

Algebraically, life becomes really interesting with *groups*. A group is a monoid in which every element has an inverse (with respect to the binary operator).

5.15 Definition. A *group* is a monoid $(V, *, I)$ satisfying, for all $x \in V$:

(3) $\qquad (\exists y : y \in V : x * y = I \wedge y * x = I)$.

An *Abelian group* is a group in which, in addition, operator $*$ is commutative.
□

As a matter of fact requirement (3) is stronger than strictly necessary: either of the two conjuncts, $x * y = I$ or $y * x = I$, can be dropped without affecting the definition. It is only for practical reasons, and because we do not wish to destroy the symmetry, that we have included both.

5.16 Lemma. Let $(V, *, I)$ be a monoid satisfying, for all $x \in V$:

(4) $\qquad (\exists y : y \in V : x * y = I)$.

Then $(V, *, I)$ is a group.

Proof. To prove that $(V, *, I)$ is a group we must prove (3) for all $x \in V$, while using (4) for all $x \in V$. So, let $x \in V$ and let, using (4), element $y \in V$ satisfy $x * y = I$. Now to prove (3) for this particular x it suffices to show that y also satisfies $y * x = I$. Let, using (4) once more but with $x := y$, element $z \in V$ satisfy $y * z = I$. Now we calculate:

$$
\begin{aligned}
& x \\
= & \qquad \{\ I \text{ is identity of } *\ \} \\
& x * I \\
= & \qquad \{\ y * z = I\ \} \\
& x * (y * z) \\
= & \qquad \{\ *\ \text{is associative}\ \} \\
& (x * y) * z \\
= & \qquad \{\ x * y = I\ \} \\
& I * z \\
= & \qquad \{\ I \text{ is identity of } *\ \} \\
& z \quad .
\end{aligned}
$$

So, we have $x = z$; now z satisfies $y * z = I$, and substituting x for z in this we obtain $y * x = I$, as required.
□

The definition of groups states that every element of the set has an inverse. From Lemma 5.14 we already know that, if an element has an inverse, this inverse is unique. The inverse of an element, of course, depends on that element. Therefore, from now onwards we denote the inverse of every element $x \in V$ by x^{-1}.

5.17 Definition. Let $(V, *, I)$ be a group. For every $x \in V$ its inverse, x^{-1}, satisfies:

$$x * x^{-1} = I \ \wedge \ x^{-1} * x = I \quad .$$

□

In the proof of Lemma 5.16 we have introduced y as the inverse of x, and z as the inverse of y, and then we have proved $z = x$. So, as an additional result, we obtain the following lemma stating that the inverse of the inverse of an element is that element itself.

5.18 Lemma. Let $(V, *, I)$ be a group. Every $x \in V$ satisfies: $(x^{-1})^{-1} = x$.

□

5.19 Lemma. Let $(V, *, I)$ be a group. All $x, y \in V$ satisfy: $(x * y)^{-1} = y^{-1} * x^{-1}$.

Proof. Using associativity several times we obtain

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * I * x^{-1} = x * x^{-1} = I$$

and

$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * I * y = y^{-1} * y = I,$$

so $y^{-1} * x^{-1}$ is the inverse of $x * y$. □

5.20 Examples.

(a) Let $V = \{\,\mathsf{i}\,\}$ and let binary operator $*$ on V be defined by $\mathsf{i} * \mathsf{i} = \mathsf{i}$. Then $(V, *, \mathsf{i})$ is a group; this is the *smallest possible* group.

(b) $(\,\mathbb{Z}\,, +\,, 0\,)$ is an (Abelian) group.

(c) $(\,\mathbb{Q}^+\,, *\,, 1\,)$ and $(\,\mathbb{Q}\backslash\{\,0\,\}\,, *\,, 1\,)$ are (Abelian) groups.

(d) For any set V we consider the set of all *bijections* from V to V, here denoted by $V \leftrightarrow V$. Then $(\,(V \leftrightarrow V)\,, \circ\,, I\,)$ is a group; it is not Abelian. If V is *finite* the bijections in $V \leftrightarrow V$ are also called *permutations* and the group is called a *permutation group*.

(e) For a fixed positive natural number n we define operator $\oplus$, of type $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, by $x \oplus y = (x+y) \bmod n$, for all $x, y \in \mathbb{Z}$. Then this operator also has type $[\,0\,..\,n\,) \times [\,0\,..\,n\,) \to [\,0\,..\,n\,)$, and $(\,[\,0\,..\,n\,)\,, \oplus\,, 0\,)$ is an Abelian group.

