"1st International Symposium on Computing in Informatics and Mathematics (ISCIM 2011)"
in Collaboration between EPOKA University and "Aleksandër Moisiu" University of Durrës
on June 2-4 2011, Tirana-Durres, ALBANIA.

Some Applications Of Group Theory.

Orgest ZAKA[1], Fabiana ÇULLHAJ[2]
Department of Mathematic, Tirana University, Albania.
Email: gertizaka@yahoo.com– Phone: +35569571062
Department of Mathematic, University of "Aleksander Moisiu" Durres, Albania
Email: fabianacullhaj@hotmail.com– Phone: +355693067339

ABSTRACT.

In this paper we will give some applications of group theory. The first application makes use of the observation that computing in **Z** can be replaced by computing in $\mathbf{Z_n}$, if *n* is suficiently large. $\mathbf{Z_n}$ can be decomposed into a direct product of groups with prime power order, so we can do the computations in parallel in the smaller components. Group theory have interesting applications in the design of computer software, they result in computing techniques which speed up calculations considerably, one such example is bringing in this paper. Group theory is the main tool to study symmetries, revolution and many geometric transactions, this will be presented in this article and furthermore we will show intersting applications of group theory in chemistry.

Keywords: *Symmetry operation, isomorphic, group, permutation, molecule.*

INTRODUCTION.

We will see some applications of group theory. The firs application makes use of the observation that computing in Z can be replaced by computing in Z_n, and can be decomposed into a direct product of groups with prime power order, so we can do the computations in parallel in the saller components. We will look at permutation groups and apply these to combinatorial problems of finding the number of "essentially different" configurations, where configurationsare considered as "essentially equal" if the second one can be obtained from the first one, e.g., by a rotation or reflection

2 SUPPORT DEFINITIONS AND THEOREM.

Definition 2.1. *A group is a set G together with a binary operation* $\circ: G \times G \to G$ *on G with the following properties. We write* $g \circ h$ *instead of* $\circ(g, f)$.

(i) $\circ$ *is* ***associative****, i.e.,* $f \circ (g \circ h) = (f \circ g) \circ h$ *for all* $f, g, h \in G$.

(ii) *There exists a* ***neutral element*** $n \in G$, *i.e.,* $n \circ g = g \circ n = g$ *for all* $g \in G$.

(iii) *For every* $g \in G$ *there is some* $h \in G$ *with* $g \circ h = h \circ g = n$, *where* n *is the neutral element.*

Examples 2.2. The set D_n of all rotations and reflections of a regular n-gon consists of the n rotations id, a: = rotation by $360^o/n$ about the center, $a \circ a := a_2$ =rotation by $2\frac{360^o}{n}, \ldots, a^{n-1}$, and n reflections on the n "symmetry axes." If b is one of these reflections, then

$$D_n = \{id, a, a^2, \ldots, a^{n-1}, b, a \circ b =: ab, a^2b, \ldots, a^{n-1}b\}.$$

We can check that (D_n, $\circ$) is a group of order $2n$, called the dihedral group of degree n. We have $ba = a^{n-1}b$, so D_n is nonabelian if $n > 3$. If $n = 4$, for instance, D_n consists of the rotations by 0°, 90°, 180°, and 270°, and of the reflections on the dotted axes: $D_4 = \{id, a, a^2, a^3, ab, a^2b, a^3b\}$ and $ba = a^3b$.

Theorem 2.3. *Let (G, o) be a group.* ***(i)*** *If ~ is a congruence in (G, o), then the class [n] of the neutral element is a subgroup N of G with:* $g \circ m \circ g^{-1} \in N$ *for all* $m \in N$ *and* $g \in G$.

(ii) *Conversely, if* $N \leq G$ *fulfills (i), then* $g \sim_N h :\Leftrightarrow g \circ h^{-1} \in N$, *gives a congruence* $\sim_N$ *on* $(G, \circ)$.

Theorem 2.5 *(Lagrange's Theorem). If* $N \leq G$ *and G is finite, then* $|N|$ *is a divisor of* $|G|$. *More precisely,* $|N|G:N] = |G|$.

Theorem 2.6*(Principal Theorem on Finite Abelian Groups). Every finite abelian group is isomorphic to the direct product of groups of the type* Z_{p^k} *(p prime).*

Definition 2.7. The *center* C(G) *of a group is the set of all* $c \in G$ *such that* $g \circ c = c \circ g$ *for all* $g \in G$.

Theorem 2.8*(Chinese Remainder Theorem for Polynomials). Let* $(f_1, \ldots, f_r)$ *be distinct irreducible polynomials over* F_q *and let* $(g_1, \ldots, g_r)$ *be arbitrary polynomials over* F_q. *Then the system of congruences* $h \equiv g_i (mod f_i)$, $i = 1,2, \ldots, r$, *has a unique solution h modulo* $f_1 f_2 \ldots f_r$.

