BASIC EXAMPLES OF GROUPS

Cyclic Groups

Recall that a group G is called cyclic if $G =< g >$ for some $g \in G$. The set $\mathbb{Z}$ of all integers with addition is a group and it is cyclic with generator 1.

Let $G =< g >$ be cyclic. Consider the map $f : \mathbb{Z} \longrightarrow G$ given by $f(n) = g^n$. Since g generates G, f is surjective. The main properties of taking powers show that f is a group homomorphism: $f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$. Thus G is isomorphic to $\mathbb{Z}/\ker f$. If g has infinite order then $\ker f$ is trivial so $G \approx \mathbb{Z}$. If g has finite order n then $\ker f =< n >= n\mathbb{Z}$ (= the set of all multiples of n), so $G \approx \mathbb{Z}/ < n >$. We see that there is unique (up to isomorphism) infinite cyclic group and for each $n > 0$ there is unique (up to isomorphism) cyclic group of order n.

Exercise. Show that if p is a prime number then the only group of order p is the cyclic group.

Groups of Automorphisms

Let X be a set equipped perhaps with some additional structure (vector space, metric space, etc.) or, more generally, an object of some category. The set $\mathrm{Aut}X$ of all automorphisms of X (i.e. all bijections $X \longrightarrow X$ which preserve the structure) is a group under composition of functions. Properties of this group often encode important information about X so we can study X via an investigation of $\mathrm{Aut}X$. This is the reason why groups play such an important role in many areas of mathematics.

The above idea of producing groups is very general and leads to many important classes of groups. We are going to discuss now some of them which are of great importance in mathematics.

Permutation Groups

Let X be just a set (no additional structure). Then $\mathrm{Aut}X$ consists of all bijections $X \longrightarrow X$ and it is usually denoted by $S(X)$ and called the **group of permutations** of X. If X is infinite, this group is infinite too and it is a rather complicated object.

Of special importance is the case when $X = \{1, 2, ..., n\}$ is finite. Then $S(X)$ is denoted by S_n and called the **symmetric group** on n letters, or just the **symmetric group of degree** n. Since S_n consists of all permutations of $\{1, 2, ..., n\}$, we see that $|S_n| = n!$.

In order to deal with elements of S_n we need a handy way of denoting a permutation $\pi \in S_n$. One such a way is to express π as a $2 \times n$ matrix $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$. Thus $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ means that $\pi(1) = 3$, $\pi(2) = 2$, $\pi(3) = 1$ and $\pi(4) = 4$.

This way of expressing permutations makes it quite easy to multiply and invert permutations. There is also another, often more convenient way of representing permutations. Before its introduction we need to define a particularly nice class of permutations.

Consider $k \geq 2$ distinct elements $a_1, a_2, ..., a_k$ in $\{1, 2, ..., n\}$. By $(a_1, ..., a_k)$ we denote the permutation $\pi \in S_n$ described by $\pi(a_1) = a_2$, ..., $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$ and $\pi(i) = i$ for all other i.

A permutation of the form $(a_1, ..., a_k)$ is called a **cycle** of length k or a $k-$cycle. A $2-$cycle is usually called a **transposition**. Two cycles $(a_1, ..., a_k)$ and $(b_1, ..., b_m)$ are said to be **disjoint** if the sets $\{a_1, ..., a_k\}$ and $\{b_1, ..., b_m\}$ have no elements in common. If π and σ are disjoint cycles then $\pi\sigma = \sigma\pi$, i.e. any two disjoint cycles commute. Note that the order of a $k-$cycle equals k.

We say that i belongs to a $k-$cycle π if $\pi(i) \neq i$. If this is so then $\pi = (i, \pi(i), \pi^2(i), ..., \pi^{k-1}(i))$.