□

A group $(V, *, I)$ has the property that, for all $a, b \in V$, equations of the shape $x : a * x = b$ can be solved. The solution of such an equation even is unique:

$$
\begin{array}{ll}
 & a * x \;=\; b \\
\Rightarrow & \qquad \{\ \text{Leibniz}\ \} \\
 & a^{-1} * (a * x) \;=\; a^{-1} * b \\
\Leftrightarrow & \qquad \{\ *\ \text{is associative}\ \} \\
 & (a^{-1} * a) * x \;=\; a^{-1} * b \\
\Leftrightarrow & \qquad \{\ a^{-1}\ \text{is}\ a\text{'s inverse}\ \} \\
 & I * x \;=\; a^{-1} * b \\
\Leftrightarrow & \qquad \{\ I\ \text{is identity of}\ *\ \} \\
 & x \;=\; a^{-1} * b \quad ,
\end{array}
$$

which shows that every solution to the equation is equal to $a^{-1} * b$. Conversely, it also is easy to show that $a^{-1} * b$ is a solution indeed, because $a * (a^{-1} * b)$ is, indeed, equal to b.

This is the characteristic property of groups: a group is the simplest possible structure in which all equations of the shape $x : a * x = b$ can be solved.

5.21 Lemma. Let $(V, *, I)$ be a group. For all $x \in V$ and $n \in \mathbb{N}$ we have:

$$(x^{-1})^n \;=\; (x^n)^{-1}$$

Proof. We have to prove that $(x^{-1})^n * x^n = I = x^n * (x^{-1})^n$, for all n. We do this by induction on n.

For $n = 0$ this holds since $(x^{-1})^0 = I = x^0$. For the induction step assume the induction hypothesis $(x^{-1})^n * x^n = I = x^n * (x^{-1})^n$. Leaving associativity implicit, we obtain:

$$\begin{array}{rcll} (x^{-1})^{n+1} * x^{n+1} & = & (x^{-1})^n * x^{-1} * x * x^n & \text{(definition, Lemma 5.12)} \\ & = & (x^{-1})^n * I * x^n & \\ & = & (x^{-1})^n * x^n & \\ & = & I & \text{(induction hypothesis)} \end{array}$$

and

$$\begin{array}{rcll} x^{n+1} * (x^{-1})^{n+1} & = & x^n * x * x^{-1} * (x^{-1})^n & \text{(definition, Lemma 5.12)} \\ & = & x^n * I * (x^{-1})^n & \\ & = & x^n * (x^{-1})^n & \\ & = & I & \text{(induction hypothesis).} \end{array}$$

□

5.22 Definition. Let $(V, *, I)$ be a group. For all $x \in V$ and $n \in \mathbb{N}$ we define x^{-n} by:

$$x^{-n} = (x^{-1})^n$$

□

5.23 Lemma. Let $(V, *, I)$ be a group. For every $x \in V$ and for all $m, n \in \mathbb{Z}$ we have:

$$x^{m+n} = x^m * x^n$$

Proof. We give the proof by case analysis.

- If $m \geq 0$ and $n \geq 0$ the lemma coincides with Lemma 5.12.
- If $m \leq 0$ and $n \leq 0$ write $m' = -m \geq 0$ and $n' = -n \geq 0$, we obtain:

$$\begin{array}{rcll} x^{m+n} & = & x^{-(m'+n')} & \\ & = & (x^{m'+n'})^{-1} & \text{(Lemma 5.21)} \\ & = & (x^{n'} * x^{m'})^{-1} & \text{(Lemma 5.12)} \\ & = & (x^{m'})^{-1} * (x^{n'})^{-1} & \text{(Lemma 5.19)} \\ & = & x^{-m'} * x^{-n'} & \text{(Lemma 5.21)} \\ & = & x^m * x^n. & \end{array}$$

- If $m \geq 0$ and $n < 0$ we apply induction on m. For $m = 0$ it was already proved in the former case. The induction step proceeds as follows. In case $n = -1$ we obtain $x^{(m+1)+n} = x^m = x^m * I = x^m * x^{n+1}$, in case $n < -1$ then by the induction hypothesis we also obtain $x^{(m+1)+n} = x^{m+(n+1)} = x^m * x^{n+1}$. So writing $n' = -n > 0$ we derive

$$\begin{array}{rcll} x^{(m+1)+n} & = & x^m * x^{n+1} & \text{(just derived)} \\ & = & x^m * x^{1-n'} & \\ & = & x^m * (x^{-1})^{n'-1} & \text{(Lemma 5.21)} \\ & = & x^m * x * x^{-1} * (x^{-1})^{n'-1} & (x * x^{-1} = I) \\ & = & x^{m+1} * (x^{-1})^{n'} & \\ & = & x^{m+1} * x^{-n'} & \text{(Lemma 5.21)} \\ & = & x^{m+1} * x^n. & \end{array}$$

- If $m < 0$ and $n > 0$ we have $x^{-m-n} = x^{-n} * x^{-m}$ by the former case, yielding

$$\begin{array}{rcll} x^{m+n} & = & ((x^{m+n})^{-1})^{-1} & \text{(Lemma 5.18)} \\ & = & (x^{-m-n})^{-1} & \text{(Lemma 5.21)} \\ & = & (x^{-n} * x^{-m})^{-1} & \text{(observed above)} \\ & = & (x^{-m})^{-1} * (x^{-n})^{-1} & \text{(Lemma 5.19)} \\ & = & x^m * x^n & \text{(Lemma 5.21).} \end{array}$$

□

5.4 Subgroups

5.24 Definition. Let $(V, *, I)$ be a group and let U be a subset of V. If $(U, *, I)$ is a group this is called a *subgroup* of $(V, *, I)$.
□

To verify that $(U, *, I)$ is a subgroup we do not have to verify that $*$ is associative, that I is the identity element, and that group elements have inverses: these properties remain valid. But, we do have to verify that subset U is *closed* under the group operations, that is, to prove that $(U, *, I)$ is a subgroup we must prove the following three properties:

$(\forall x, y : x, y \in U : x * y \in U)$, and:

$I \in U$, and:

$(\forall x : x \in U : x^{-1} \in U)$.