3. FAST ADDITION.

Group and ring theory have interesting applications in the design of computer software. They result in computing techniques which speed up calculations considerably. If we consider two numbers such as a = 37 and b = 56, it makes no difference whether we add them as natural numbers or as members of some Z_n with n sufficiently large, say n = 140 in our case. The only requirement is that **a+b < n**. We now decompose n canonically as $n = p_1^{t_1} p_2^{t_2} \dots p_n^{t_n}$. Theorem.2.6 shows that: $Zn \cong Z_{p_1}^{t_1} \oplus \dots \oplus Z_{p_n}^{t_n}$.

An isomorphism is given by $h: [x]_n \to \left([x]_{p_1^{t_1}}, \dots, [x]_{p_k^{t_n}}\right)$, where $[x]_m$ denotes the residue class of x modulo m. Surjectivity of h means that for all $y_1, y_2 \dots y_n \in Z$ can be found with $x \equiv y_1 (mod\ p_1^{t_1}), \dots, x \equiv y_k (mod\ p_n^{t_n})$, a result wich is known as the *Chinese Reminder Theoreme.* It is not hard to find this solution x explicitly. Similar to the proof of T.2.8, see [6] form $q_i = n p_i^{t_i}$. Because gcd $(p_i^{t_i}, q_i) = q_i$ has a multiplicative inverse r_i in $\boldsymbol{Z}_{p_i^{t_i}}$. Thus

$x := y_1 q_1 r_1 + \dots + y_n q_n r_n$, and x is unique modulo n.

A quick algorithm ("Garner's algorithm") can be found in (**[1]** p.176). The importance of this theorem lies in the fact that we can replace the addition of large natural numbers by parallel "small" simultaneous additions. We illustrate this by the example mentioned above:

$$n = 140 = 2^2 \cdot 5 \cdot 7,$$

$$a\{= 37 \to [37]_{140} \to ([37]_4, [37]_5, [37]_7)\}$$
$$+ b\{= 56 \to [56]_{140} \to ([56]_4, [56]_5, [56]_7)\} =$$

$$\Rightarrow a + b = ([1]_4, [3]_5, [2]_7)$$

Now we have to solve: $\equiv 1 (mod 4)\ ; x \equiv 3 (mod 5); x \equiv 2 (mod 7)$, by the method mentioned above. We get x = 93, hence 37 + 56 =93.

Of course, using this method does not make sense if we just have to add two numbers. If, however, some numbers are entered in a computer which has to work with them a great number of times, it definitely does make sense to transform the numbers to residue classes and to calculate in parallel in small Z_{p^t}'s . This avoids an exponential growth of the coefficients. Before we really adopt this method, we estimate the time we save by using it. Adding devices in computers consist of a great number of "gates." Each gate has a small number r of inlets ($r < 4$ is typical), and one outlet. Each gate requires a certain unit time (10^{-8} seconds, say) to produce the output.**[2]**.

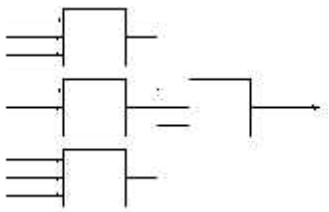
Fig.1.

Notation 3.1: For $x \in \boldsymbol{R}$, let $[x]$ be the smallest integer $\geq x$.

Theorem: 3.2. T*he time required to produce a single output essentially depending on m inputs by means of r-input gates is* $[\log_r m]$.

Here is a sketch for r=3, m=8.(*Fig 1*). We need $2=[\log_3 8]$ time units to produce the single output. If we add two m-digit binary numbers, we get $m + 1$ outputs; one can easily see that the last output (the "carry-over") depends on all inputs. So we get:

Theorem 3.3: *Usual addition of two m-digit binary numbers needs* $[\log_r 2m]$ *time units.*

Theorem 3.4: *Addition modulo n (i.e., addition in Zn) in binary form consumes* $[\log_r(2\log_2 n)]$ *time units.*

Theorem 3.5: *Addition of two (binary) numbers in Zn by the method described at the beginning of this section needs* $[\log_r(2[\log_2 n])]$ *time units.*

Here, n' is the greatest prime power in the decomposition of n. Hence we will choose n in such a way that n' is as small as possible. It is wise to fix n' and look for a large n.

Example. *3.6:* We want n' < 50 and can choose n in an optimal way as

$$n := 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$$

Now $n > 3 \cdot 10^{21}$ and n'=49. So we can add numbers with 21 decimal digits. If we choose $r = 3$, the method in *Theorem3.3* needs $[\log_3(2[\log_2(3 \cdot 10^{21})])] = [4.52] = 5$ time unite. With **3.5** we get (again with r=3). $[\log_3(2[\log_2 49])] = [2.26] = 3$ time unite.

