Topology and statistics of formulae of arithmetics

V. I. Arnol’d

Abstract. This paper surveys some recent and classical investigations of geometric progressions of residues that generalize the little Fermat theorem, connect this topic with the theory of dynamical systems, and estimate the degree of chaotic behaviour of systems of residues forming a geometric progression and displaying a distinctive mutual repulsion. As an auxiliary tool, the graphs of squaring operations for the elements of finite groups and rings are studied. For commutative groups the connected components of these graphs turn out to be attracting cycles homogeneously equipped with products of binary rooted trees, the algebra of which is also described in the paper. The equipping with trees turns out to be homogeneous also for the graphs of symmetric groups of permutations, as well as for the groups of even permutations.

Contents

Introduction 637
§1. Fermat–Euler dynamical system 638
§2. Are the residues of the elements of a geometric progression random? 641
§3. Topology of the squaring operation 644
§4. Algebra of rooted trees 645
§5. Graphs of squaring in permutation groups 648
§6. Homogeneity of the monads of all finite groups 650
§7. Modular topology of the Kepler cubes 652
§8. Kepler cubes and Hamiltonian subgroups 655
§9. Riemann surface of heptagons and its Kepler cubes 658
§10. Statistics of the Fermat–Euler periods 663
Bibliography 663

Introduction

Not only curves and surfaces but also formulae and theories can be objects of topology.

In studying the arithmetics of quadratic forms (and relations to the de Sitter relativistic universe), I recently discovered, on the one hand, the topological nature of a large series of phenomena in number theory and, on the other hand, some strange statistical properties of the simplest objects of the theory.

AMS 2000 Mathematics Subject Classification. Primary 11B50, 11K99; Secondary 37A45, 05C05.
Although in many cases these statistical properties and topological phenomena remain experimental facts (confirmed only by several millions of observations) rather than theorems, I decided to tell about some of them here, all the more so because I have been able to formulate and prove a small number of them in the form of mathematical theorems (see [1]–[5]).

§ 1. Fermat–Euler dynamical system

The simplest essentially topological example of geometry of formulae is the ‘little Fermat theorem’ generalized by Euler and describing the number-theoretic properties of geometric progressions reduced modulo $n$, like the periodic sequence of residues of division of the powers of two by 13,

\[ \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2, \ldots \} \]

(for $n = 13$). Fermat’s observation is that such a sequence $\{a^t \mod n\}$ is always periodic (he considered the case of a prime number $n$, and Euler extended his theorem to the general case in which the base $a$ and the modulus $n$ are only coprime).

Already in this simple case we face the problem of the asymptotic behaviour for large $n$ of the peculiarly irregular value $T(n)$ of the period of the geometric progression of residues modulo $n$ (for instance, of the sequence $\{2^t \mod n, t = 0, 1, 2, \ldots\}$ if $n$ is an odd number), at least in the sense of the weak asymptotic behaviour introduced in [6], and this is an example of an unsolved statistical problem in ergodic number theory.

Observations show a growth of the period which is linear on the average (although deviations in both directions are rather large, they are fairly rare):

| $n$ | 5 | 7 | 9 | 13 | 15 | 19 | 29 | 31 | 71 | 509 | 511 |
|-----|---|---|---|----|----|----|----|----|----|-----|-----|
| $T$ | 4 | 3 | 6 | 12 | 4  | 18 | 28 | 5  | 8  | 35  | 508 | 9   |

The mean values (at least over a small interval of change of the modulus $n$) have a more regular behaviour. For example, the sums of successive tens of odd numbers $1 \leqslant n \leqslant 19$, $21 \leqslant n \leqslant 39$, and so on, and of the corresponding tens of values of the periods $T$ are

\[
\begin{array}{ccccccc}
\sum n & 100 & 300 & 500 & 700 & 900 \\
\sum T & 68 & 158 & 246 & 299 & 329 \\
\end{array}
\]

According to computations carried out by F. Aicardi, the sums of all periods for the odd moduli $1 \leqslant k \leqslant n$ behave as follows:

| $n$ | 9 | 109 | 509 | 1009 | 1509 | 2009 |
|-----|---|-----|-----|------|------|------|
| $\sum T$ | 15 | 1409 | 23607 | 82761 | 176016 | 302277 |

On the average, these numbers, when studied using a double logarithmic scale (similar to that used by Kolmogorov to discover the exponents in his laws of turbulence), rather correspond to an empirical formula of the form

\[ T \approx 1.4n^{4/5} \]
(which leads to a growth of the sums of order $n^{9/5}$). However, no theorems on the asymptotic behaviour have been proved here so far, and even the possibilities $T \approx Cn$ or $T \approx Cn/\log n$ are not excluded.

The ‘topological’ aspect of the little Fermat theorem is the following reformulation, which is mainly due to Euler (for a discussion, see [1]).

Let us consider the multiplicative group of residues modulo $n$ that are coprime to $n$ (I call this group the Euler group and denote it by $\Gamma(n)$).

