

Some Groups in Geometry and in Number Theory

B. Waldmüller

12th September 2002

These notes were made for your convenience. They are not self-contained, and they are written in a very German English. I apologize for any trouble.

For further reading you might use the books 'Groups and Symmetry' by M. A. Armstrong or 'The Little Book on Big Primes' by P. Ribenboim, both published by Springer-Verlag. If there are any questions, feel free to contact me: bernhard@waldmuellers.de

Contents

1	Geometry	1
1.1	The Group T of Symmetries of the Tetrahedron	1
1.2	A Subgroup of T , Stabilizers and Orbits	2
2	Number Theory	3
2.1	Introduction	3
2.2	Quadratic Residues	4
2.3	The Miller-Rabin-Test	4

1 Geometry

1.1 The Group T of Symmetries of the Tetrahedron

There are mappings of the space onto itself, which preserve the distance of any two points - like rotations, translations and reflections.¹ Let T be the set of all of these mappings, which map a given tetrahedron onto itself; they are called the symmetries of the tetrahedron.

We name the vertices of the tetrahedron 1, 2, 3 and 4. Look at the straight line

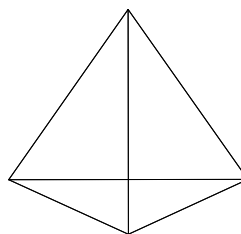


Figure 1: tetrahedron

through 4 and the center of the triangle 123. The rotation of 120° about this line

¹These mappings are called isometries.

maps the tetrahedron onto itself. We name this rotation a , and we write

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1, 2, 3)(4) = (1, 2, 3) \quad (1)$$

Now look at the plane through 1 and 4 perpendicular to the edge 23. The reflection at this plane maps the tetrahedron onto itself. We name this reflection r , and we write

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (1)(2, 3)(4) = (2, 3) \quad (2)$$

Now we can write down all the symmetries we find like we wrote down a and r , and we hope that no symmetries are missing. But this is not the end of the story. A most important fact is, that we can calculate in T : If we apply first a and then r , we get another element of T , denoted by $a \cdot r$:

$$a \cdot r = (1, 2, 3) \cdot (2, 3) = (1, 3) \quad (3)$$

The product² is the reflection at the plane perpendicular to the edge 13 through the vertices 2 and 4. It is the existence of this product defined for pairs of elements of T , that makes T a group. The associative law

$$x(yz) = (xy)z \quad (4)$$

holds for all $x, y, z \in T$, there is an element $e \in T$ such that

$$ex = xe = x \quad (5)$$

for all $x \in T$, and for every $x \in T$ there is an element $x^{-1} \in T$, such that

$$xx^{-1} = x^{-1}x = e \quad (6)$$

Thus the multiplication in T behaves like the multiplication in the positive rationals. But be cautious: the multiplication in T is not commutative! So $ar \neq ra$ in T .

1.2 A Subgroup of T , Stabilizers and Orbits

The subset U of all elements of T , which map the vertex 4 to itself is a group itself: the product of two symmetries, which do not move 4, does not move 4. This subgroup U is called the stabilizer of 4 in T , and it is usually denoted by T_4 . There are elements in U , which map 1 to 2 and 2 to 3. The U -orbits of $\{1, 2, 3, 4\}$ are $\{1, 2, 3\}$ and $\{4\}$.

In T itself there is an element, which maps 4 to 1, say

$$b = (1, 4)(2, 3) \quad (7)$$

But there are more elements in T , which map 4 to 1. For every $u \in U$ we have

$$4ub = 4b = 1 \quad (8)$$

And vice versa, if $4x = 1$ for $x \in T$, then is $4xb^{-1} = 1b^{-1} = 4$. That means $xb^{-1} = u \in U$, $x = ub$ for a $u \in U$. There are exactly $|U|$ elements x in T with $4x = 1$, and these are the elements of the set

$$Ub := \{ub \mid u \in U\} \quad (9)$$

²We usually omit the dot \cdot .

There are, too, elements $c = (2, 4)(1, 3)$ and $d = (3, 4)(1, 2)$ in T , and the elements in T , which map 4 to 2, are exactly the $|U|$ elements of Uc , while the elements of T , which map 4 to 3, are exactly the $|U|$ elements of Ud . Now let $x \in T$. If $4x = 4$ holds, then $x \in U$. If $4x = 1$ holds, then $x \in Ub$. If $4x = 2$ holds, then $x \in Uc$, and if $4x = 3$ holds, then $x \in Ud$. So every $x \in T$ belongs to exactly one of the sets U, Ub, Uc, Ud , and

$$|G| = |U| + |Ub| + |Uc| + |Ud| = 4 \times |U| \quad (10)$$

This argument is a very typical argument from group-theory. By this method one can prove the following theorems:

Theorem 1 *Let G be a finite group of mappings of a set M onto M , and $m \in M$. Then the size $|G|$ of G is the product of the size $|G_m|$ of the stabilizer G_m of m in G and the size $|mG|$ of the orbit mG of m .*

Theorem 2 (Lagrange) *If G is a finite group and U is a subgroup of G , then the size $|U|$ of U divides the size $|G|$ of G .*

Now let us use theorem 1 to count the elements of T . The T -orbit of 4 is $\{1, 2, 3, 4\}$, and the stabilizer of 4 in T is $T_4 = U$. Therefore $|T| = |U| \times 4$. The U -orbit of 1 is the set $\{1, 2, 3\}$ of order 3, and the stabilizer U_1 of 1 in U has size 2. Therefore $|U| = 2 \times 3 = 6$ and $|T| = 6 \times 4 = 24$.

