Groups

Definition 1.1. An algebra (G,*) is called a group iff

(a) * is associative

(b) G has an identity element *e*

(c) every element of G is invertible

The group is called abelian if

(d) * is commutative.

Example 1.1. $(2^X,\div)$, $(\mathbf{Z}_n,\oplus)$, $(\mathbf{R},+)$,$(\mathbf{Z},+)$, $(\mathbf{R}^+,\cdot)$ are groups. The first two cases were considered in the previous chapter, the other are obvious. They are all abelian groups. The dot in the last example denotes ordinary multiplication.

Example 1.2. $(\mathbf{R},\cdot)$ is not a group because 0 is not invertible under multiplication.

Example 1.3. For every positive integer n, $(\mathbf{Z}_n,\oplus)$ is a group. See Proposition 1.1.

Example 1.4. $(\mathbf{Z}_6,\otimes)$ is not a group because 2 is not invertible.

Example 1.5. Let PERM(X) denote the set of all bijections from X into X. (PERM(X),$\circ$) is a group, in general it is not commutative. In the case an *n*-element set X we use the symbol S_n instead of PERM(X), and the group $(S_n,\circ)$ is called the symmetric group on n elements.

Example 1.6. Let X be any set and let (**G**,#) be a group. Consider the pair $(\mathbf{G}^X,*)$ with the * defined as (f*g)(x)=f(x)#g(x). * is obviously an operation on $\mathbf{G}^X$. It is associative because # is. The identity element for * is f_e defined as $f_e(x)=e$ for every $x\in X$, with *e* denoting the identity element of **G**. The inverse element to a function $f\in \mathbf{G}^X$ is the function f^{-1} defined as $f^{-1}(x)=(f(x))^{-1}$, where the $^{-1}$ on the right hand side denote the inverse with respect to #. Notice that our f^{-1} symbol has nothing to do with the ordinary inverse function.

Example 1.7. $\mathbf{Q}(\sqrt{p}) = \{ a+b\sqrt{p} : a,b\in \mathbf{Q}\}$. $(\mathbf{Q}(\sqrt{p}),+)$ is a group for every number *p*.

Example 1.8. $\mathbf{Q}(\sqrt{2})-\{0\}$ is a group with respect to regular multiplication. Here we must verify first that the set is closed under multiplication. Take two elements from $\mathbf{Q}(\sqrt{2})-\{0\}$, $a+b\sqrt{2}$ and $c+d\sqrt{2}$, and consider $(a+b\sqrt{2})(c+d\sqrt{2}) = ac+2bd+(ad+bc)\sqrt{2}$. The last number is in the form required for elements of $\mathbf{Q}(\sqrt{2})$ and is certainly different from 0 – because it is the product of two nonzero real numbers. Multiplication is obviously associative in $\mathbf{Q}(\sqrt{2})-\{0\}$ because it is associative in **R**. The identity element for multiplication is 1and $1 = 1+0\sqrt{2}$ belongs to $\mathbf{Q}(\sqrt{2})-\{0\}$. To prove that every element in $\mathbf{Q}(\sqrt{2})-\{0\}$ is invertible

we transform the arithmetic inverse of $a+b\sqrt{2}$, $\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a}{a^2-2b^2}$

$+\frac{-b}{a^2-2b^2}\sqrt{2}$ and obtain that it belongs to $\mathbf{Q}(\sqrt{2})-\{0\}$. This group is also abelian.

Theorem 1.1. ($\mathbf{Z}_n-\{0\},\otimes$) is a group iff n is a prime.

Proof. ($\Leftarrow$) Recall that n is a prime iff for every two integers p and q, n|pq implies n|q or n|q (n|p means "n divides p"). This implies that for any p,q$\in\{1,2,\ldots,n-1\}=\mathbf{Z}_n-\{0\}$, pq is not divisible by n, hence p$\otimes$q$\neq$0 and $\mathbf{Z}_n-\{0\}$ is closed under $\otimes$. Associativity of $\otimes$ follows from Proposition 1.1???. Number 1 is obviously the identity element.