5.25 Examples.

(a) In $(\mathbb{Z}, +, 0)$ the subset of the *even* integers, with $+$ and 0, form a subgroup. More generally, for any natural number n the subset of all *multiples of* n, with $+$ and 0, form a subgroup.

(b) $(\mathbb{Q}^+, *, 1)$ is a subgroup of $(\mathbb{Q}\backslash\{0\}, *, 1)$.

(c) For any group $(V, *, I)$ and for any fixed $a \in V$ we can define a subset U by $U = \{a^i \mid i \in \mathbb{Z}\}$. Then $(U, *, I)$ is a subgroup of $(V, *, I)$, called the subgroup *generated by* a.

(d) Actually, in $(\mathbb{Z}, +, 0)$ the subgroup of all multiples of n, for some natural n, is the subgroup generated by n.

□

5.26 Definition. A group $(V, *, I)$ is called *cyclic* if V contains an element a, say, such that the subgroup generated by a is the whole group, that is, $\{a^i \mid i \in \mathbb{Z}\} = V$.
□

5.27 Definition. A group $(V, *, I)$ is finite if its set V of elements is finite. For a finite group $(V, *, I)$ the *order* of the group $(V, *, I)$ is $\#V$.
□

5.28 Examples.

(a) Let group $(V, *, I)$ be finite of order N and let this group be cyclic. Then V contains an element a, say, such that $V = \{ a^i \mid 0 \leq i < N \}$ and $a^N = I$.

(b) For positive natural n, the group $([0\,..\,n), \oplus, 0)$, with $\oplus$ as defined in Example 5.20 (e), has order n. This group is cyclic, as it is generated by 1.

□

5.5 Cosets and Lagrange's Theorem

5.29 Definition. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. Then for every $a \in V$ the *left coset* of a is the subset $\{ a * y \mid y \in U \}$ and the *right coset* of a is the subset $\{ x * a \mid x \in U \}$. The left and right cosets of a are denoted by $a * U$ and $U * a$, respectively.
□

Notice that U is a (left and right) coset too, because $I * U = U$ and $U * I = U$.

If $(V, *, I)$ is a group with subgroup $(U, *, I)$ and for fixed $a \in V$, we can define a function $\varphi : U \to V$ by $\varphi(x) = a * x$, for all $x \in U$. Then, the left coset $a * U$ just is the image of U under function φ, that is, in terms of lifted functions, we have $a * U = \varphi(U)$.

5.30 Lemma. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. For fixed $a \in V$ the function $\varphi : U \to a * U$, defined by $\varphi(x) = a * x$, for all $x \in U$, is bijective.

Proof. Because $a * U = \varphi(U)$ function φ is surjective. That φ is injective as well follows from, for all $x, y \in U$:

$$
\begin{array}{ll}
 & \varphi(x) = \varphi(y) \\
\Leftrightarrow & \quad \{ \text{ definition of } \varphi \ \} \\
 & a * x = a * y \\
\Rightarrow & \quad \{ \text{ Leibniz } \} \\
 & a^{-1} * (a * x) = a^{-1} * (a * y) \\
\Leftrightarrow & \quad \{ \ * \text{ is associative; definition of inverse; identity element } \} \\
 & x = y \quad .
\end{array}
$$

□

All subsets of a finite set are finite as well. Therefore, in a finite group $(V, *, I)$ every subgroup $(U, *, I)$ is finite too, and so are all (left and right) cosets of this subgroup. In this case we arrive at an important consequence of the above lemma.

Corollary: In a finite group $(V, *, I)$ with subgroup $(U, *, I)$ we have, for all $a \in V$, that $\#(a*U) = \#U$ and $\#(U*a) = \#U$. In words: in a finite group with a subgroup all cosets have the same size as the subgroup from which they are derived.

□

Because $I \in U$ we have $a \in a*U$, for all $a \in V$. For $a, b \in V$ one may well wonder how the cosets $a*U$ and $b*U$ are related. By careful analysis we can derive that these cosets either are disjoint or are the same, and it so happens that $a*U = b*U$ if and only if $a^{-1}*b \in U$. This gives rise to the following lemma.

5.31 Lemma. Let $(V, *, I)$ be a group and let $(U, *, I)$ be a subgroup. On V we define a relation $\sim$ by, for all $a, b \in V$: $a \sim b \Leftrightarrow a^{-1}*b \in U$. Then:

(a) $\sim$ is an equivalence relation;

(b) The left cosets $a*U$, for all $a \in V$, are the equivalence classes of $\sim$.