Thus we can add nearly twice as fast.

4. POLYA'S THEORY OF ENUMERATION.

Groups of permutations (i.e., subgroups of the symmetric group S_M) were the first groups which were studied. The notion of an abstract group came about half a century later by Cayley in 1854. N. H. Abel and E. Galois, for instance, studied groups of permutations of zeros of polynomials. Moreover, it is a big understatement to say that one is "only" studying permutation groups. The following classical theorem tells us that all groups are—up to isomorphism—permutation groups, more precisely, every group can be embedded into a permutation group.

Theorem 4.1: (Cayley's Theorem). *If G is a group, then $G \hookrightarrow S_G$.*

Proof. The map $h: G \to S_G \; ; \; g \mapsto \varphi_g$ with $\varphi_g: G \to G; x \mapsto gx$ does the embedding job: $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$ ensures that h is a homomorphism, and $Kerh = \{g \in G / \varphi_g = id\} = \{1\}$, so h is a monomorphism. It follows that every group of order $n \in \mathbb{N}$ can be embedded in S_n. In writing products $\pi\sigma$ of permutations $\pi, \sigma \in S_n$ we consider π and σ to be functions. Hence in $\pi\sigma$ we first perform σ, then π. □

Definition 4.2 : *$\pi \in S_n$ is called a cycle of length r if there is a subset $\{i_1 \ldots i_r\}$ of $\{1,\ldots,n\}$, with $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_r) = i_1$ and $\pi(j) = j, \forall j \notin \{i_1 \ldots i_r\}$. We will then write $\pi = (i_1, i_2, \ldots, i_r)$. Cycles of length 2 are called transpositions. Cycles of length 1 are equal to the identity permutation, so they are often omitted.*

Example 4.3: ***(i)*** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2,4) = (4,2) = (1)(2,4)(3)$ is a transposition in S_5.

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix} = (2,5,3,4)$ is a 4-cycle in S_5.

(iii) $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

So every $\pi \in S_3$ is a cycle. This is not true any more from S_4 upward. But we shall see in **4.6** that every permutation in S_n is a product of cycles.

Definition 4.4: *For $\pi \in S_n$ let $W_\pi := \{i \in \{1 \ldots n\} / \pi(i) \neq i\}$ be the domain of action of π.*

The following result shows that permutations with disjoint domains of action commute.

Theorem 4.5*: If $\pi, \sigma \in S_n$ me $W_\pi \cap W_\sigma = \emptyset$ then $\pi\sigma = \sigma\pi$.*

Theorem 4.6*: Every $\pi \in S_n$ can be written as a product of cycles with disjoint domains of action. This decomposition is unique up to the arrangement of the cycles and is called "**canonical**".*

Example 4.7. Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 7 & 4 & 3 & 8 \end{pmatrix} \in S_8$.

π moves 1 into 2 and 2 into 1; this gives the first cycle (1,2). Next we observe that 3 is transferred into 5, 5 into 7, 7 into 3; second cycle: (3,5,7). 4 and 6 are transposed, which yields (4, 6) as the third cycle. Finally, 8 is left fixed. Hence π=(1,2)(3,5,7)(4,6)(8). By 4.5, there is no reason to worry about the order of these cycles. Without loss of generality we assume that the cycles in a canonical decomposition are ordered in such a way that their length is not decreasing. This gives, for instance, $\pi = (8)(1.2)(4.6)(357)$ in 4.7**.** Two canonical decompositions are called similar if the sequences of the lengths of the cycles involved are equal. Hence $\pi = (8)(1.2)(4.6)(357)$ and $\sigma = (6)(1.3)(2.4)(587)$ are different elements of S_8 having similar decomposition. These considerations prove very useful in looking at the structure of S_n.

Let $n \in N$. A partition of n is a sequence $(a_1, a_2, .., a_s) \in N^s$ with $s \in N, a_1 \leq a_2 ... \leq a_s$ and $a_1 + a_2 + ... + a_s = n$. Let $P(n)$ be the number of all different partitions of n. We give a few values: Let C(G):={c ∈ G| *cg = gc*, for all $g \in G$} denote the center of G, as in **2.7**.