If $n = p$ is a prime number, then the Euler group contains all $p - 1$ non-zero residues. In the general case the number $\varphi(n)$ of elements of the Euler group varies with $n$ in a rather complicated way:

| $n$   | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|
| $\varphi(n)$ | 1  | 1  | 2  | 2  | 4  | 2  | 6  | 4  | 6  | 4  | 10 | 4  |

Gauss called the function $\varphi$ the Euler function. If the (distinct) prime factors of the modulus $n$ are $p_k$ and their multiplicities are $a_k$, then the value of the Euler function $\varphi(n)$ is

$$\varphi \left( \prod p_k^{a_k} \right) = \prod [(p_k - 1)p_k^{a_k - 1}].$$

Corresponding to multiplication of all residues in $\Gamma(n)$ by one of them (for example, by 2 if $n$ is odd) is a permutation $(2*)$ of the finite set $\Gamma(n)$ consisting of $\varphi(n)$ elements (of all residues coprime to $n$).

Euler’s observation (equivalent to the Euler–Fermat theorem, which is usually formulated in another way) is as follows.

**Euler theorem.** The Young diagram of the permutation “multiplication by a fixed element $a$ of the group $\Gamma(n)$” is a rectangle, that is, all cycles of this permutation have the same length $T(n)$.

We denote by $N(n)$ the number of these cycles, that is, the number of orbits of the dynamical system “multiplication by $a$”,

$$(a*): \Gamma(n) \to \Gamma(n)$$

(for definiteness we shall choose $a = 2$ and odd $n$).

Then the area of the entire Young diagram of the permutation $(a*)$ is the value of the Euler function,

$$\varphi(n) = T(n)N(n),$$

and thus both the period $T$ and the number $N$ of orbits are divisors of the value of the Euler function.

**Example.** For $n = 31$ and $a = 2$ we have

$$\varphi(n) = 30, \quad T(n) = 5, \quad N(n) = 6.$$
The Young diagram (filled by the elements of the cycles of the permutation “multiplication by 2”) has the following form (mod 31):

\[
\begin{array}{cccccc}
1 & 2 & 4 & 8 & 16 & \\
3 & 6 & 12 & 24 & 17 & \\
5 & 10 & 20 & 9 & 18 & \\
7 & 14 & 28 & 25 & 19 & \\
11 & 22 & 13 & 26 & 21 & \\
15 & 30 & 29 & 27 & 23 & \\
\end{array}
\]

\[16 \cdot 2 \equiv 1 \pmod{31}, \quad T(31) = 5\]

\[N(31) = 6.\]

Here are several examples of values of the period \(T\) and of the number \(N\) of orbits for the operation of multiplying the residues by 2 for diverse values of the modulus \(n\) (cf. [2]):

\[
\begin{array}{cccccccc}
\hline
n & 37 & 65 & 129 & 229 & 381 & 509 & 511 \\
T & 36 & 12 & 14 & 76 & 14 & 508 & 9 \\
N & 1 & 4 & 6 & 3 & 18 & 1 & 48 \\
\hline
\end{array}
\]

On the average, the growth of the product \(\varphi(n) = T(n)N(n)\) is \(cn\), where \(c = 6/\pi^2\), namely, it was proved (by B. A. Venkov) that

\[
\lim_{n \to \infty} \frac{\sum_{k=1}^{n} \varphi(k)}{\sum_{k=1}^{n} k} = c = \frac{1}{\zeta(2)}.
\]

The coefficient \(c\) occurs here as the probability that the fraction \(p/q\) is irreducible (in quite the same way, \(1/\zeta(m)\) is the probability that there are no integral points on the segment between 0 and an integral vector in \(m\)-dimensional space).

The fact that this probability (in the case of the plane) is \(1/\zeta(2)\) follows from the Euler formula

\[
\prod_p \frac{1}{1 - 1/p^m} = \sum_{n=1}^{\infty} \frac{1}{n^m}
\]

(the product over all primes), which was conceived by Euler for this very reason (for the details, see [1]).

Euler also discovered that \(\zeta(2) = \pi^2/6 \approx 3/2\), which follows from the theory of Fourier series (one must expand the \(2\pi\)-periodic function coinciding with \(|x|\) on the segment \(|x| \leq \pi\) in a Fourier series).

It should be noted that, by [1], the empirical average growth of the number \(N(n)\) of orbits is approximately the same as if the number \(N\) of orbits were increasing by the rule

\[N \approx 0.67n^{2/5}\]

(this is the ‘weak asymptotic behaviour’ in the sense of the paper [6]).
The sum $2/5 + 4/5$ of the exponents of the empirical means of the asymptotic expressions for $N$ and for $T$ is greater than the exponent 1 of the average asymptotic expression for the Euler function $\varphi$. This does not contradict the Euler formula $\varphi = NT$, because a product of means is certainly not the mean value of the product. On the contrary, this deviation is a distinctive indication of frequent alternation of large deviations of the factors in both directions from the means (similar to the intermittency phenomenon in the theory of turbulence and in hydrodynamics).

Although existing observations do give some empirical average ‘asymptotics’ for this number-theoretic intermittency, no theorems have yet been proved.