Proof. First we prove that $\sim$ is a equivalence relation:

- reflexive: for $a \in V$ we have $a^{-1}*a = I \in U$, so $a \sim a$.
- symmetric: for $a, b \in V$ satisfying $a \sim b$ we have $a^{-1}*b \in U$, so $b^{-1}*a = (a^{-1}*b)^{-1} \in U$, so $b \sim a$.
- transitive: for $a, b, c \in V$ satisfying $a \sim b$ and $b \sim c$ we have $a^{-1}*b \in U$ and $b^{-1}*c \in U$, so

$$a^{-1}*c = a^{-1}*I*c = a^{-1}*(b*b^{-1})*c = (a^{-1}*b)*(b^{-1}*c) \in U,$$

so $a \sim c$.

Next we derive

$$\begin{array}{rcl} x \in a*U & \Leftrightarrow & (\exists u \in U : x = a*u) \\ & \Leftrightarrow & (\exists u \in U : a^{-1}*x = u) \\ & \Leftrightarrow & a^{-1}*x \in U \\ & \Leftrightarrow & a \sim x \\ & \Leftrightarrow & x \in [a], \end{array}$$

so $[a] = a*U$, proving (b). □

Now we are ready for our final theorem, which is due to the famous mathematician Joseph Louis Lagrange.

5.32 Theorem. [**Lagrange**] The order of every subgroup of a finite group is a divisor of the order of the whole group.

Proof. Let M be the order of the group and let N be the order of the subgroup. The equivalence classes of relation $\sim$, as defined in Lemma 5.31, form a partitioning of

V. Each of these classes – the left cosets – has size N, and because V is finite there are only finitely many such cosets: let K be the number of left cosets. Because these sets are mutually disjoint and because their union equals V we have $M = K * N$, hence N is a divisor of M.
□

5.6 Permutation Groups

5.6.1 Function restriction and extension

In this section we will be studying functions on intervals of the shape $[0..n)$, for positive naturals n. If f is a function on the interval $[0..n)$, then we wish to speak of the *restriction of* f to the interval $[0..m)$, for any naturals $m, n : 1 \leq m \leq n$; this is a function with domain $[0..m)$, and on this domain it has the same values as f. We denote this restriction as $f\lceil m$ – "f take m" –.

5.33 Definition. For function f on $[0..n)$ and for m with $1 \leq m \leq n$ the function $f\lceil m$, on $[0..m)$, is defined by:

$$(f\lceil m)(i) = f(i) \quad \text{, for all } i : 0 \leq i < m \quad .$$

□

Property: If f, on $[0..n)$, is injective then so is $f\lceil m$, for all $m, n : 1 \leq m \leq n$.
□

* * *

As a converse to function restriction we also have need of the possibility of *function extension*. If f is a function on $[0..n)$ then we wish to define a new function, on $[0..n+1)$, that coincides with f on $[0..n)$ and for which the value in n equals a pre-specified value v, say. We denote this function as $f \lhd v$ – "f snoc v" –.

5.34 Definition. For function f on $[0..n)$ and for any value v, the function $f \lhd v$, on $[0..n+1)$, is defined by:

$$(f \lhd v)(i) = f(i) \quad \text{, for all } i : 0 \leq i < n$$
$$(f \lhd v)(n) = v$$

□

5.35 Lemma. Function f, on $[0..n+1)$, satisfies:

$$f = (f\lceil n) \lhd f(n) \quad ,$$

and function f, on $[0..n)$, and value v satisfy:

$$(f \lhd v)\lceil n = f \quad .$$

□

5.6.2 Continued Compositions

For any finite list fs of functions, all of the same type $V \to V$, we define the *continued composition* of (the functions in) list fs. Informally, if list fs has length k then the continued composition of fs is:

$$fs_0 \circ fs_1 \circ \cdots \circ fs_{k-1} \quad .$$

Formally, the continued composition of (finite) lists of functions can be defined as a function $\mathcal{C}$, say, such that $\mathcal{C}(fs)$ is the composition of the functions in fs. Function $\mathcal{C}$ can be defined recursively as follows, for all lists fs, gs of functions and for function f, all of type $V \to V$.

5.36 Definition.

$$\begin{array}{lll} & \mathcal{C}([\,]) & = \; I_V \\ & \mathcal{C}([f\,]) & = \; f \\ (5) & \mathcal{C}(fs +\!\!+ gs) & = \; \mathcal{C}(fs) \circ \mathcal{C}(gs) \quad . \end{array}$$

□

Notice that we have defined $\mathcal{C}([\,]) = I_V$ here because I_V is the identity element of function composition: thus, we guarantee that rule (5) also holds if either fs or gs equals $[\,]$. Also notice that rule (5) is ambiguous: the decomposition of a list of functions as a concatenation $fs +\!\!+ gs$ of two lists fs and gs of functions is not unique, but, fortunately, this is harmless, because of the associativity of function composition: the result will be the same, independently of this decomposition. As a matter of fact, *lists* are the appropriate data structure here, because of this associativity and because function composition is *not* commutative.

