§12. Generators and Relations.

Let S be a set of symbols, e.g. $\{a, b\}$. Let s^{-1} be the set of symbols $\{s^{-1} | s \in S\}$. At this stage we have no multiplication defined, so we are thinking of s^{-1} as a symbol and not as the inverse of s. We assume $S \cap S^{-1} = \emptyset$. A word is a finite string of symbols from $S \cup S^{-1}$ possibly with repetitions. Thus if $S = \{a, b\}$, then $aba^{-1}bb^{-1}ab$ is a word. Let W_S be the set of all words in symbols from $S \cup S^{-1}$. Also we regard the empty word as a word and denote it 1. Multiplication is defined on W_S by defining $w_1 w_2$ to be the word obtained by writing w_1 and then w_2: e.g. if $w_1 = aba^{-1}$ and $w_2 = ab^{-1}b$, then $w_1 w_2 = aba^{-1}ab^{-1}b$. With multiplication defined in this way, W_S is a semi-group but not a group because

Let R be a subset of W_S. If $u, v \in W_S$, we write $u = v (\text{mod } R)$, if there is a finite sequence

$$u = w_1, w_2, ..., w_k = v$$

of words such that w_i is obtained from w_{i-1}, $i = 2, ..., k$ by inserting or deleting either an element of R or a word of the form ss^{-1} or $s^{-1}s$ where $s \in S$.

EXAMPLE.
If $S = \{a, b\}$ and $R = \{a^2, b^3, a^{-1}bab^{-2}\}$, then $aba^{-1}bb^{-1}aba = b$ (mod R). (Note that we write a^2 to denote the word aa and b^{-2} to denote the word $b^{-1}b^{-1}$ etc.)
In this case the sequence

$aba^{-1}bb^{-1}aba,\ aba^{-1}aba,\ abba,\ abaa^{-1}ba,\ abaa^{-1}bab^{-1}b,$
$abaa^{-1}bab^{-1}b^{-1}bb,\ abab^2,\ aaa^{-1}bab^2,\ a^{-1}bab^2,\ a^{-1}bab^{-1}b^3,$
$a^{-1}bab^{-2}b^4,\ b^4,\ b$

has the required property.

THEOREM 12.1.
If $u = v(\text{mod } R)$ and $w \in W_S$, then $wu = wv(\text{mod } R)$ and $uw = vw(\text{mod } R)$

Proof.

Using this result the example above becomes much easier. Thus $a^{-1}bab^{-2} = 1$ $(\text{mod}R) \Rightarrow ba = ab^2$ $(\text{mod}R)$, multiplying on the left by a and on the right by b^2. Hence

$$\begin{aligned} aba^{-1}bb^{-1}aba &= ab^2a \ (\text{mod}R) \\ &= baa \ (\text{mod}R) \\ &= b \ (\text{mod}R) \end{aligned}$$

THEOREM 12.2.
Equality $(\text{mod}R)$ is an equivalence relation.

Proof.

Let $< w >$ denote the equivalence class of W_S containing w. It follows from Theorem 12.1 that if $u_1 = u_2 \ (\mathrm{mod}R)$ and $v_1 = v_2 \ (\mathrm{mod}R)$, then $u_1 v_1 = u_2 v_2 \ (\mathrm{mod}R)$, since

$$u_1 u_2 =$$

i.e. if $< u_1 >=< u_2 >$ and $< v_1 >=< v_2 >$, then $< u_1 u_2 >=< v_1 v_2 >$. This means that it is possible to define a multiplication on the equivalence classes of W_S under equality $(\mathrm{mod}R)$ by putting $< u >< v >=< uv >$.

THEOREM 12.3.
The equivalence classes of W_S determined by equality $(\mathrm{mod}R)$ form a group with multiplication as defined above.

Proof.

The above group is called the group with the elements of S as generators and the elements of R as relations.
Relations are usually written as equations, thus the group

$$(a, b|a^2 = b^3 = 1,\ ab = b^2a)$$

is the group as described above, in which

$$S = \{a, b\} \text{ and } R = \{a^2,\ b^3,\ aba^{-1}b^{-2}\}.$$

If $R = \emptyset$, the $w_1 = w_2 \ (\text{mod}R)$ if w_2 can be obtained from w_1 by inserting or deleting words of the form ss^{-1} or $s^{-1}s$, where $s \in S$. The group obtained in this case is called the free group on the set S.

Exercises

12.1. If $S = \{a, b\}$ and $R = \{a^{-1}bab^4,\ a^2\}$, prove that

$$b^{15} = 1 \ (\text{mod}R).$$

12.2. Prove that the group

$$(a,\ b\ |a^{-1}ba = b^2,\ b^{-1}ab = a^2)$$

has order 1.

§13. The Word Problem.

Let S be a set of symbols, and let $R \subseteq W_S$.