A permutation $\tau \in S_n$ can be expressed in at most one way (up to the order of factors) as a product of disjoint cycles. In fact, if $\tau = \pi_1 ... \pi_s$ is a product of disjoint cycles and i belongs to π_l then all other π_j's fix i and therefore $\pi_l = (i, \pi_l(i), \pi_l^2(i), ..., \pi_l^{k-1}(i)) = (i, \tau(i), \tau^2(i), ..., \tau^{k-1}(i))$. Thus π_l is determined by τ.

This argument shows also that in fact every permutation can be written as a product of disjoint cycles. In fact, each $i \in \{1, 2..., n\}$ is either a fixed point of τ (i.e. $\tau(i) = i$) or determines a cycle $(i, \tau(i), ..., .\tau^{t-1}(i))$, where t is the smallest positive integer such that $\tau^t(i) = i$. Note that any two elements of $\{1, 2, ..., n\}$ which are not fixed by τ determine cycles which are either disjoint or equal. The product

π of different cycles obtained in this way from τ is equal to τ. This can be seen by checking that both permutations act in the same way on each i. If i is a fixed point of τ then it does not belong to any of the cycles so it is fixed by all the cycles hence by their product, i.e. $\pi(i) = i = \tau(i)$. If i is not a fixed point of τ then it belongs to the cycle $(i, \tau(i), ..., .\tau^{t-1}(i))$ and all elements which belong to this cycle are fixed by all other cycles so again $\pi(i) = \tau(i)$. Thus $\pi = \tau$. We have therefore the following important

Proposition 1. *Every permutation τ can be uniquely (up to order) expressed as a product of disjoint cycles.*

Since disjoint cycles commute, it is not hard to see that the order of a permutation τ equals the least common multiple of the lengths of the cycles in the cycle decomposition of τ (prove it !).

Let us record now the following useful identity in S_n:

$$(a_1, ..., a_k) = (a_1, a_k)(a_1, a_{k-1})...(a_1, a_2),$$

which can be easily proved by inspecting how both sides act on elements of $\{1, 2, ..., n\}$. This shows that each cycle can be written as a product of transpositions. Proposition 1 implies now that

Proposition 2. *Every permutation can be expressed as a product of transpositions.*

This should not be surprising at all for it just says that each permutation can be realized by performing a series of interchanges of two objects at a time. There is no uniqueness in representing a permutation as a product of transpositions. However, the parity of the number of transpositions needed is the same for all such representations. This in not an obvious observation but it can be proved in a purely combinatorial way (Exercise). We do not provide such a proof here since we will obtain this result almost for free from our discussion in the next example.

Note now that $(i, j) = (1, i)(1, j)(1, i)$ for any $1 < i < j$. Consequently, every permutation is a product of transpositions of the form $(1, j)$. In other words, the set $\{(1, 2), ..., (1, n)\}$ generates S_n.

Another useful observation is that for $j > 2$ we have $(1, j) = (1, j, 2)(1, 2)(1, 2, j)$ and $(1, j, 2) = (1, 2, j)^{-1}$. Since $(1, i)^{-1} = (1, i)$, the previous observation implies now that any two transpositions are conjugate, i.e. for any (i, j) and (a, b) there is a permutation τ such that $(i, j) = \tau(a, b)\tau^{-1}$.

A more general result is that $\pi(a_1, ..., a_k)\pi^{-1} = (\pi(a_1), ..., \pi(a_k))$, so in particular any two $k-$cycles are conjugate in S_n.

Exercise. Show that two permutations π, τ are conjugate in S_n iff for each integer k they have the same number of $k-$cycles in their cycle decomposition.

Matrix Groups

Let K be a field and V an $n-$dimensional vector space over K. The group $\mathrm{Aut}(V)$ is usually denoted by $GL(V)$. After a choice of a basis, the vector space V may be identified with K^n and then $GL(V)$ is identified with $GL_n(K)$ (= the set of all $n \times n$ invertible matrices with entries in K). Note that $GL_n(K)$ is nothing but the set of all invertible elements in the ring $M_n(K)$ of all $n \times n$ matrices. It is not hard to see that the set of all invertible elements $R^\times$ in any ring R forms a group under multiplication. Note that $GL_1(K)$ is just $K^\times$.