Theorem 4.8:

(i)*If $\pi\sigma \in S_n$, then $\sigma\pi\sigma^{-1}$ can be obtained from the canonical decomposition of ® by replacing every i in its cycles by $\sigma(i)$.*

(iii) *Two cycles are conjugate if and only if they are of the same length.*

(iii) *$\pi_1, \pi_2 \in S_n$ are conjugate if and only if they have similar canonical decompositions.*

(iv) *P(n) is the class number of S_n.*

(v) *For all $n \geq 3$, $C(S_n) = \{id\}$ and $C(S_n) = S_n$, for n =1,2.*

Proof. ***(i)*** If $\pi = \xi_1\xi_2 \dots \xi_m$ is the canonical decomposition of π into cycles ξ_i, then $\sigma\pi\sigma^{-1} = (\sigma\xi_1\sigma^{-1})(\sigma\xi_2\sigma^{-1}) \dots (\sigma\xi_m\sigma^{-1})$ so that it suffices to look at a cycle ξ. Let $\xi = (i_1, \dots, i_r)$. If $1 \le k \le r-1$, then $\xi(i_k) = i_1$ whence $(\sigma\xi\sigma^{-1})\big(\sigma(i_k)\big) = \sigma(i_1)$. If $i \notin W_\xi$ then $\xi(i) = i$, and so $(\sigma\xi\sigma^{-1})\big(\sigma(i)\big) = \sigma(i)$. Thus $\sigma\xi\sigma^{-1} = \big(\sigma(i_1), \dots, \sigma(i_r)\big)$. ***(ii), (iii),*** and ***(iv)*** now follow from ***(i). (v)*** Let $\pi \in S_n$, $\pi \neq id$. Then there is some i with $\pi(i) \neq i$. If $n \ge 3$ then there is some $k \in \{1, \dots, n\}$ with $i \neq k \neq \pi(i)$. By (i) we get $\pi(i,k)\pi^{-1} \neq \big(\pi(i), \pi(k)\big) \neq (i,k)$, whence $\pi \notin C(S_n)$ Hence $C(S_n) = \{id\}$ for $n > 3$. Since S_1 and S_2 are abelian, $C(S_n) = S_n$ in these cases.

Since $(i_1,i_2,\dots,i_r) = (i_1,i_r)(i_1,i_{r-1})\dots(i_1,i_2)$ we get from **4.6:**

Theorem 4.9. *Every permutation is a product of transpositions.*

Incontradiction to **T.4.6,** this type of decomposition is not unique.

Definition 4.10: For $\pi \in S_n$, $\operatorname{sign}(\pi) = \prod_{i>j} \frac{\pi(i)-\pi(j)}{i-j}$ *is called the signature of* π.

Theorem 4.11: Let $n > 1$: ***(i)*** sing: $S_n \to (\{1, -1\})$ *is an epimorphism.*

(ii) *If* $\pi = \tau_1, \tau_2 \dots \tau_s$, *where all* τ_i *are transpositions, then* $sig(\pi) = (-1)^s$.

(iii) *If* $\pi = \xi$ *is a cycle of length k, then* $sign(\xi) = (-1)^{k-1}$.

(iv) *If* $\pi = \xi_1\xi_2 \dots \xi_n$ *is a canonical decomposition of* ® *into cycles of length* $k_1 \dots k_r$ *respectively, then* $sign(\pi) = (-1)^{k_1+k_2\dots+k_r-r}$

(v) $A_n := Ker\ sign = \{\pi \in S_n / sign(\pi) = 1\}$, *is a normal subgroup of* S_n.

(vi) $[S_n : A_n] = 2$, so $|A_n| = \frac{n!}{2}$.

Proof. ***(i)*** For $\pi, \sigma \in S_n$ we get: $sign(\pi\sigma) = \prod_{i>j} \frac{\pi(\sigma(i))-\pi(\sigma(j))}{i-j} = \prod_{i>j} \frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)} \cdot \frac{\sigma(i)-\sigma(j)}{i-j}$

$$= \Big(\prod_{\sigma(i)>\sigma(j)} \frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)}\Big)\Big(\prod_{i>j} \frac{\sigma(i)-\sigma(j)}{i-j}\Big) = sing(\pi)sing(\sigma).$$

For the last equation but one observe that for i<j and $\sigma(i) > \sigma(j)$ we have:

$\frac{\pi(\sigma(i))-\pi(\sigma(j))}{\sigma(i)-\sigma(j)} = \frac{\pi(\sigma(j))-\pi(\sigma(i))}{\sigma(j)-\sigma(i)}$. Obviously, the signature can take values in {1,-1} only. Because sign(r) = -1 for every transposition, Imsign = {1,-1}. ***(ii)*** follows from (i) since $sign(\pi) = -1$ for every transposition. ***(iii)*** is a special case of (ii) using the decomposition before **4.9.** ***(iv)*** If $\pi = \xi_1 \dots \xi_r$ then by (ii) $sign(\pi) = (sign(\xi_1)) \dots (sign(\xi_r)) = (-1)^{k_1-1} \dots (-1)^{k_r-1}$. ***(v)*** The kernel of every homomorphism is a normal subgroup due to **2.4**. ***(vi)*** follows from **2.5.**

Definition 4.12: $A_n = \{ \pi \in S_n \mid \text{sign } (\pi) = 1\}$ *is called the* ***alternating group****. Permutations in* A_n *are also called even.*

Note that A_3 is abelian because $|A_3| = \frac{3!}{2} = 3$ □ $A_3 \cong \mathbb{Z}_3$. But A_n is nonabelian if $n \geq 4$. We list several important properties of these alternating groups (without proofs).