By [1], empirical formulae for the mean frequencies $p_N$ of occurrence of the values $N = 1, 2, 4, 8$ and $N \geq 10$ in a neighbourhood of a fixed value $n$ (between 1 and 2000) have power-law weak asymptotic behaviour of the form

$$p_1 \sim a n^{-7/18}, \quad p_2 \sim b n^{-1/9}, \quad p_4 \sim c n^{1/3}, \quad p_8 \sim d n^{1/9}, \quad p_{\geq 10} \sim e n.$$  

However, we see no reasons for the rationality of these exponents (in contrast to the rationality of the Kolmogorov exponents in the theory of turbulence and the preceding hydrodynamical exponents of Leonardo da Vinci).

The values $T(n)$ and $N(n)$ for odd $n = 2k + 1$, $k = 1, \ldots, 1000$, were computed by F. Aicardi. Her results are shown in the bilogarithmic scale below in §10; Kolmogorov found his 5/3 law in the theory of turbulence in a similar way (his graph is also shown below in §10).

Aicardi’s line indicates empirical weak (averaged) asymptotics

$$T(n) \sim 0.94 n^{0.834}, \quad N(n) \sim 0.60 n^{0.36}, \quad \varphi(n) \sim c n^a,$$

where the constants for $n$ from 1 to 10$^5$ are approximately equal to $a = 0.9994$ and $c = 0.612$, whereas $6/\pi^2 \approx 0.6079$.

In fact, the graphs of the quantities $(\Sigma T)(n) = \sum_{k=1}^n T(k)$ and $(\Sigma N)(n) = \sum_{k=1}^n N(k)$ (k odd) in the bilogarithmic scale were used for a smoothing averaging. The almost rectilinear logarithmic graphs correspond to the power-law functions

$$(\Sigma T)(n) \sim 0.255 n^{1.834}, \quad (\Sigma N)(n) \sim 0.223 n^{1.36}.$$  

§ 2. Are the residues of the elements of a geometric progression random?

We describe here the ‘stochasticity criteria’ developed to recognize the level of randomness of a sequence.

The Lyapunov exponent of the operation of multiplying the residues by 2 shows a rather rapid growth of perturbations in the Fermat–Euler dynamical system. Thus, one can expect a chaotic distribution of these residues (among all $n$ residues in $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ or at least among the $\varphi(n)$ residues in the Euler group $\Gamma(n)$ that are coprime to $n$).

However, the observed statistics of the periods $T(n)$ shows an incompelty chaotic behaviour of the elements of the orbit of $T(n)$ residues, namely, one can observe a certain mutual repulsion between the residues of the elements of a geometric progression.
The fact of the matter is that all \( T(n) \) residues of the elements \( \{2^t(t = 1, 2, \ldots, T)\} \) modulo \( n \) within a single period are distinct, because a repetition of some residue would lead to the repetition of all subsequent residues.

If the residues of the \( T \) elements of the orbit in question were independent random elements of a set of \( m \) elements (\( m = n \) in the case of the distribution of residues in \( \mathbb{Z}_n \), and \( m = \varphi(n) \) in the case of the distribution of residues in the Euler group \( \Gamma(n) \)), then the famous ‘birthday problem’ in probability theory would suggest a value for \( T(n) \) much less than \( n \) (of order \( \sqrt{n} \)).

Namely, the probability of the absence of coincidences in a sample of \( T \) elements of an \( m \)-element set is small as long as \( T \) is ‘not very large’, and is close to 1 if \( T \) is ‘large’, and the change happens near a special critical value \( T_* \sim \sqrt{2m} \).

Indeed, \( m(m-1)\cdots(m-T+1) \) is the number of \( T \)-element sequential samples from \( m \) elements and \( m^T \) is the number of all such samples (possibly with repetitions), so the probability of the absence of repetitions is

\[
p(T, m) = \prod_{k=0}^{T-1} \frac{m-k}{m} \sim e^{\sum \log(1-k/m)} \sim e^{-\sum k/m} \sim e^{-T^2/2m}.
\]

Although the exponent of the power-law asymptotic behaviour of the dependence of the period \( T \) on the modulus \( n \) is not known even in the sense of smoothed means and weak asymptotics, the empirical data of the papers \([1]–[3]\) suggest that, if this exponent differs from 1, it is in any case closer to 1 than to the exponent \( 1/2 \) which would be observed if the elements of the orbit were independent random residues.

Thus, the observed period of the geometric progression is greater than the period corresponding to a random choice of the elements in the orbit. That is, the residues of the members of the progression avoid close approach and are pushed apart in this sense.

To measure this mutual repulsion, I computed the mean distance on a circle of length \( L \) between neighbouring points in a given \( T \)-point set, defining this mean in the following way (introduced in [1]).

If the lengths of the arcs into which the circle is divided by the points of the set are equal to \( x_i, i = 1, \ldots, T \) (and thus \( \sum x_i = L \)), then we first find the sum of squares of these lengths,

\[
R = \sum x_i^2.
\]

In order to get rid of the (dimensional) length of the circle \( L \), let us take the normalized sum of squares of the distances between neighbours as the ‘stochasticity measure’ of the set of \( T \) elements,

\[
r = R/L^2
\]

(this division by \( L^2 \) is equivalent to the normalizing compression of the circle of length \( L \) to the circle of length 1).