5.6.3 Bijections

We recall that a *bijection* on a set V is a function in $V \to V$ that is both *injective* and *surjective*. Informally, this means that, for every $v \in V$, there is *exactly one* $u \in V$ satisfying $f(u) = v$: that f is injective means that, for every v, there is *at most one* such u, and that f is surjective means that, for every v, there is *at least one* such u. For any given set V, the bijections on V have the following properties:

- The identity function I_V is a bijection on V;
- If f and g are bijections on V then so is their composition $f \circ g$;
- If f is a bijection on V, then f has an inverse, f^{-1}, and f^{-1} is a bijection on V too.

From this we conclude that the bijections on V, with $\circ$ and I, form a group.

5.6.4 Permutations

For *finite* set V the bijections on V are also called *permutations of* V. In what follows we will restrict our attention to finite sets of a very particular shape, namely, initial segments of the natural numbers. That is, we consider nonempty intervals of the shape $[\,0\,..\,n\,)$, for $n : 1 \leq n$. In this section we denote the identity permutation on $[\,0\,..\,n\,)$ as I_n. Notice that there is only *one* permutation of $[\,0\,..\,1\,)$, namely I_1.

* * *

We will use $\mathcal{P}_n$ to denote the set of all permutations of $[\,0\,..\,n\,)$, for $n : 1 \leq n$. So, $\mathcal{P}_n$ is the subset of those functions in $[\,0\,..\,n\,) \to [\,0\,..\,n\,)$ that are bijections. In what follows, the requirement $1 \leq n$ is left implicit. Hence, as permutations are bijections, we now have that $(\mathcal{P}_n\,, \circ\,, I_n)$ is a group, for every n.

* * *

Every permutation in $\mathcal{P}_n$ can be represented compactly by enumerating its values in a list of length n. That is, if $s \in \mathcal{P}_n$ then it is represented by the list $[\,s_0, s_1, \cdots, s_{n-2}, s_{n-1}\,]$. Notice that, because every permutation is a bijection, this list contains each of the naturals $i : 0 \leq i < n$ exactly once. For example $[\,0, 1, 2, 3\,]$ is the identity permutation of $[\,0\,..\,4\,)$, and $[\,3, 0, 1, 2\,]$ is the permutation that "rotates the elements of $[\,0\,..\,4\,)$ one place to the left".

If $s \in \mathcal{P}_{n+1}$ then s is a permutation of $[\,0\,..\,n{+}1\,)$; so, s is injective and, therefore, $s \lceil n$ also is injective on $[\,0\,..\,n\,)$. Function s also is surjective and if, in addition, $s_n = n$, then $s \lceil n$ also is surjective in $[\,0\,..\,n\,) \to [\,0\,..\,n\,)$. Hence, if (and only if) $s_n = n$ then $s \lceil n$ is a permutation in $\mathcal{P}_n$ as well. This is expressed by the following lemma.

5.37 Lemma. $(\forall s : s \in \mathcal{P}_{n+1} : s_n = n \Rightarrow s \lceil n \in \mathcal{P}_n\,)$.

□

Conversely, every permutation in $\mathcal{P}_n$ can be extended to a permutation in $\mathcal{P}_{n+1}$ in a simple way, namely by extending the function with value n.

5.38 Lemma. $(\forall s : s \in \mathcal{P}_n : s \lhd n \in \mathcal{P}_{n+1}\,)$.

□

corollary: As a result of these lemmas and of Lemma (5.35) we have:

$$(\forall s : s \in \mathcal{P}_{n+1} : s_n = n \Rightarrow s = (s \lceil n) \lhd n\,) \quad ,$$

and:

$$(\forall s : s \in \mathcal{P}_n : s = (s \lhd n) \lceil n\,) \quad .$$

□

This shows that the subset of those permutations in $\mathcal{P}_{n+1}$ that map n to n is *isomorphic* to $\mathcal{P}_n$: the functions $(\lceil n)$ and $(\lhd n)$ are the bijections from that subset to $\mathcal{P}_n$ and back, respectively.

In what follows, therefore, we will identify the subset of the permutations in $\mathcal{P}_{n+1}$ that map n to n and $\mathcal{P}_n$, that is, we will leave the application of the bijections implicit. Thus, for every permutation $s \in \mathcal{P}_{n+1}$ with $s_n = n$ will also say that $s \in \mathcal{P}_n$ and, conversely, we consider every permutation in $\mathcal{P}_n$ to be a permutation in $\mathcal{P}_{n+1}$ as well.