Now let us chose an element x from $\mathbf{Z}_n-\{0\}$. Suppose x$\otimes$p=x$\otimes$q for some p,q$\in\mathbf{Z}_n-\{0\}$. That means xp mod n = xq mod n, which implies that x(p–q) mod n =0, which in turn implies n|x(p–q). Since n is a prime it follows that n|x (impossible as x$\in\{1,2,\ldots,n-1\}$) or n|p–q. Now, –n+2$\leq$p–q$\leq$n–2, and the only number in that interval divisible by n is 0. Hence p=q. We have shown that the numbers x$\otimes$1, x$\otimes$2, … x$\otimes$(n-1) are n–1 pairwise different members of $\mathbf{Z}_n-\{0\}$. Since $\mathbf{Z}_n-\{0\}$ has exactly n–1 elements, each element of $\mathbf{Z}_n-\{0\}$ appears somewhere on the list, hence one of them is 1 and x is ivertible.

($\Rightarrow$) If n is a composite number then n=pq for some p,q$\in\mathbf{Z}_n-\{0\}$. But then p$\otimes$q=0, so $\mathbf{Z}_n-\{0\}$ is not closed under $\otimes$.□

Theorem 1.2. In every group (G,*) with identity e, and for every a,b$\in$G we have

(1) $(a*b)^{-1}=b^{-1}*a^{-1}$

(2) $(a^{-1})^{-1}=a$

Proof. To prove (1) it is enough to notice that $(b^{-1}*a^{-1})*(a*b)=((b^{-1}*a^{-1})*a)*b=((b^{-1}*(a^{-1}*a))*b=(b^{-1}*e)*b=b^{-1}*b=e$. Part (2) is obvious.□

Theorem 1.3. (Cancellation law)

In every group (G,*), for every a,b,c$\in$G if a*b=a*c then b=c.

Proof. Let e denote the identity element of *. a*b=a*c implies $a^{-1}*(a*b)=a^{-1}*(a*c)$. By associativity of * we have $(a^{-1}*a)*b=(a^{-1}*a)*c$, hence e*b = e*c and b=c. □

Definition 1.2. In every group (G,*) with identity e, and for every a$\in$G we will denote $a^0=e$ and for all n$\in\mathbf{N}$, $a^n=a*a^{n-1}$ and $a^{-n}=(a^n)^{-1}$.

Proposition 1.1. In every group (G,*) for every $a \in G$, and for every integer $n>0$, $a^n = a^{n-1}*a$.

Proof. It is enough to show that $a^{n-1}*a = a*a^{n-1}$. We will prove it using induction on n. For n=1 there is nothing to prove, since $a^0=e$. Suppose the equality holds for some n and consider a^{n+1}.

$a^{n+1} = a* a^n$ by Definition 1.2

$= a* (a^{n-1}*a)$ by induction hypothesis

$= (a*a^{n-1})*a$ by associativity of *

$= a^n*a$ by Definition 1.2 again.□

Theorem 1.4. Let (G,*) be a group, $a,b \in G$ and $m,n \in \mathbf{Z}$. Then

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

(2) $a^m*a^n = a^{m+n}$

(3) $(a^m)^n = a^{mn}$

Proof. (1) First we prove that $a^{-n} = (a^n)^{-1}$. For $n \geq 0$ it follows from Definition 1.2. For $n<0$ we put $k=-n$ and we write $a^{-n} = a^k = ((a^k)^{-1})^{-1} = (a^{-k})^{-1} = (a^n)^{-1}$.

Now we take care of the equality $(a^{-1})^n = (a^n)^{-1}$.We will prove it by induction on n. For n=0 it is obvious. Suppose n>0 and the equality holds for n–1.

$(a^{-1})^n = a^{-1}*(a^{-1})^{n-1}$ by Definition 1.2

$= a^{-1}*(a^{n-1})^{-1}$ by the induction hypothesis

$= (a^{n-1}*a)^{-1}$ by Theorem 1.2(1)

$= (a^n)^{-1}$ by Proposition 1.1

We are done in case $n \geq 0$. Now suppose $n<0$. We put $k=-n$.

$(a^{-1})^n = (a^{-1})^{-k}$ by definition of k

$= ((a^{-1})^k)^{-1}$ by Definition 1.2, we may use it as $k>0$

$= ((a^k)^{-1})^{-1}$ by the initial part of the proof

$= a^k$ Theorem 1.2(2)

$= a^{-n}$ by definition of k.

(2) First we will prove that for every m $a^{m+1} = a*a^m$. For $m \geq 0$ it follows from Definition 1.2. Suppose $m<0$ and put $k=-m$. Now

$a^{m+1} = (a^{-1})^{-m-1}$ by (1)

$= (a^{-1})^{k-1}$ by definition of n

$= (a^{-1})^{-1}(a^{-1})^k$	follows from the nonnegative m case of (2) with k−1 in place of m and a^{-1} in place of a
$= a*a^m$	from (1) Theorem 1.2(2).