PROBLEM. Is it possible to program a computer so that if the computer is given two words w_1, w_2 it will be able to give the correct answer to whether or not $w_1 = w_2 \ (\mathrm{mod} R)$?
This problem is in fact "unsolvable". It was shown by P. S. Novikov (1955) that there is a finite set S and a finite set $R \subseteq W_S$ for which it is impossible to program a computer to answer the above question.
In particular cases the question above can be solved. If the group with S as set of generators and R as set of relations is finite, then the word problem can be solved (Mendelsohn 1964), although it has to be assumed that the computer involved has an unbounded amount of storage space and unlimited time to work on the problem.
The following theorem is useful in solving the word problem in some cases.

THEOREM 13.1.
Let G be a group with S as set of generators and R as set of relations. Let H be a group and suppose $\theta : \ S \longrightarrow H$ is a mapping such that for all $w \in R$, if $w = s_1^{\epsilon_1} s_2^{\epsilon_2} ... s_r^{\epsilon_r}$, then

$$(s_1\theta)^{\epsilon_1}(s_2\theta)^{\epsilon=2}...(s_r\theta)^{\epsilon_r} = 1_H.$$

Under these circumstances there exists a homomorphism $\theta_1 : \ G \longrightarrow H$ such that $< s > \theta_1 = s\theta$ for all $s \in S$.

EXAMPLE
Let $G = (a, \ b \,| a^2 = b^3 = 1)$. If $S = \{a, b\}$, then $\theta : \ S \longrightarrow S_3$, $a\theta = (12)$, $b\theta = (123)$ satisfies $(a\theta)^2 = 1, \ (b\theta)^3 = 1$. Theorem 13.1 then states that there is a homomorphism $\theta_1 : \ G \longrightarrow S_3$ such that $< a > \theta_1 = (12), \ < b > \theta_1 = (123)$.

Proof. (Theorem 13.1).
We define a mapping $\theta' : \ W_S \longrightarrow H$ as follows. If $w = s_1^{\epsilon_1} s_2^{\epsilon_2} ... s_r^{\epsilon_r}$, then $w\theta' = (s_1\theta)^{\epsilon_1}(s_2\theta)^{\epsilon=2}...(s_r\theta)^{\epsilon_r}$.
From the hypothesis of the theorem if $w \in R$, then $w\theta' = 1$. Suppose $w_1 = w_2 (\mathrm{mod} R)$.

Hence $w_1\theta' = w_2\theta'$, i.e. if $< w_1 >=< w_2 >$, then $w_1\theta' = w_2\theta'$. It follows that we can define a mapping $\theta_1 : \ G \longrightarrow H$ by putting $< w_1 >= w\theta'$. The mapping θ_1 is a homomorphism because

EXAMPLE.
Let $G = (a,\ b,\ |a^2 = b^5 = 1,\ a^{-1}ba = b^4)$. Let $S = \{a, b\}$ and $R = \{a^2,\ b^5,\ a^{-1}bab^{-4}\}$. Since $ba = ab^4 \ (\mathrm{mod}R)$, every word w of W_S is equal $(\mathrm{mod}R)$ to a word of the form a^ib^j and since $a^2 = 1 \ (\mathrm{mod}R)$ and $b^5 = 1 \ (\mathrm{mod}R)$ every word of W_S is equal $(\mathrm{mod}R)$ to one of the set

$$\{1,\ a,\ b,\ ab,\ b^2,\ ab^2,\ b^3,\ ab^3,\ b^4,\ ab^4\}.$$

The problem is to show that these elements lie in distinct equivalence classes under equality $(\mathrm{mod}R)$. If they are distinct, then the Cayley homomorphism

$$\rho : \ G \longrightarrow A(G)$$

gives

$$a\rho =$$
$$b\rho = (1,\ b,\ b^2,\ b^3,\ b^4)(a,\ ab,\ ab^2,\ ab^3,\ ab^4).$$

(Here we should really write $< a >, < b >$ etc. instead of $a,\ b$.) This gives us a clue as to how to show that G has 10 elements. Let

$$\alpha = (1,6)(2,10)(3,9)(4,8)(5,7)$$
$$\beta = (1,2,3,4,5)(6,7,8,9,10)\ ,$$

then $\alpha^2 = \beta^5 = 1$ and $\alpha^{-1}\beta\alpha = \beta^4$. Hence by Theorem 10.1 there is a homomorphism $\theta_1 : \ G \longrightarrow S_{10}$ such that $< a > \theta_1 = \alpha, < b > \theta_1 = \beta$. It is easy to check that θ' maps each element of the set

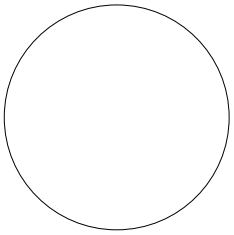
$$\{1,\ a,\ b,\ ab,\ b^2,\ ab^2,\ b^3,\ ab^3,\ b^4,\ ab^4\}$$

to a distinct element of S_{10} and so no two elements of this set represent the same element of G. Thus $o(G) = 10$.

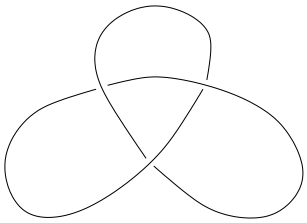
DEFINITION.
A subset K of $\mathbf{R}^3$ is called a knot if there is a continuous injective mapping $\theta : C \longrightarrow \mathbf{R}^3$ where $C \subseteq \mathbf{R}^2$ is the set $C = \{(x, y) | x^2 + y^2 = 1\}$ and $Im\theta = K$

EXAMPLES.