The group $GL_n(K)$ is called the **general linear group** of degree n. Recall that to each $n \times n$ matrix A we associate a number $\det A$ in K. The group $GL_n(K)$ consists of all matrices with nonzero determinant. Since $\det(AB) = \det(A)\det(B)$, we see that det is a group homomorphism from $GL_n(K)$ to $K^\times$. The kernel of this homomorphism is denoted by $SL_n(K)$ and called the **special linear group** of degree n. Note that det is surjective, so it induces an isomorphism of $GL_n(K)/SL_n(K)$ and $K^\times$.

There are many other interesting subgroups of $GL_n(K)$. Let us introduce some of them. We have the subgroup $D_n(K)$ which consists of all **diagonal** matrices, i.e. matrices with all off-diagonal entries equal to 0. The diagonal matrix with the (i, i) entry a_i, $i = 1, 2, ..., n$ is usually denoted by $\mathrm{diag}(a_1, ..., a_n)$. The group $D_n(K)$ is abelian and $D_n(K) \cap SL_n(K)$ is denoted by $SD_n(K)$. The diagonal matrices whose diagonal entries are equal to each other are called **scalar** matrices. They form a subgroup of $D_n(K)$ which is isomorphic to $K^\times$ via the map $k \mapsto kI$, where I is the identity matrix. We denote the group of scalar matrices by $Z_n(K)$ and its intersection with $SL_n(K)$ by $SZ_n(K)$ (this is not a standard notation). The set of all **upper triangular** matrices, i.e. matrices with all entries below the main diagonal equal to 0, is denoted by $T_n(K)$. It is easy to see that $T_n(K)$ is a group and so is its subset $UT_n(K)$ consisting of all **unipotent** triangular matrices, i.e. triangular matrices with all diagonal entries equal to 1. Unipotent triangular matrices with first $i-1$ diagonals above the main diagonal consisting of 0 form a subgroup of $UT_n(K)$ denoted by $UT_n^i(K)$ (so $UT_n^1(K) = UT_n(K)$).

This ends our inspection of subgroups of $GL_n(K)$ but note that we left out many important subgroups. More about them can be found in the book [1].

Note that the permutation group S_n can be realized as a subgroup of $GL_n(K)$ for any field K. In fact, let $e_1, ..., e_n$ be the standard basis of K^n. Given a permutation $\pi \in S_n$ there is unique liner isomorphism of K^n which maps e_i to $e_{\pi(i)}$ for $i = 1, 2, ..., n$. The matrix of this linear transformation is denoted by P_π and called a **permutation matrix**. It is straightforward to verify that the association $P : \pi \mapsto P_\pi$ is an injective group homomorphisms from S_n to $GL_n(K)$. Its image consists of those linear transformations which permute the vectors of the standard basis.

Let $\pi = (i, j)$. If we exchange the $i - th$ and $j - th$ rows of P_π we get the identity matrix. It follows that $\det P_\pi = -\det I = -1$, i.e. the determinant of the matrix corresponding to a transposition is -1. Recall now that every permutation can be written as a product of transpositions. Since the determinant is a group homomorphism we see that if τ is a product of k transpositions then $\det P_\tau = (-1)^k$. Moreover, the map $\epsilon : \tau \mapsto \det P_\tau$ is a group homomorphism onto the subgroup $\{1, -1\}$ of $K^\times$.

Suppose now that the field K does not have characteristic 2, so $-1 \neq 1$. For example, take $K = \mathbb{R}$. Then ϵ is a surjective homomorphism from S_n onto the cyclic group $\{1, -1\}$ of order 2. From our formula for ϵ we see that a permutation can not be both a product of an even and an odd number of transpositions. This proves the claim we made some time ago. Also, the homomorphism ϵ does not depend on the field K (provided K has characteristic different from 2). The number $\epsilon(\tau)$ is called the **sign** of the permutation τ. Permutations with sign equal to 1 are called **even**, and those with sign -1 are called **odd**. Thus even permutations are exactly those which can be expressed as a product of an even number of transpositions. For example, a $k-$cycle is even iff k is odd.