5.6.5 Swaps

For $p, q \in [\,0\,..\,n\,)$ we define the permutation $p \leftrightarrow q$ – "p swap q" – as follows:

$$\begin{array}{lcl} (p \leftrightarrow q)(p) & = & q \quad , \\ (p \leftrightarrow q)(q) & = & p \quad , \\ (p \leftrightarrow q)(i) & = & i \quad , \text{ for all } i : i \in [\,0\,..\,n\,) \wedge i \neq p \wedge i \neq q \quad . \end{array}$$

So, $p \leftrightarrow q$ is the permutation that interchanges p and q and leaves everything else in place. Obviously, if $p = q$ then $p \leftrightarrow q = I_n$, so, if $p = q$ then $p \leftrightarrow q$ is not a true "swap", but it is a permutation nevertheless: it equals I_n. We are mainly interested in *proper* swaps, which are swaps $p \leftrightarrow q$ with $p \neq q$. In the literature proper swaps are also known as "transpositions".

convention: Because of the isomorphism discussed in the previous section we consider $p \leftrightarrow q$ to be a permutation in $\mathcal{P}_n$, for every n satisfying $p, q \in [\,0\,..\,n\,)$, without distinguishing these swaps notationally.
□

Property: Swapping p and q is symmetric in p and q, that is: $(p \leftrightarrow q) = (q \leftrightarrow p)$, for all p, q. Usually, we will, however, represent swaps uniquely, by confining ourselves to swaps $(p \leftrightarrow q)$ with $p < q$.
□

5.39 Lemma. Every swap is its own inverse; that is, for all $p, q \in [\,0\,..\,n\,)$ we have:

$$(p \leftrightarrow q) \circ (p \leftrightarrow q) \quad = \quad I_n \quad .$$

proof: Directly from the definitions of $\circ$ and $\leftrightarrow$.
□

The following property shows the effect of the composition of a permutation and a swap: the permutation $s \circ (p \leftrightarrow q)$ differs from s only in that s_p and s_q are interchanged.

Property (6): For $s \in \mathcal{P}_n$ and for $p, q \in [\,0\,..\,n\,)$ we have:

$$
\begin{array}{lcl}
(\,s \circ (p \leftrightarrow q)\,)\,(p) & = & s_q \quad , \\
(\,s \circ (p \leftrightarrow q)\,)\,(q) & = & s_p \quad , \\
(\,s \circ (p \leftrightarrow q)\,)\,(i) & = & s_i \quad , \quad \text{for all } i : i \in [\,0\,..\,n\,) \wedge i \neq p \wedge i \neq q \quad .
\end{array}
$$

proof: Directly from the definitions of $\circ$ and $\leftrightarrow$.

□

5.40 Lemma. Every permutation is the continued composition of a finite sequence of swaps.

proof: The lemma states that, for every $n : 1 \leq n$ and for every permutation in $\mathcal{P}_n$, there exists a finite list of swaps, the continued composition of which equals s. We prove this by Mathematical Induction on n.

base: The only permutation in $\mathcal{P}_1$ is I_1, and I_1, being the identity element of function composition, is the continued composition of $[\,]$.

step: Let $s \in \mathcal{P}_{n+1}$. Let p, $0 \leq p < n$, be such that $s_p = n$. Then we have, by property (6), that $(\,s \circ (p \leftrightarrow n)\,)\,(n) = n$, from which we conclude, using Lemma (5.37), that $s \circ (p \leftrightarrow n) \in \mathcal{P}_n$. By Induction Hypothesis, let ss be a (finite) list of swaps the continued composition of which equals $s \circ (p \leftrightarrow n)$; so, we have: $\mathcal{C}(ss) = s \circ (p \leftrightarrow n)$. Now we derive:

$$
\begin{array}{ll}
 & s \\
= & \quad \{\ I_n \text{ is identity of } \circ\text{; Lemma (5.39)}\ \} \\
 & s \circ (p \leftrightarrow n) \circ (p \leftrightarrow n) \\
= & \quad \{\ \text{definition of } ss\ \} \\
 & \mathcal{C}(ss) \circ (p \leftrightarrow n) \\
= & \quad \{\ \text{definition of } \mathcal{C}\ \} \\
 & \mathcal{C}(ss) \circ \mathcal{C}([\,(p \leftrightarrow n)\,]) \\
= & \quad \{\ \text{definition of } \mathcal{C}\ \} \\
 & \mathcal{C}(\,ss +\!\!+ [\,(p \leftrightarrow n)\,]) \quad ,
\end{array}
$$

from which we conclude that permutation s is the continued composition of the list $ss +\!\!+ [\,(p \leftrightarrow n)\,]$ of swaps.

□

The proof of this lemma also provides some information on the *length* of the list of swaps. The permutation I_1 is the continued composition of $[\,]$, which has length 0, that is, $1-1$. If we now, by Induction Hypothesis, assume that list ss has length $n-1$, then list $ss +\!\!+ [\,(p \leftrightarrow n)\,]$ has length $(n+1)-1$. Thus, we conclude that every permutation in $\mathcal{P}_n$ is the composition of $n-1$ swaps.

Notice that, in the above proof, we have *not* distinguished the cases $p = n$ and $p \neq n$, as this is unnecessary: the given proof is valid for either case. If, however, $p = n$ then $(p \leftrightarrow n)$ equals the identity and can, therefore, be omitted. As a result, we conclude that every permutation in $\mathcal{P}_n$ is the composition of *at most* $n-1$ swaps.