Theorem 4.13:

(i) A_n *is the subgroup of* S_n *generated by the 3-cycles.*

(ii) A_n *is not simple, since it has a normal subgroup isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}_2$. *But* A_4, *a group of order 12, has no subgroup of order 6.*

(iii) *For n* ≥*5,* A_n *is simple and nonabelian.* (*This is the deep reason for the fact that there cannot exist "solution formulas" for equations of degree* ñ 5.) *Also,* A_5 *has order 60 and is the smallest nonabelian simple group.*

(iv) $C(A_n) = \{id\}$ *for* $n \geq 4$; $C(A_n) = A_n$ *for* n □ {1,2,3}.

(v) $\bigcup_{n \square N} A_n = A$ *is an infinite (nonabelian) simple group.*

Now suppose that X is a set and $G \geq S_X$. Then every $\pi \in G$ can be thought of as being an operator acting on X by sending $x \in X$ into $\pi(x)$. We are interested in what happens to a fixed $x \in X$ under all $\pi \in G$.

Theorem and Definition 4.14: Let $G \leq S_X$ *and* x, y □ X. *Then*:

(i) x *and* y *are called G-equivalent (denoted by* $x \sim_G y$*) if there is a* $\pi \in G$ *with* $\pi(x) = y$

(ii) $\sim_G$ *and G is an equivalence relation on X.*

(iii) *The equivalence classes Orb(x) =* $\{y \square X / x \sim_G Y\}$ *are called orbits (of G on X)*

(iv) *For every $x \in X$, $Stab(x)=\{\pi \in G / \pi(x) = x\}$ is a subgroup of G, called the stabilizer of x. As in 2.3, we have for all $\pi, \tau \in G$: $\pi \sim_{stab(x)} \tau \Leftrightarrow \pi\tau^{-1} \in Stab(x)$.*

Example 4.15:

(i) Let G be a group, $S \leq G$ dhe $X = G$. By 4.1, S can be considered as a subgroup of $S_G = S_X$. If $g \in G$ the orbit $Orb(g) = Sg$ (the right coset of g with respect to S) and $Stab(g) = \{s \in S \mid sg = g\} = \{1\}$.

(iii) ***Let G be a group, X = G and Inn $G \leq S_G$ ku, Inn G = $\{\varphi_x / x \in G\}$ is*** the set of all inner automorphisms. $\varphi_x: G \to G;\ g \mapsto xgx^{-1}$.

Then for all $g \in G$ we get $Orb(g) = \{\varphi_x(g) / \varphi_x \in InnG\}$ = conjugacy class of g and Stab(g)=$\{\varphi_x \in$ Inn G $\mid x\,g\,x^{-1}=\varphi_x(g) = g\}=\{\varphi_x \in InnG \mid xg = gx\}$.

(iv) ***(iii)*** Let Y be a set. $\mathbb{Z}_n$ operates on $X = Y^n$ by "shifting the components cyclically": if $k \in \mathbb{Z}_n$, let $\pi_k: (y_1,\dots,y_n) \to (y_k, y_{k+1},\dots,y_{k-1})$. For $n = 3$, for instance, the orbit of (y_4, y_2, y_3) is $\{(y_1, y_2, y_3),(y_2, y_3, y_1),(y_3, y_1, y_2)\}$ and $Stab(y_1, y_2, y_3) = \mathbb{Z}_3$ if $y_1 = y_2 = y_3$ and $=\{0\}$ otherwise.

These concepts turn out to be very useful in several applications. As an example, we mention an application to chemistry, due to G. Polya.

Example 4.16: From the carbon ring (a) we can obtain a number of molecules by attaching hydrogen (H^-) atoms or CH_3-groups in the places (1)—(6) in (b). For instance, we can obtain xylole (c) and benzene (d) as shown in figure 4.1**.** Obviously, (c') gives xylole as well, as shown in figure 4.2.

The following problem arises: How many chemically different molecules can be obtained in this way? Altogether, there are 26 possibilities to attach either H or CH_3 in (1)—(6). But how many attachments coincide chemically.