The kernel of ϵ consists of all even permutations. We denote it by A_n and call the **alternating** group of degree n. It is a normal subgroup of S_n of index 2, so $|A_n| = n!/2$.

Exercise. Prove that A_n is generated by all $3-$cycles. (Hint. Show that if a, b, c, d are pairwise distinct, then $(a, b)(a, c) = (a, c, b)$ and $(a, b)(c, d) = (a, b, c)(b, c, d)$.). Prove that for $n \geq 5$ any two $3-$cycles in A_n are conjugate (in A_n).

Exercise. Let $\pi \in S_n$ and suppose that $\pi(i) = i$. Then π can be considered as an element of S_{n-1} regarded as the group of permutations of $\{1, 2, ..., n\} - \{i\}$. Prove that π is odd in S_n iff it is odd in S_{n-1}.

Exercise Show that the center of S_n for $n \geq 3$ and of A_n for $n \geq 4$ is trivial. Describe the centers of A_n and S_n in the remaining cases.

Exercise. Show that $[S_n, S_n] = A_n$ for all n and $[A_n, A_n] = A_n$ for $n \geq 5$. Describe the derived group of A_n for $n < 5$.

Let us mention some further properties of the general linear group $GL_n(K)$. For $i \neq j$ denote by $t_{i,j}(a)$ the matrix with all diagonal entries 1, the $(i, j)-$entry equal to a and all other entries 0. Matrices of this form are called **elementary** matrices (or **transvections**). They all belong to $SL_n(K)$, and if $i < j$ then $t_{i,j}(a) \in UT_n(K)$.

It can be proved that the elementary matrices generate $SL_n(K)$. To get generators for $GL_n(K)$ it is enough to add to the collection of all elementary matrices all diagonal matrices of the form $\text{diag}(1, ..., 1, a)$ with $a \in K^{\times}$.

To prove these claims note first that for any matrix $A \in GL_n(K)$, the product $t_{i,j}(a)A$ is obtained from A by adding to the $i-$th row of A the $j-$th row multiplied by a. The product $At_{i,j}(a)$ is an analogous operation on columns of A. It is now easy to see that by performing a row operation on A we can obtain a matrix with a nonzero $(2, 1)$-entry $a_{2,1}$. Performing one more row operation, namely adding to the first row the second row multiplied by $(1 - a_{1,1})/a_{2,1}$, we get a matrix with $(1, 1)-$entry 1. By adding suitable multiples of the first row to the other rows and then suitable multiples of the first column to the other columns we arrive at a matrix with zeros in the first row and column, except the $(1, 1)$ entry, where we have 1. Now apply this process to the second row and column by using only matrices $t_{i,j}(a)$ with $i, j \geq 2$ (which do not affect the first row and column), etc. so at the end we arrive at a diagonal matrix $\mathrm{diag}(1, 1, ..., 1, a)$. This shows that $A = t_1...t_r\mathrm{diag}(1, ..., 1, a)t_{r+1}...t_{r+s}$ for some elementary matrices t_i. This proves the claim about generators of $GL_n(K)$. To get the claim about generators of $SL_n(K)$ it is enough to note that $\det A = a$ so $a = 1$ for $A \in SL_n(K)$.

Exercise. Prove that $T_n(K)$ is generated by the diagonal matrices and the matrices $t_{i,j}(a)$ with $i < j$. Prove that $UT_n^m(K)$ is generated by $t_{i,j}(a)$ with $j - i \geq m$.

The center of $GL_n(K)$ equals $Z_n(K)$, and the center of $SL_n(K)$ is $SZ_n(K)$. To see this note that $t_{i,j}(1)A = At_{i,j}(1)$ implies that $a_{i,k} = 0$ for $k \neq j$, $a_{k,j} = 0$ for $k \neq i$ and $a_{i,i} = a_{j,j}$.