Finally, we note that the representation of a permutation by a list of swaps is not *unique*: every finite list of swaps represents some permutation, and one and the same permutation may be represented by very many different lists of swaps. In the following section, however, we will prove quite a surprising result: the permutations can be partitioned into two classes, which we will call "even permutations" and "odd permutations", and every swap changes the class of the permutation; that is, the composition of a permutation and a swap always is in the other class than the original permutation. As a consequence, every permutation is even if and only if it is the composition of an even number of swaps, *independently* of the actual composition!

5.6.6 Neighbor swaps

A special case of swaps are the, so-called, "neighbor swaps", which are swaps of the form $(p \leftrightarrow (p{+}1))$. As we will see, these provide useful stepping stones in the analysis of even and odd permutations, in the next subsection.

Just as every permutation can be composed from swaps, every swap, in turn, can be composed from neighbor swaps. To prove this we need the following lemma first.

5.41 Lemma. For every p, q with $0 \leq p < q$ we have:

$$(p \leftrightarrow (q{+}1)) \;=\; (q \leftrightarrow (q{+}1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q{+}1)) \quad .$$

proof: We prove this by showing that $(p \leftrightarrow (q{+}1))\,(i)$ is equal to $((q \leftrightarrow (q{+}1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q{+}1)))\,(i)$, for all $i : 0 \leq i$. This requires distinction of 4 cases: $i = p$, $i = q$, $i = q{+}1$, and all other values of i. We illustrate this for the case $i = q{+}1$; the other cases can be verified similarly:

$$\begin{array}{ll}
 & ((q \leftrightarrow (q{+}1)) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q{+}1)))\,(q{+}1) \\
= & \quad \{ \text{ Property (6) } \} \\
 & ((q \leftrightarrow (q{+}1)) \circ (p \leftrightarrow q))\,(q) \\
= & \quad \{ \text{ Property (6) } \} \\
 & (q \leftrightarrow (q{+}1)))\,(p) \\
= & \quad \{ \text{ definition of } \leftrightarrow, \text{ using } p < q, \text{ so } p \neq q \text{ and } p \neq q{+}1 \ \} \\
 & p \\
= & \quad \{ \text{ definition of } \leftrightarrow \ \} \\
 & (p \leftrightarrow (q{+}1)))\,(q{+}1) \quad .
\end{array}$$

□

This lemma shows that the swap $(p \leftrightarrow (q{+}1))$ can be defined recursively as the composition of $(p \leftrightarrow q)$ and 2 neighbor swaps $(q \leftrightarrow (q{+}1))$. As a result we obtain the following lemma, which turns out useful in the next subsection.

5.42 Lemma. Every swap $(p \leftrightarrow q)$, for p, q with $0 \leq p < q$, is the continued composition of exactly $2*k+1$ neighbor swaps, where $k = q-1-p$. Notice that the number $2*k+1$ is *odd*.

proof: We prove this by Mathematical Induction on the value of k. The basis of the induction, of course, is the swap $(p \leftrightarrow (p+1))$, so $k=0$, which all by itself is a *single* neighbor swap. For p, q with $0 \leq p < q$, the swap $(p \leftrightarrow (q+1))$ is, by Lemma (5.41), the composition of $(p \leftrightarrow q)$ and 2 neighbor swaps $(q \leftrightarrow (q+1))$. Hence, if, by Induction Hypothesis, $(p \leftrightarrow q)$ is the composition of $2*k+1$ neighbor swaps then $(p \leftrightarrow (q+1))$ is the composition of $2*(k+1)+1$ neighbor swaps.

□

Aesthetic aside: Because $(q \leftrightarrow (q+1)) = ((q+1) \leftrightarrow q)$, the formula in Lemma (5.41) can be rendered in a more *symmetric* way as:

$$(p \leftrightarrow (q+1)) \;=\; ((q+1) \leftrightarrow q) \circ (p \leftrightarrow q) \circ (q \leftrightarrow (q+1)) \quad .$$

For p, q with $0 \leq p < q$, Lemma (5.42) can now be rendered, informally, as:

$$\begin{aligned}(p \leftrightarrow q) \;=\; & (q \leftrightarrow (q-1)) \circ ((q-1) \leftrightarrow (q-2)) \circ \cdots \circ ((p+2) \leftrightarrow (p+1)) \circ \\ & (p \leftrightarrow (p+1)) \circ \\ & ((p+1) \leftrightarrow (p+2)) \circ \cdots \circ ((q-2) \leftrightarrow (q-1)) \circ ((q-1) \leftrightarrow q) \quad .\end{aligned}$$

□

* * *

We are now ready to harvest the results of the above labor. To start with, we observe that the actual number of inversions in a permutation does not give much information, but this number being even or odd does. This we call the *parity* of a permutation.

5.43 Definition. For $s \in \mathcal{P}_n$ the *parity* of s is:

$$(\#i, j : 0 \leq i < j < n : s_j < s_i) \bmod 2 \quad .$$

□

If the parity of a permutation equals 0 we also call the permutation "even" and if its parity equals 1 we also call the permutation "odd". Now the above analysis boils down to the following lemma.