The least value of the ‘stochasticity measure’ \( r \), namely, the value \( 1/T \), is attained for the ‘barracks formation’ of the arithmetic progression of equidistant points (partitioning the circle into \( T \) arcs of length \( 1/T \) each). The largest value \( r = 1 \) is
attained for the cluster distribution of total congestion (all arcs but one of zero length).

It is convenient to represent these facts by interpreting $r$ as the squared distance from the origin to the point $z = x/L$ of the $(T-1)$-dimensional simplex $0 \leq z_i \leq 1$, $\sum z_i = 1$, in $T$-dimensional Euclidean space.

The minimum distance from the origin is attained at the centre of the simplex and the maximum at the vertices.

Corresponding to a random choice of the points of the set on the circle is the random distribution of the point $z$ on the simplex (uniformly distributed with respect to the Lebesgue measure on the simplex). The value of the ‘stochasticity measure’ $r$ for this ‘freedom-loving’ distribution of points on the circle can readily be computed explicitly: it is intermediate between the barracks minimum value (for strongly repulsed particles) and the cluster maximal value (attained for particles congested at a single place).

To compare sets with different numbers $T$ of points, I have divided the value of the exponent $r$ by its minimum value for a given number of points and defined the doubly (with respect to $L$ and with respect to $T$) normalized stochasticity parameter

$$s = r/r_{\text{min}} = Tr.$$  

The barracks (minimum) and the cluster (maximum) values of this new parameter are

$$(s_{\text{min}} = 1) \leq s \leq (s_{\text{max}} = T).$$

The computations show that the freedom-loving value of this stochasticity parameter is close to two and equal to (see [1])

$$s_* = 2T/(T + 1).$$

The values of the stochasticity parameter that are less than the freedom-loving value ($1 \leq s < s_*$) indicate a mutual repulsion of the particles in the set (the less $s$ is, the stronger the repulsion is), and greater values ($s_* < s \leq T$) show the mutual attraction of the particles.

Explicit calculations ([1], [3]) of the values of the stochasticity parameter $s$ for the residues of geometric progressions (these calculations were carried out by F. Aicardi with the help of a computer) gave values of order 1.5 for the doubly normalized stochasticity parameter $s$ in most cases (now and then values close to 1, or significantly greater than 2). However, there are no theorems, only results of thousands of experiments.

I carried out similar calculations for other sets as well, for instance, for the distribution of residues of the first few hundreds of prime numbers and for arithmetic progressions of residues (see [1]).

The mutual repulsion was observed in both cases (the values of the parameter $s$ were less than the freedom-loving value). Moreover, for an arithmetic progression the result depends strongly on the length $T$ of the segment of the progression under consideration. Both for the mean values with respect to the parameter $T$ and for the optimal choices of $T$ depending on the convergents of the quantity $a/n$ one can assume the possibility of obtaining the asymptotic behaviour (distinct in...
these two cases) of the stochasticity parameter for the sequence \( \{at + b \mod n\} \), \( 1 \leq t \leq T \), in terms of the continued fraction for \( a/n \) (with possible averaging by the Gauss–Kuz’min theorem on the ergodic characteristics of the elements of continued fractions). Here we speak principally of the weak asymptotic behaviour, of course.

The mutual repulsion of the residues of the terms of a geometric progression also affects the distribution of arclengths of the integral circle \( \mathbb{Z}_n \) (or the Euler group \( \Gamma(n) \)) between these residues. The frequencies of occurrences of arcs with different arclengths \( k \) (from the maximum length \( m - (T - 1) \) to the minimum arclength 1 on the integral circle of length \( m \) divided into \( T \) integral arcs by \( T \) randomly and independently chosen distinct points) are to one another as the numbers in the Pascal triangle lying on a line parallel to a side of the triangle at a distance \( T - 2 \) from the side:

\[
p_k = \left( \frac{m-1-k}{T-2} \right) \left/ \left( \frac{m-1}{T-1} \right) \right. \]

For example, when choosing four points \( (T = 4) \) among eight points \( (m = 8) \), the frequencies of the arcs of lengths 1, 2, 3, 4, and 5 are to one another as \( 15 : 10 : 6 : 3 : 1 \) (that is, arcs of length 4 occur five times more rarely than those of length 1).

Let us consider the geometric progression \( \{2^t \mod 15\} \) as the four-point subset \( \{1, 2, 4, 8\} \) of the eight-point circle of residues, \( \Gamma(15) = \{1, 2, 4, 7, 8, 11, 13, 14\} \) (with distance 1 between consecutive numbers written and between 14 and 1). The ‘distances’ between the neighbouring points of the progression along\(^1\) the Euler group \( \Gamma(15) \) are \( \{1, 1, 2, 4\} \), that is, an arc of unit length occurs \( 2\frac{1}{2} \) times more rarely than for random points, which again confirms the mutual repulsion of the residues of the terms of a geometric progression.