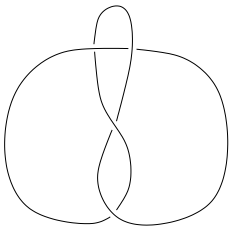
The trivial knot



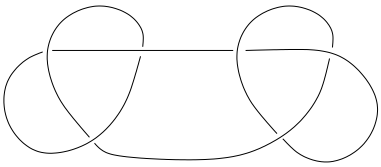
The trefoil



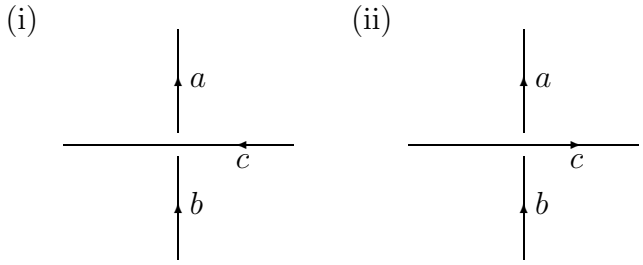
The figure-eight knot



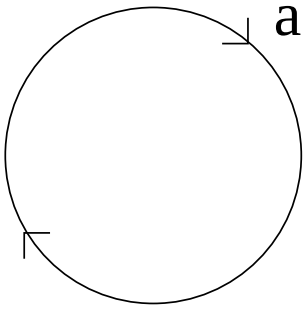
The granny knot



The main problem in knot theory is to give a procedure for deciding whether or not two knots are the same (whatever that means). Loosely speaking if one thinks of two knots as being made up of string, then they are the same if one can be moved to take up the same position as the second knot without cutting the string.
The problem above is unsolved. However it is often possible to show that two knots are different by computing knot groups.
In a knot diagram insert arrows giving one direction around the curve. Label each continuous piece of line by a symbol. Let S be the set of all labelling symbols. For each crossing point of the diagram we take a word r from W_S as follows: if the intersection is like (i) below with the line crossing over going from right to left take $r = cac^{-1}b^{-1}$, if as in (ii), then take $r = c^{-1}acb^{-1}$. Let R be the subset of W_S obtained by selecting an element for each crossing point of the knot diagram. Let G be the group with S as set of generators and R as set of relations. It can be shown that two different diagrams of the same knot give rise to isomorphic groups. Therefore G is called the group of the knot K. Actually G is isomorphic to the fundamental group of $\mathbf{R} - K$.



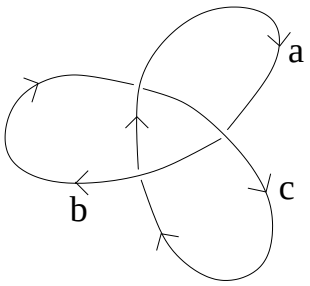
EXAMPLES
If K is the trivial group, then G is the group generated by a with no relations. Thus G is the infinite cyclic group with elements $1,\ a,\ a^{-1},\ a^2,\ a^{-2}, \cdots$.



If K is the trefoil, then

$G =$

Note that $c = aba^{-1}$. So substituting for c and c^{-1} wherever they occur: $G = (a,\ b,\ |aba^{-1}aab^{-1}a^{-1}b^{-1}, baba^{-1}b^{-1}a^{-1})$,



i.e.

$$\begin{aligned} G &= (a,\ b,\ |aba^{-1}aab^{-1}a^{-1}b^{-1}, baba^{-1}b^{-1}a^{-1}) \\ &= (a,\ b\ |aba = bab). \end{aligned}$$

We will be able to show that the trefoil is not the same as the trivial knot if we can show that this group is not isomorphic to the infinite cyclic group.

Now in S_3 if $\alpha = (12)$ and $\beta = (13)$, then

$$\alpha\beta\alpha = \qquad = \beta\alpha\beta.$$

Hence by Theorem 13.1 there is a homomorphism $\theta : \ G \longrightarrow S_3$ such that $a\theta = \alpha$, $b\theta = \beta$. This homomorphism is surjective, and so $S_3 \cong G/\mathrm{Ker}\theta$. But S_3 is not abelian and any factor of an abelian group is abelian. Hence G is not abelian and therefore cannot be infinite cyclic.

Exercises

13.1. Let $G = (a,\ b\ |a^2 = b^3 = (ab)^5 = 1)$. Prove that if H is abelian and $\theta : \ G \longrightarrow H$ is a homomorphism, then $a\theta = b\theta = 1$. Prove that there is a non-trivial homomorphism $\phi : \ G \longrightarrow A_5$.

13.2. Use Theorem 13.1 to show that

$$(a,\ b\ |aba = bab) \cong (c,\ d\ |c^2 = d^3).$$

13.3. Write down the knot group of the figure eight knot. Write down the knot group of the granny knot. Show that the granny knot is not the same as the trivial knot.