In order to solve this problem we can employ the following result of Burnside,

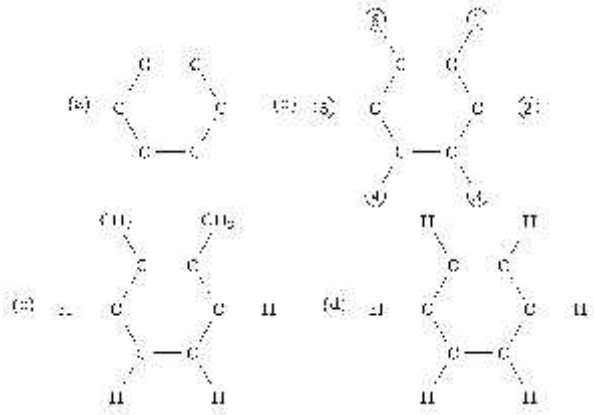

Fig.4.1

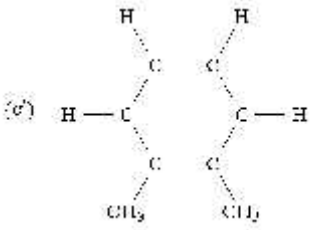

Fig.4.2

Cauchy, and Frobenius.

Theorem 4.17: (*Burnside's Lemma*) *Let X be finite and $G < S_X$. For every $x \in X$, $|Orb(x)|$ divides $|G|$, and the number n of different orbits of X under G is given by:*

$n = \frac{1}{|G|}\sum_{g\in G}|Fix(g)| = \frac{1}{|G|}\sum_{x\in X}|Stab(x)|$, *where* $Fix(g) := \{x \in X / g(x) = x\}$.
Also $[G:Stab(x)] = [Orb(x)]$, *and hence* $|Stab(x)||Orb(x)| = |G|$.

Proof. First we compute $|Orb(x)|$. Let $x \in X$

and $f: Orb(x) \to G|_{\sim Stab(x)};\ g(x) \to gStab(x)$.

Since: $g_1(x) = g_2(x) \Leftrightarrow g_2^{-1}g_1(x) = x \Leftrightarrow g_2^{-1}g_1 \in Stab(x) \Leftrightarrow g_1 \sim_{Stab(x)} g_2$

$\Leftrightarrow g_1Stab(x) = \Leftrightarrow g_2Stab(x)$. f is well defined.

Obviously f is bijective and hence $|Orb(x)| = |G/\sim stab(x)| = [G:Stab(x)]$,

so $|Orb(x)|$ divides $|G|$.

Now we compute the cardinality of $\{(g,x) | g \in G, x \in X, g(x) = x\}$ in two different ways:

$$\sum_{x\in X}|Stab(x)| = |\{(g,x) | g \in G, x \in X, g(x) = x\}| = \sum_{g \square G}|Fix(g)|.$$

Let us choose representatives $x_1, \ldots, x_n$ from the n orbits. Since $Orb(x) = Orb(y)$ implies:

$$|Stab(x)| = \frac{|G|}{|G:Stab(x)|} = \frac{|G|}{|Orb(x)|} = \frac{|G|}{|Orb(y)|} = \frac{|G|}{|G:Stab(y)|} = |Stab(y)|,$$

we get $\sum_{x\in X}|Stab(x)| = \sum_{i=1}^{n}|Orb(x_i)| \cdot |Stab(x_i)| = \sum_{i=1}^{n}\frac{|G|}{|Stab(x_i)|} \cdot |Stab(x_i)| = n \cdot |G|$.

Now we use 4.17 for our problem 4.16.

Example 4.16(continued): Letus denote the said 2^6 = 64 attachments by $\{x_1,..,x_{64}\} =: X$. Attaching x_i and x_j will yield the same molecule if and only if x_j can be obtained from x_i by means of a symmetry operation of the hexagon (1) - (6), i.e., by means of an element of D_6, the dihedral group of order 12 (see 2.2). Hence the number *n* of different possible molecules we are looking for is just the number of different orbits of X under D_6. From 4.17 we get:

$n = \frac{1}{|D_6|}\sum Fix(g) = \frac{1}{12}\sum Fix(g)$. Now id fixes all elements, whence $|Fix(id)| = 64$. A reflection *r* on the axis (1)–(4) in (b) fixes the four attachments possible in (1) and (4) and also the four other possible attachments in (2) and (3) n if they are the same as those in (6)and(5), respectively. Hence $|Fix(r)| = 4 \cdot 4 = 16$, and so on. Altogether we get $n = \frac{1}{12}156 = 13$ different molecules. Observe that reflections in space usually yield molecules with different chemical properties. We see that this enumeration can be applied to situations where we look for the number of possible "attachments". The results in **4.17** shows that *n* is the arithmetic mean of |Fix(g)|'s and |Stab(*x*)|'s in G. We can improve the formula in **4.17** by the remark that if g_1 and g_2 are conjugate, then $|Fix(g_1)| = |Fix(g_2)|$. Of course, this only helps in the nonabelian case. So we get.