Exercise. Describe the centers of $T_n(K)$ and $UT_n^m(K)$.

The derived group of $GL_n(K)$ is $SL_n(K)$ except when $n = 2$ and $|K| = 2$. The derived subgroup of $SL_n(K)$ is $SL_n(K)$ (so $SL_n(K)$ is perfect) except when $n = 2$ and $|K| \leq 3$. To prove this note that $[t_{i,k}(a), t_{k,j}(b)] = t_{i,j}(ab)$ if i, j, k are pairwise distinct. This easily implies our claims for $n > 2$. For $n = 2$ use the fact that $[t_{i,j}(a), \mathrm{diag}(b_1, ..., b_n)] = t_{i,j}(a(b_j - b_i)/b_i)$.

Exercise. Prove that $[T_n(K), T_n(K)] = UT_n(K)$ if $|K| > 2$ and $[UT_n^i(K), UT_n^j(K)] = UT_n^{i+j}(K)$ for all fields K.

The group $GL_n(K)/Z_n(K)$ is denoted by $PGL_n(K)$ and called the **projective linear group** of degree n. The group $SL_n(K)/SZ_n(K)$ is called the **special projective group** of degree n and is denoted by $PSL_n(K)$. The importance of these groups stems from the following result:

Jordan-Dikson Theorem. *If K has more than 3 elements or $n > 2$ then $PSL_n(K)$ is simple.*

Exercise. Show that $UT_n(K) \triangleleft T_n(K)$ and that $T_n(K)/UT_n(K)$ is isomorphic to $D_n(K)$. Show that $UT_n^i(K)$ is normal in $T_n(K)$ for all i. Describe $UT_n^m(K)/UT_n^{m+1}(K)$.

Dihedral Groups

The finite dihedral group D_n occurs naturally in Euclidean geometry as the group of isometries of a regular $n-$gon $A_1...A_n$ (counterclockwise orientation). Let $\rho \in D_n$ be the rotation counterclockwise by $2\pi/n$. Then ρ has order n and $\rho^{k-1}(A_1) = A_k$. Let $\tau \in D_n$ be the reflection about the unique symmetry axis passing through A_1. Thus τ has order 2 and $\tau(A_i) = A_{n+2-i}$. Let $t \in D_n$ be arbitrary. If $t(A_1) = A_k$ then $(\rho^{n-k+1}t)(A_1) = A_1$. Note now that any isometry of a regular $n-$gon which fixes A_1 maps A_2 either to A_n or to A_2 and in the first case it is τ and in the second it is the identity. It follows that $\rho^{n-k+1}t$ is either the identity or τ, so t is of the form $\rho^a\tau^b$ for some $0 \le a \le n-1$ and $0 \le b \le 1$. Thus D_n has at most $2n$ elements, but it also has at lest $2n$ elements (the rotations and the symmetries), so $|D_n| = 2n$. Consequently, each element of D_n can be uniquely written as $\rho^a\tau^b$ for some $0 \le a \le n-1$ and $0 \le b \le 2$. In order to understand the multiplication in D_n we need to be able to write $(\rho^a\tau^b)(\rho^c\tau^d)$ in the form $\rho^s\tau^t$. The key observation is that $\tau\rho\tau^{-1} = \rho^{-1}$. Using it, it is easy to see that $s \equiv a + (-1)^b c \pmod{n}$ and $t \equiv b + d \pmod{2}$ (prove it).

We may identify isometries of a regular $n-$gon with the corresponding permutations of vertices. This induces an injective homomorphism $D_n \longrightarrow S_n$ and the image of D_n is the subgroup of S_n generated by the permutations $(1, 2, ...n)$ (the image of ρ) and $(2, n)(3, n-1)...(\lceil n/2\rceil, n+2-\lceil n/2\rceil)$ (the image of τ).