Prove, that the size of the group O of symmetries of a given cube is 48! And the picture shows, that T is a subgroup of O .

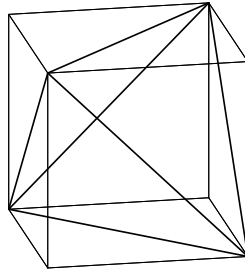


Figure 2: A tetrahedron contained in a cube

2 Number Theory

2.1 Introduction

In this section p is an odd prime. If we divide an integer z by p , we get a remainder in $\{0, 1, \dots, p-1\}$. We write \bar{z} for this remainder. Let

$$E := \{\bar{z} \mid p \text{ does not divide } z\} \quad (11)$$

We define a multiplication in E by $\bar{x} \cdot \bar{y} := \overline{xy}$ for $\bar{x}, \bar{y} \in E$. Now E is a group, its size is $|E| = p-1$.

Theorem 3 *Let $\bar{z} \in E$, and let s be the smallest number with $\bar{z}^s = \bar{1}$. Then $\{\bar{z}, \bar{z}^2, \bar{z}^3, \dots, \bar{z}^s\}$ is a subgroup of E . Its order is s , and therefore s divides $p-1$.*

Theorem 4 (Fermat's little theorem) *The prime p divides $a^{p-1} - 1$ for every integer a prime to p .*

Theorem 5 *The group E is cyclic, that means, there is an element $\bar{x} \in E$, such that $E = \{\bar{x}, \bar{x}^2, \bar{x}^3, \dots, \bar{x}^{p-1}\}$.*

We omit the proof.

2.2 Quadratic Residues

We call $\bar{x} \in E$ a quadratic residue, if there is $\bar{y} \in E$ such that $\bar{x} = \bar{y}^2$. The set Q of quadratic residues in E is

$$Q = \{\bar{x}^2, \bar{x}^4, \bar{x}^6, \dots, \bar{x}^{p-1}\}$$

where \bar{x} is a generator of the cyclic group E (see theorem 5). Of course, Q is a subgroup of E , the product of squares is a square. Now take $\bar{y}, \bar{z} \in E$, neither \bar{y} nor \bar{z} being an element of Q . You will find, that $\bar{y}\bar{z} \in Q$!

Let us prove, that $\bar{y}\bar{z} \in Q$ for all $\bar{y}, \bar{z} \in E$ such that $\bar{y}, \bar{z} \notin Q$. We have $|E| = |Q| \cdot 2$. None of the elements of $Q\bar{y}$ are elements of Q for $\bar{y} \notin Q$. But $|Q\bar{y}| = |Q|$, therefore we have $E = Q \cup Q\bar{y}$. But this means, that our \bar{z} is an element of $Q\bar{y}$. It follows, that $\bar{z} = \bar{w}\bar{y}$ for a $\bar{w} \in q$, and $\bar{y}\bar{z} = \bar{y}\bar{w}\bar{y}$ is a square in E .

2.3 The Miller-Rabin-Test

How can we see, whether a given number N is a prime? For big numbers this question is a very difficult one. There is a test, called the Miller-Rabin-test, which gives two possible answers: (1) N is composite, (2) N is likely a prime. The test is based on the following theorem on odd primes p .

Theorem 6 *Let p be an odd prime. We write $p - 1 = 2^s \cdot r$ with r an odd number. Then we have:*

For every integer y prime to p one of the following conditions hold:

- $\bar{y}^r = \bar{1}$
- $(\bar{y})^{r2^i} = \overline{p-1}$ for a number $i \in \{0, 1, \dots, s-1\}$

The test works as follows. Choose at random a number $y \in \{3, \dots, N-1\}$ and calculate the *g.c.d.* of y and N . If the *g.c.d.* is greater than 1, we found a divisor of N , and N is composite. If not, we test whether \bar{y} fulfills the statement of the theorem. If not, we know, that N is not a prime. Unfortunately, the number N might be composite, but our \bar{y} fulfills the statement of the theorem. But if N is composite, at most $1/4$ of the $y \in \{3, \dots, N-1\}$ fulfill the statement of the theorem. You test several y , say, 10. If N is composite, the probability, that all 10 chosen numbers fulfill the statement of the theorem, is at most $(1/4)^{10}$, and that is a small value.

I do not give an outline of the proof in these notes. If there is enough time, we shall discuss the proof.