Here the doubly normalized stochasticity exponent is equal to

\[
s = \frac{1 + 1 + 4 + 16}{8^2} \cdot 4 = \frac{22}{16} = 1.375,
\]

which is significantly less than the freedom-loving value \( 2T/(T+1) = 1.6 \) of this exponent and also indicates the mutual repulsion of residues of the terms of the progression.

§ 3. Topology of the squaring operation

Let us begin with a quite abstract and rather logical object.

**Definition.** By a **monad** we mean a map of a finite set into itself. By the **graph of a monad** we mean an oriented graph whose vertices are the points of this finite set and whose edges join the points of the graph with their images under the map.

In other words, the graph of a monad is an arbitrary finite graph each of whose vertices has only 1 issuing edge.

The geometric progressions of residues \( \{2^t \mod n\} \) treated above are connected with the following ‘Frobenius monads’: every element of a finite group (or ring) is

\(^1\)By the distance between two elements along the group \( \Gamma \) we mean here the number of arcs between two given residues, counting only the arcs that are free of elements of the group.
sent to its square, \( x \mapsto x^2 \). The exponents of the powers of \( x \) obtained in the course of iterations of this monad form a geometric progression.

**Example.** The graph of squaring in the residue class ring \( \mathbb{Z}_7 \) has three connected components:

```
0  1  6
```

```
3  2  4  5
```

For example, \( 4^2 \equiv 2 \pmod{7} \) and \( 5^2 \equiv 4 \pmod{7} \).

**Theorem 1.** The connected components of each monad are attracting cycles that are equipped with rooted trees joined by their roots to every vertex of the attracting cycle.

The length of a cycle can also be equal to 1, as is the case for the components \( \{1,6\} \) and \( \{0\} \) in the above example.

As a monad we now take the squaring operation for the elements of a finite commutative group (when taking the logarithm of this operation, we obtain the monad \( x \mapsto 2x \) generating the geometric progression \( \{2^t, t = 0, 1, 2, \ldots\} \)).

**Theorem 2.** Each connected component of the graph of the squaring operation for the elements of a finite commutative group is a cycle equipped homogeneously (with the same tree at each vertex).

The equipping tree has \( 2^k \) vertices (including the root belonging to the attracting cycle) and is a product of binary trees in the sense of the definition of product given below.

The binary tree \( T_{2^n} \) with \( 2^n \) vertices consists of the root and \( n \) floors, and exactly two edges (from two vertices of the \((i + 1)\)st floor) lead to each vertex of the \( i \)th floor for \( i = 1, 2, \ldots, n - 1 \).

Two edges (from the root itself and from the (only) vertex of the first floor) lead to the root of the tree \( T_{2^n} \), which can be regarded as a vertex of the zeroth floor.

**Example.** The doubling monad \( x \mapsto 2x \) in the group \( \mathbb{Z}_4 \) has the binary tree \( T_4 \) as its graph.

---

§ 4. **Algebra of rooted trees**

The *multiplication of monads* is defined as the componentwise action of both operations on the direct product of the sets of vertices of the graphs of these monads: the *product monad* \( X \ast Y \) acts on a point \((x, y)\) of the direct product of the set of vertices of the graph \( X \) and the set of vertices of the graph \( Y \) by the rule

\[ (X \ast Y)(x, y) = (Xx, Yy). \]

**Example.** Let us multiply the \( n \)-vertex cycle \( O_n \) by the simplest binary graph \( T_2 = A_1 \) (\( A_1 \) is, for instance, the above component \( \{1, 6\} \) of the graph of squaring in the ring \( \mathbb{Z}_7 \)). The product \( A_n = O_n \ast A_1 \) is a \( 2n \)-vertex graph with the attracting cycle \( O_n \) homogeneously equipped with one-edge rooted trees at each of its vertices,
likethethirdcomponent $A_2 = O_2 \ast A_1 = \{2, 3, 4, 5\}$ of the graph of squaring in the residue class ring $\mathbb{Z}_7$ (this graph is shown in the above figure).

The rooted trees are connected graphs of monads (with only one cycle of unit length).

The graph of a product of such monads is itself a rooted tree. The graph (tree) of a product of monads is referred to as the product of the graphs (trees) of the multiplied monads.

**Example.** The graph $A_1 \ast A_1 = D_1$ is a four-vertex rooted tree such that exactly three edges go to the root (from the other three vertices). This is the graph of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The graph $D_n = O_n \ast D_1$ has $4n$ vertices and one attracting cycle such that three edges from the outside go to each of its vertices (and together form the tree $D_1$ equipping this vertex).

When investigating products of rooted trees, it is useful to assign to a tree the following set of ‘ranks’; we denote by $r_i$ the number of vertices for which the path from the vertex to the root consists of $i$ edges and is of length $i$ (in particular, $r_0 = 1$, $r_1(D_1) = 3$, $r_1(T_4) = 1$, and $r_2(T_4) = 2$).