5.44 Lemma. Composition of a permutation with a proper swap changes its parity.

□

By "repeated application" – that is, of course, by Mathematical Induction – of this lemma we obtain the following theorem.

5.45 Theorem. If a permutation equals the continued composition of a sequence of proper swaps, then its parity equals the parity of the number of swaps.

proof: By Mathematical Induction on the length of the sequences, using the previous lemma.
□

Notice that this theorem pertains to *all possible* ways in which a given permutation equals the continued composition of a sequence of proper swaps. As a consequence, if two different such sequences represent the same permutation, then their lengths have equal parities. So, an even permutation can only be composed from an even number of swaps and an odd permutation can only be composed from an odd number of swaps, independently of *how* the permutation is composed from swaps.

Having the same parity is an equivalence relation. This relation partitions $\mathcal{P}_n$ into two equivalence classes, containing the even and the odd permutations in $\mathcal{P}_n$, respectively. Recalling that $(\mathcal{P}_n, \circ, I_n)$ is a group, we now also obtain the following additional result.

5.46 Theorem. In the group $(\mathcal{P}_n, \circ, I_n)$ the subset of the even permutations, with $\circ$ and I_n, form a subgroup of $(\mathcal{P}_n, \circ, I_n)$. This means that:

a) I_n is even;

b) if s and t are even then so is $s \circ t$;

c) if s is even then so is s^{-1}.

proof: Left as an exercise.
□

5.7 Exercises

1. Prove that every group $(V, *, I)$ satisfies: $I^{-1} = I$.
2. Describe all groups with exactly 2 elements, with 3 elements, and with 4 elements.
3. Why is $(\mathbb{N}, +, 0)$ not a group?
4. Prove that in every group $(V, *, I)$ we have, for all $x \in V$ and $n \in \mathbb{N}$: $x^n = I \;\Leftrightarrow\; x^{-n} = I$.
5. Let $(M, *, I)$ be a monoid and let $a, b \in M$ satisfy $a^2 = b^3 = I$. Prove that $(a * b * a)^6 = I$.
6. For a fixed natural number p, $2 \leq p$, we define operator $\otimes$, of type $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, by $x \otimes y = (x * y) \bmod p$, for all $x, y \in \mathbb{Z}$. Prove that:
   (a) $([0\,..\,p), \otimes, 1)$ is a monoid;
   (b) $([0\,..\,p), \otimes, 1)$ is not a group;
   (c) $([1\,..\,p), \otimes, 1)$ is a group if and only if p is a prime number.

7. What is, in a group $(V, *, I)$, the subgroup generated by I?
8. What is, in the group $(\mathbb{Q}\backslash\{0\}, *, 1)$, the subgroup generated by 2?
9. Why is $(\mathbb{Q}^-, *, 1)$ *not* a subgroup of $(\mathbb{Q}\backslash\{0\}, *, 1)$?
10. Show that $(\mathbb{Z}, +, 0)$ is cyclic.
11. We consider a group $(V, *, I)$. Prove that, for every non-empty subset $U \subseteq V$, the structure $(U, *, I)$ is a subgroup of $(V, *, I)$ if and only if:

$$(\forall x, y : x, y \in U : x * y^{-1} \in U) \quad .$$

12. We consider, for some positive natural n, the group $([0..n), \oplus, 0)$, with $\oplus$ as defined in Example 5.20 (e).
    (a) Prove that, for all positive natural m, the subgroup generated by m is the whole group if and only if m and n are relatively prime.
    (b) Identify all subgroups of this group.
13. Let $(G, *, I)$ be a group and let $a \in G$. Let $f : G \to G$ be the function defined by $f(x) = x * a$ for all $x \in G$. Prove that f is bijective.
14. Compute the order of each of the following permutations on $\{a, b, c, d, e\}$:
    (a) $\{(a, d), (b, e), (c, c), (d, a), (e, b)\}$.
    (b) $\{(a, a), (b, e), (c, b), (d, d), (e, c)\}$.
    (c) $\{(a, d), (b, b), (c, e), (d, c), (e, a)\}$.
    (d) $\{(a, b), (b, e), (c, a), (d, c), (e, d)\}$.
    (e) $\{(a, d), (b, e), (c, b), (d, a), (e, c)\}$.
15. Prove that there is no permutation on $\{a, b, c, d, e\}$ of order 8.
16. Prove that there is a permutation on $\{a, b, c, d, e, f, g, h\}$ of order 15.
17. (Warning: this exercise is quite hard) We consider a monoid $(M, *, I)$ with exactly 8 elements. M contains an element g, say, *of order* 7. This means that $g^7 = I$ and that $g^i \neq I$, for all $i : 1 \leq i < 7$.
    (a) Prove that M contains an element h, say, that is not a power of g.
    (b) Prove that such h satisfies $h * g = h$.
18. Identify all subgroups of the group of permutations on $\{1, 2, 3\}$.
19. Give an example showing that composition of swaps usually is not commutative. That is, give example values for k, l, p, q such that:
    $(k \leftrightarrow l) \circ (p \leftrightarrow q) \neq (p \leftrightarrow q) \circ (k \leftrightarrow l)$.