Theorem 4.18: L*et X be finite and G < Sx. Let* $g_1,...,g_r$ *be a complete set of representatives for the conjugacy classes in G/~ and let* k_i *be the number of elements conjugate to* g_i. *Then the number n of orbits of X under G is given by:* $n = \frac{1}{|G|} \cdot (k_1|Fix(g_1)| + \cdots + k_r|Fix(g_r)|)$.

We give a simple example in which we can use our knowledge about the conjugacy classes of S_3.

Example 4.19: Find the number *n* of essentially different possibilities for placing three elements from the set {A, B, C, D, E} at the three corners 1, 2, 3 of an equilateral triangle such that at least two letters are distinct**.**

*Solution***:** G = S_3 acts on {1,2,3} as the group of symmetries. Take, in the language of Theorem **4.18.** $g_1 = id$, $g_2 = (1,2)$, $g_3 = (1,2,3)$. Then $k_1 = 1$, $k_2 = 3$, $k_3 = 2$. Now X contains all triples (a, b, c) such that at least two of the three elements a, b, c are distinct. Hence: |x|=5(4+4·5)=120; |Fix(g_1)|=120; |Fix(g_2)|=20 since g_2 fixes precisely all (a, a, b). $|F_i x(g_3)|$=0 since g3 fixes exactly all (a, a, a); these combinations are not allowed.

Hence Theorem **4.18** gives us: $n = \frac{1}{6}(120+60+0) = 30$.

The results **4.17** and **4.18** are indeed useful for Example **4.19**. A direct treatment of **4.19** would require an examination of all $\binom{120}{2} = 7140$ pairs of attachments with respect to being essentially different. There might, however, remain quite a bit to do in **4.17** and **4.18**, especially if G is big and if there are many conjugacy classes. So we might still be dissatisfied with what we have accomplished so far. Also, we still have no tool for finding a representative in each class of essentially equal attachments.

Definition 4.20: *Suppose that* $\pi \in S_n$ *decomposes into* j_1 *cycles of length 1,* j_2 *cikle cycles of length2,...,* j_n *cycles of length n according to* **4.6** *(we than have* $1j_1+2j_2+\ldots+nj_n = n$*). We than call* $(j_1, j_2 \ldots j_n)$ *the cycle index of* π*. If* $G \leq S_n$ *than* $Z(G) = \frac{1}{|G|}\sum x_1 j^1 x_2^{j_2} \ldots x_n^{j^n} \in \mathbb{Q}[x_1 \ldots x_n]$ *is called the cycle index polynomial of G.*

Example 4.21: In S_3, we have one permutation (namely id) with cycle index (3,0,0), three permutations ((1,2),(1,3),(2,3)) with cycle index (1,1,0) (since (1,2) = (3)(1,2) and so on), and two permutation with cycle index (0,0,1). Hence ; $Z(S_3) = \frac{1}{16}(x_1^3+3x_1x_2+2x_3)$.

Definition 4.22: *Let F be a set of r figures* $f_1 \ldots f_r$ $m \in \mathbb{N}$*. If* $G \leq S_m$ *then G can be thought of as a permutation group on* F^m *via* $g(f_1 \ldots f_m) = (f_{g(1)} \ldots f_{g(m)})$*; so G is considered as a subgroup of* S_{r^m}.

Theorem 4.23 (*Pòlya's Theorem*): *In the situation of* ***4.22****, the number n of different orbits on* $X = F^m$ *under G is given by* $n = Z(G)(r,r,...,r)$. *(This equals the value of the induced polynomial function of Z(G) at* $x_1 = r_1 ... x_m = r$*).*

Proof. If $g \in G$, then $(f_1 \dots f_m) \in Fix(g)$ if and only if all f_i, where i runs through the elements of a cycle of g, are equal. Hence $|Fix(g)| = r^{j_1+j_2+\cdots+j_m}$, where $(j_1, j_2, \dots, j_m)$ is the cycle indes of g. Now Burnside's Theorem **4.17** gives us the desired result

$n = \frac{1}{|G|}\sum_{g \square G}|Fix(g)| = \frac{1}{|G|}\sum_{g \square G} r^{j_1} r^{j_2} \dots r^{j_m}$. If we actually want to find a representative in each orbit, we can simply try to find one by brute force. Otherwise, more theory is needed. For a proof and a detailed account of the following, see[3] or [4].