Under multiplication of graphs the ranks behave as follows:

$$r_k(X \ast Y) = \sum r_i(X)r_j(Y),$$

where $\max(i, j) = k$. In other words, the sums $s_k = r_0 + r_1 + \cdots + r_k$ satisfy the identity $s_k(X \ast Y) = s_k(X)s_k(Y)$.

This means that, to compute the ranks of the product tree, one must form the matrix of products of the ranks of the factor trees and compute the sums of its elements in the corners bounding the vertex $i = j = 0$.

For example, for the product of the binary trees $T_4$ and $T_8$ the matrix of products of the ranks is of the form (the corners are marked)

$$
\begin{pmatrix}
2 & 2 & 4 & 8 \\
1 & 1 & 2 & 4 \\
1 & 1 & 2 & 4
\end{pmatrix},
$$

and therefore the ranks of the product are

$$r_0 = 1, \quad r_1 = 3, \quad r_2 = 12, \quad r_3 = 16.$$

In the same way, the ranks of the product $T_{2n} \ast T_{2n}$ of a binary tree by itself are $\{1, 3, 3 \cdot 4, 3 \cdot 16, \ldots, 3 \cdot 4^{n-1}\}$ (if the second binary tree is replaced by a larger one, then the sequence of ranks is continued by powers of two).

I describe the products of binary trees in detail because only these objects occur (as trees homogeneously equipping cycles) when describing the graphs of finite commutative groups.

This follows from the fact that such a group is a direct product of cyclic groups, and the graph of the operation of multiplying by 2, that is, of adding an element
to itself, in an (additively represented) cyclic group of odd order decomposes into
non-equipped cycles.

Indeed, it follows from the Euler theorem that \(2^{\varphi(n)} \equiv 1 \pmod{n}\) for any odd
number \(n\). Therefore, \(2^{\varphi(n)}a \equiv a \pmod{n}\), and hence each element \(a\) belongs to a
cycle of the monad of the cyclic group \(\mathbb{Z}_n\).

The multiplication table of these cycles is

\[O_m \ast O_n = dO_c,
\]

where \(d\) is the greatest common divisor and \(c\) is the least common multiple of the
numbers \(m\) and \(n\) (we mean the disjoint union of \(d\) cycles of the same length \(c\)).

For example, the following identities hold in the algebra of graphs:

\[O_3 \ast O_5 = O_{30}, \quad O_6 \ast O_{10} = 2O_{30}.
\]

The graph of the operation of adding elements to themselves in the additive
cyclic group of order \(2^n\) turns out to be the binary tree \(T_{2^n}:

The above algebra of graphs enables one to quickly investigate more complicated
cases as well. For instance, the largest connected component of the graph of the
squaring operation in the Euler group \(\Gamma(125) \approx \mathbb{Z}_{100}\) containing 100 elements (this
component is very useful in the analysis of quadratic residues modulo 125) is of the
form \(O_{20} \ast T_4\) and has 80 vertices (see the figure on the next page).

The arrows of this graph lead to quadratic residues modulo 125 (for example, \(13^2 ≡ 44 \pmod{125}\)), and the vertices standing at a distance from the cycle
\((22, 37, \ldots)\) and belonging to the trees equipping it are quadratic non-residues (the
congruence \(x^2 ≡ 2 \pmod{125}\) is non-soluble).

It is the topology of such graphs that explains certain facts in the theory
of quadratic forms, for instance, the structure of semigroups of values of ‘per-
fec’t’ quadratic forms in the paper [5] (like the form \(x^2 + 2y^2\)). In the last example
the odd values of the form constitute a semigroup of numbers representable as a product

\[\prod p_i^{a_i} q_j^{b_j} r_k^{c_k} s_l^{2d_l},
\]

where \(p_i, q_j, r_k, \text{ and } s_l\) are distinct odd prime factors whose residues when divided
by 8 are 1, 3, 5, and 7, respectively. The factors \(r\) and \(s\) (which are congruent to 5
and 7 mod 8) must occur with even degrees.

For example, the numbers 5, 7, 125, and 343 are not representable, and the
numbers 3, 17, 25, and 49 are representable in the form \(x^2 + 2y^2\) with integers \(x\n\text{and } y\) (say, \(17 = 3^2 + 2 \cdot 2^2\)).
§ 5. Graphs of squaring in permutation groups

I discovered the following fact in trying to extend the theorem on homogeneity of the equipping with trees of a cycle of a monad, from commutative groups to arbitrary finite groups.

**Theorem 3.** Every connected component of the graph of the squaring operation in the symmetric group of permutations of $n$ elements (or in the subgroup of it formed by the even permutations) is equipped homogeneously (that is, the equipping trees are isomorphic for all vertices of the cycle of the component).

This result on the homogeneity of the equipping is derived from the following description of elements of the attracting cycle for the graph of a permutation group: the attractor consists of the permutations whose cycles all have odd length.