Exercise. Find the center and the derived group of D_n. Describe all subgroups and all normal subgroups of D_n.

Exercise. Prove that the group D_n is isomorphic to the subgroup of $GL_2(\mathbb{C})$ generated by the matrices $\begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, where ζ_n is a primitive $n-$th root of 1.

Exercise. Let G be the set of all bijections $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ which preserve distance, i.e. $|f(i) - f(j)| = |i - j|$ for all integers i, j.

a) Show that G is a group.

b) The group G contains elements T, S such that $T(a) = a + 1$ and $S(a) = -a$ for all integers a. Find the order of T and S.

c) Show that if $F \in G$ and $F(0) = 0$ then either $F = 1$ (the identity) or $F = S$.

d) Show that every element of G is of the form T^i or ST^i for some integer i (try to use similar argument to the one we used for dihedral group of order n).

e) Suppose that $T^5S^7T^3 = S^aT^b$. Find a and b.

f) Find the center and the derived group of G.

The above group G is called the **infinite dihedral** group and it is denoted by D_∞.

The Quaternion Group

The quaternion group Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with multiplication given by the following formulas:

- $1a = a1 = a$ for all $a \in Q_8$ (i.e. 1 is the identity in Q_8);
- $(-1)a = a(-1) = -a$ for all $a \in Q_8$ (here we use the convention that $-(-x) = x$);
- $ii = (-i)(-i) = jj = (-j)(-j) = kk = (-k)(-k) = -1$;
- $ij = (-i)(-j) = (-j)i = j(-i) = k$; $ji = (-j)(-i) = (-i)j = i(-j) = -k$;
- $jk = (-j)(-k) = (-k)j = k(-j) = i$; $kj = (-k)(-j) = (-j)k = j(-k) = -i$;
- $ki = (-k)(-i) = (-i)k = i(-k) = j$; $ik = (-i)(-k) = (-k)i = k(-i) = -j$.

It is a straightforward but tedious task to verify that the multiplication defined by these formulas indeed satisfies the group axioms.

Exercise. Prove that the quaternion group Q_8 is isomorphic to the subgroup of $GL_2(\mathbb{C})$ generated by the matrices $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Exercise. Find the center and the derived group of Q_8. Describe all subgroups of Q_8 and conclude that they are all normal.

Exercise. Prove that D_4 and Q_8 are not isomorphic.

Free Groups

Recall that a group generated by a set S consists of all products of the form $s_1^{u_1}s_2^{u_2}...s_k^{u_k}$ where $s_i \in S$ and $u_i = \pm 1$. In general, many expressions of this form represent the same element of the group. There is an obvious reason for that, coming from the identity $aa^{-1} = e$. A natural question to ask is whether there are groups generated by a subset S such that there are no non-obvious identities among the expressions of the form $s_1^{u_1}s_2^{u_2}...s_k^{u_k}$. Such groups indeed exist and they play an important role in the world of groups. In order to construct these groups let us start with a nonempty set X and set $Y = X \times \{-1, 1\}$. For convenience, we identify x and $(x, 1)$ and set x^{-1} for $(x, -1)$. Thus $Y = X \cup X^{-1}$, where $X^{-1} = X \times \{-1\}$. Moreover, we define $(x^{-1})^{-1} = x$.

A **word** w on Y is any sequence $w = y_1...y_k$ of elements in Y. The number k is called the **length** of w and by e we denote the empty word (of length 0). A word $w = y_1...y_k$ is called **reduced** if $y_{i+1} \neq y_i^{-1}$ for all $i = 1, ..., k-1$. In particular, all words of length ≤ 1 are reduced. Let $F(X)$ be the set of all reduced words. We define a multiplication on $F(X)$ by induction on the length of words as follows:

- $e \centerdot w = w \centerdot e = w$ for all $w \in F(X)$;
- suppose that the multiplication of reduced words of lengths $\leq k-1$ has been defined. For any reduced words $w = y_1y_2...y_l$ and $w' = y'_1...y'_m$ with $l, m \leq k$ define

$$w \centerdot w' = \begin{cases} y_1...y_ly'_1...y'_m & \text{if } y_l^{-1} \neq y'_1, \\ (y_1...y_{l-1}) \centerdot (y'_2...y'_m) & \text{if } y_l^{-1} = y'_1. \end{cases}$$

It is a straightforward exercise to verify that $(F(X), \centerdot, e)$ is a group. Let us just mention that the inverse of a reduced word $w = y_1...y_m$ is the reduced word $w^{-1} = y_m^{-1}...y_1^{-1}$.

The group $F(X)$ is called the **free** group on X. It is clear from the definition that the set X generates $F(X)$. Note that any word $w = y_1...y_k$ on Y (not necessarily reduced) can be interpreted as the element $y_1 \centerdot ... \centerdot y_k$ of $F(X)$. In the future, we will not write the $\centerdot$ and we will identify words on Y with products of elements in Y.

The free group on X has the following universal property: for any group G and any function $f : X \longrightarrow G$ there is unique homomorphism $\phi : F(X) \longrightarrow G$ such that $\phi(x) = f(x)$ for all $x \in X$. Clearly, if ϕ exists it has to be defined by $\phi(x) = f(x)$, $\phi(x^{-1}) = f(x)^{-1}$ for all $x \in X$ and $\phi(y_1...y_k) = f(y_1)...f(y_k)$ for any reduced word

$w = y_1 ... y_k$. The verification that so defined ϕ is indeed a group homomorphism is a straightforward exercise.

A group is called **free** if it is isomorphic to a group $F(X)$ for some set X. If $X = \{a\}$ consists of 1 element then $F(X)$ is just the infinite cyclic group. For $|X| > 1$, the group $F(X)$ is nonabelian.

Let us mention the following important result:

Nielsen-Schreier Theorem. *Any subgroup of a free group is free.*

The free groups provide an important method of defining groups, by **generators and relations**. Let X be a set and R be a subset of $F(X)$. Let H be the smallest normal subgroup of $F(X)$ which contains R. We denote by $< X|R >$ the group $F(X)/H$. If G is isomorphic to $F(X)/H$ then we say that G is presented by generators X and relations R. Of course, there are many ways of presenting a group. A group is called **finitely presented** if it can be given by a finite number of generators subject to a finite number of relations. A presentation is often given in the form $< (x_i)_{i \in I} | (w_j = w'_j)_{j \in J} >$. where w_j, w'_j are elements of $F(X)$ and $X = \{x_i : i \in I\}$. By definition, this is the same as $< X|R >$, where R consists of elements $w_j^{-1} w'_j$, $j \in J$. For example, $G =< a, b | a = b, a^2 = 1 >$ defines a cyclic group of order 2.

The method of generators and relations allows to define groups but it is in general a difficult problem to decribe in a more explicit form a group given by generators and relations or to present a given group by generators and relations.

Exercise. Prove that D_n has presentation $< a, b | aba^{-1} = b^{-1}, a^2 = 1 = b^n >$, $< a, b | aba^{-1} = b^{-1}, a^2 = 1 >$ is a presentation for D_∞ and $< a, b | a^4 = 1, a^2 = b^2, aba = b >$ is a presentation for Q_8.

For more about free groups and presentations consult [2], [4] or [3].

References

[1] J. L. Alperin, R. B. Bell, **Groups and Representations**, GTM 162, Springer-Verlag, New York, 1995.

[2] P. de la Harp, **Topics in Geometric Group Theory**, Chicago Lecture Notes in Mathematics, The University of Chicago Press, Chicago and London, 2000.

[3] R. C. Lyndon, P. E. Schupp, **Combinatorial group theory**, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89, Springer, 1977.

[4] W. Magnus, A. Karras, D. Solitar, **Combinatorial group theory**, J. Wiley, 1966.