Theorem 4.24(*Redfild- Pòlya Theorem*): *Recall the situation in* ***4.22****. Let us "invent" formal products of the figures* $f_1 \dots f_r$ *and write* f^2 *for* $f \cdot f$ *etc. If we now substitute* $f_1 + f_2 + \dots + f_r$ *for* x_1, $f_1^2 + \dots + f_r^2$ *for* x_2, *and so on, in Z(G), then by expanding the products we get sums of the form* $n_{i_1 \dots i_r} f_1^{i_1} f_2^{i_2} \dots f_r^{i_r}$ *with* $i_1 + i_2 + \dots i_r = m$. *This means that there are precisely* $n_{i_1 \dots i_r}$ *orbits in* $X = F^m$ *under G such that each orbit-tuple consists of precisely* i_1 *figures* f_1, i_2 *of the* f_2 *etc.*

Example 4.16 (revisited). Let f_1, be the H-group and f_2 the $CH_3 -$ groups. If we expand as in 4.24, we get: $\frac{1}{12}((f_1 + f_2)^6 + 3(f_1 + f_2)^2(f_1^2 + f_2^2)^2 + 4(f_1^2 + f_2^2)^3 + 2(f_1^3 + f_2^3)^2 + 2(f_1^6 + f_2^6)) = f_1^6 + f_1^5 f_2 + 3f_1^4 f_2^2 + 3f_1^3 f_2^3 + 3f_1^2 f_2^4 + f_1 f_2^5 + f_2^6$.

Hence there are:

• one possibility to give only H-atoms;

• one possibility to give five H-atoms and one CH3-molecule;

• three possibilities to take four H-atoms and two CH3-molecules;

and so on. In order to find a complete set of representatives, we have to collect instances for each of these (altogether 13) possibilities.

Of course, if we replace all f_i by 1, we get Polya's Theorem **4.4** as acorollary of **4.6**. Even after the discovery of these two powerful results, they were not widely known. Let us consider a final example.

Example 4.27: Let us call two truth functions (or switching functions) $f_1, f_2: \{0,1\}^n \to \{0,1\}$ *essentially similar* if, after a suitable relabeling $(i_1, \dots, i_n)$ of $(1, \dots, n)$ we have $f_1(b_1, \dots, b_n) = f_2(b_{i_1}, \dots, b_{i_n})$ for all $(b_1, \dots, b_n) \in \{0,1\}^n$. For switching theory, this means that the corresponding switching circuits of f_1 and f_2 "work identically" after a suitable permutation of the input wires.

Problem. How many essentially different such functions exist?

History. This problem was explicitly carried out and solved by means of a gigantic computer program in 1951 for $n = 4$. The total number of these functions is $2^{2^4} = 65\,536$, and 3984 essentially different functions were found.

Solution. Our solution is rather immediate. The group G is basically S_n. However, care must be taken, since G acts as described above on $\{0,1\}^n$ and not on {1,...,n}. If we take n = 4, for instance, the effect of g = (1,2)(3, 4) on the quadruple (*a,b,c,d*) e $\{0,1\}^4$ 4 is given by (*b,a,d,c*). Obviously, Fix(g) consists of precisely those functions which are constant on each cycle of g. In our case forg = (1, 2)(3, 4) we get $|Fix(g)| = 2 \cdot 2 = 4$. Now S_4 decomposes into the following conjugacy classes (see **4.8**): ***(i)*** id; ***(ii)*** six 2-cycles; ***(iii)*** three products of two 2-cycles; ***(iv)*** eight 3-cycles; ***(v)*** six 4-cycles. Now ***(i)*** fixes all 16 combinations (*a,b,c,d*), yielding x_1^{16} in the cycle index polynomial. Also, (ii) contributes $6x_1^8x_2^4$ since for instance (1, 2) yields the four 2-cycles ((*0,1, c, d*), (*1, 0, c, d*)) and fixes all (*0, 0, c, d*) and (*1,1, c, d*), thus producing eight 1-cycles and four transpositions, and so on. The cycle index polynomial for G acting on $\{0,1\}^4$ is then given by $Z(G) = \frac{1}{24}(x_1^{16} + 6x_1^8x_2^4 + 3x_1^4x_2^6 + 8x_1^4x_3^4 + 6x_1^2x_2x_4^3)$. Hence $x_1 = x_2 = x_3 = x_4 = 2$ gives 3984 equivalence classes of functions from $\{0,1\}^4$ to $\{0,1\}$.

REFERENCES

[1] Geddes, R. O., S. R. Czapor & G. Labahn (1993). Algorithms for Computer Algebra. Dordrecht: Kluwer.

[2] Dornhoff, L. & F. E. Hohn (1978). Applied Modern Algebra. New York: Macmillan.

[3] Stone, H. S. (1973). Discrete Mathematical Structures and Their Applications. Chicago: Scientific Research Association.

[4] Kerber, A. (1991). Algebraic Combinatorics via Finite Group Actions. Mannheim: Bibliographisches Institut.

[5] Gilbert (1976, p. 144) and cf. Exercise 12. Gilbert, W. J. (1976). Modern Algebra with Applications. New York: Wiley.

[6] Rudolf Lidl, Gunter Pilz, Applied Abstract Algebra, Second Edition(1998).