However, a cyclic permutation of odd length is conjugate to its square. This conjugation not only takes one of the vertices of the attracting cycle to a neighbouring vertex but also acts on the trees equipping this cycle, again by permuting the trees, and therefore all trees equipping the same component are isomorphic.
In the group of even permutations the square of the permutation with the cycle 
(1, 2, 3) is no longer conjugate to the original permutation in the group of even 
permutations of three elements, because the conjugating permutation (2, 3) is odd.

However, such a ‘conjugation’ by an odd permutation still defines an (outer) 
automorphism shifting a vertex of the attracting cycle to a neighbouring place and 
taking the tree equipping the vertex to the corresponding neighbouring equipping 
tree, and thus the equipping of the cycle of the component remains homogeneous 
for the graph of the squaring operation for the elements of the group of even per-
mutations.

The homogeneity of the equipping is preserved for all finite groups.

I do not know to what extent the algebraic skewness of a skew product of groups 
1 → H → E → G → 1 influences the topological skewness of the graph of the 
‘product’ group E in comparison with the product of the graphs of the groups 
(the ‘factors’) G and H (not even in the case of two-sheeted coverings, in which 
case $H = \mathbb{Z}_2$, or of index-two subgroups $H$, in which case $G = \mathbb{Z}_2$).

The group $SL(2, \mathbb{Z}_6)$ consists of the 144 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ whose elements are 
residues modulo 6 for which $ad - bc \equiv 1 \pmod{6}$.

The graph of squaring consists of 14 components:

$$[\text{graph } (SL(2, \mathbb{Z}_6))] = T + (O_2 * R) + 4(O_2 * E_8) + 8A_2,$$

where the tree $T$ has the sums of ranks $s = (1, 8, 32)$ and the tree $R$ has the sums 
of ranks $s = (1, 2, 8)$.

Explicitly, the 16 matrices forming the graph $O_2 * R$ are

In this component the homogeneity of the equipping with trees of the cycle is 
explained by the (outer) automorphism conjugating each matrix by means of the 
orientation-inverting map of the plane which transposes the coordinate axes and 
transforms a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} d & c \\ b & a \end{pmatrix}$. 
The numbers of matrices with different traces \( a + d \) in each of the components are

| \( a + d \) | \( T \) | \( O_2 \ast R \) | \( 4(O_2 \ast E_8) \) | \( 8A_2 \) |
|------------|---------|----------------|------------------|---------|
| 0          | 24      | 0              | 0                | 0       |
| 1          | 2       | 2              | 0                | 8 \cdot 2 |
| 2          | 3 + 1   | 0              | 3 \cdot (6 + 2) + 6 | 0       |
| 3          | 0       | 12             | 0                | 0       |
| 4          | 3 + 1   | 0              | 3 \cdot 8 + (8 + 2) | 0       |
| 5          | 0       | 2              | 0                | 8 \cdot 2 |

The notation of the form \( 3 + 1 \) in the graph \((2, T)\) means that the 4 points of the graph \(T\) for which \( a + d = 2 \) are subdivided into two classes, one of which has 3 elements and the other 1 element, and which occupy non-isomorphic places in the tree \(T\) (in the example under consideration, these matrices

\[
\begin{pmatrix}
1 & 3 \\
0 & 1
\end{pmatrix},
\begin{pmatrix}
1 & 0 \\
3 & 1
\end{pmatrix},
\begin{pmatrix}
4 & 3 \\
3 & 4
\end{pmatrix}
\]

and
\[
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\]

are at distances 1 and 0 from the root).

It would be of interest to relate these structures of graphs for the monads of groups to the actions of ordinary and inner automorphisms and also of the wider class of monadomorphisms on these groups: do the automorphisms or inner automorphisms form normal subgroups in the groups of monadomorphisms (and what are the quotient groups if the answer is positive)?

§ 6. Homogeneity of the monads of all finite groups

The monadomorphisms, and groups and categories formed by them, deserve special investigation.

**Theorem 4.** For any finite group the equipping of the attracting cycle of each connected component of the graph of the monad of squaring is homogeneous (the rooted trees joined to the cycle at all its points are the same for each connected component).

**Proof.** Let us construct a map taking the tree attracted by the cycle at a vertex \( a \) to the tree attracted by the cycle at its next vertex, \( a^2 \).

**Definition.** We say that a vertex is of rank \( r \) if it is separated by \( r \) edges from the attracting cycle.

**Example.** The vertices of the attracting cycle are of zero rank.

Let us consider an attracting cycle of period \( T \) formed by the vertices \( \{a, a^2, a^4, \ldots, a^{2^{T-1}}\} \) (the next vertex of the cycle is \( a \) again). In this case the periodicity condition holds:

\[ a^S = 1, \quad \text{where} \quad S = 2^T - 1. \]
Definition. By the connection of a component attracted by a cycle of period $T$ we mean a map $P$ taking each vertex $b$ of rank $r$ to the vertex

$$Pb = c = b^x, \text{ where } x = (2^r - 1)S + 2.$$ 

Example. The vertices $(a, b_1, b_2, \ldots)$ of ranks $(0, 1, 2, \ldots)$ are taken to $Pa = a^2,$ $Pb_1 = b_1^{S+2},$ $Pb_2 = b_2^{3S+2}, \ldots.$

It follows from the periodicity condition $a^S = 1$ that the relations $b_1^{2S} = 1,$ $b_2^{4S} = 1,$ $\ldots,$ $b_r^{2r} = 1$

hold for the vertices $b_r$ of rank $r$ (because the vertices $b_r^T = a$ belong to the attracting cycle).

The choice of the value $x(r)$ in the definition of connection is explained by the following fact.

Lemma 1. The connection is a monomorphism:

$$P(b^2) = (P(b))^2.$$

Proof. If $b$ is a vertex of rank $r$, then the rank of the vertex $b^2$ is equal to $r - 1$. Therefore, the following identities hold:

$$P(b^2) = (b^2)^y = b^{2y}, \text{ where } y = (2^{r-1} - 1)S + 2;$$

$$(P(b))^2 = (b^x)^2 = b^{2x}, \text{ where } y = (2^{r-1} - 1)S + 2.$$ 

The ratio of these two powers of the vertex $b$ is equal to $b^{2(x-y)}$. However, $2(x-y) = 2'S$, and therefore the ratio is equal to 1 by the periodicity condition. This proves Lemma 1.

Lemma 2. If distinct vertices $b$ and $b'$ have equal squares, $b^2 = (b')^2$, then the vertices $c = b^x$ and $c' = (b')^x$ are also distinct.

Proof. If $r > 0$, then the number $x = 2k + 1$ is odd. In this case we have the identities

$$c = b(b^2)^{k}, \quad c' = b'(b^2)^{k},$$

and therefore the equality $c = c'$ implies the equality $b = b'$, which proves Lemma 2.

Lemma 3. If a vertex $b$ is of rank 1, then the vertex $c = Pb$ does not belong to the attracting cycle (and thus the rank of $c$ is equal to 1).

Proof. If the vertex $c = b^{S+2}$ were in the attracting cycle, then this vertex would be a power $a^{2k}$ of the vertex $a = b^2$ belonging to the cycle.

There are $T$ distinct powers of this kind, but the relations

$$(Pb)^2 = P(b^2) = P(a) = a^2$$

would lead to the conclusion $Pb = a$, that is, $b^{S+2} = b^2$. The last equality would mean that $b^{2T+1} = b^2$, and thus the relations

$$b = b^{2^{T-1}} = a^{2^{T-1}}$$

would be valid. Then the rank of the vertex $b$ would be equal to zero rather than 1.

The contradiction thus obtained proves Lemma 3.
Lemma 4. The connection maps the tree attracted by the vertex \( a \) of the cycle isomorphically onto the tree attracted by the next vertex \( a^2 \) (in particular, preserving the ranks of the vertices).

Proof. By \( n_i \) we denote the number of tree vertices attracted by the vertex \( a_i \) of the attracting cycle,

\[
\{ a_0 = a, \ a_1 = a^2, \ldots, a_i \equiv a^{2^i}, \ldots \} \quad (i = 0, 1, \ldots, T - 1).
\]

The isomorphisms into the consecutive trees discussed in Lemmas 1–3 prove the chain of inequalities \( n_0 \leq n_1 \leq \cdots \leq n_T \).

It follows from \( T \)-periodicity of the cycle that \( n_T = n_0 \), and thus all the numbers in the periodic sequence \( n_i \) are the same, and all the trees attracted by the vertices of the cycle are isomorphic, which proves Lemma 4 (and Theorem 4 as well).

Remark. Along with the special connection introduced above, one can consider other connections, defining them as monado-isomorphisms of the components shifting the cycle by one.

The iterated connection \( M = P^T \) takes each of the trees equipping the cycle onto itself.

Definition. The monadomorphism \( M \) is called the monodromy (of the component of period \( T \)).

The monodromy acts trivially on the lower floors of the trees (where \( r \leq 1 \)), but it can be non-trivial on the higher floors (and possibly enables one to define interesting invariants of groups).

Example. For a cycle of period \( T = 5 \) and for a vertex \( b \) of rank \( r = 2 \) the vertex \( b^4 = a \) belongs to an attracting cycle, and thus \( a^{32} = a, a^{31} = 1 \), and \( b^{124} = 1 \).

In this case \( S = 31 \), \( x = 3S + 2 = 95 \), \( Mb = b^5 \), and \( z = 95^5 \equiv 63 \) (mod 124). The vertex \( Mb = b^{53} \) can differ from \( b \), despite the fact that their projections on the first floor of the tree (that is, \( b^2 \) and \( (Mb)^2 \)) coincide: \( b^2 = b^{126} \).

§ 7. Modular topology of the Kepler cubes

In his book “Harmonice Mundi” Kepler described the radii of planetary orbits in terms of regular polyhedra inscribed in one another and, to this end, inscribed five cubes in a dodecahedron. The edges of these cubes are diagonals of the twelve faces of the dodecahedron (one edge for each face).

These Kepler cubes arise automatically in a description of the geometry of the monad of squaring for the group \( G = SL(2, \mathbb{Z}_5) \) consisting of 120 elements. This graph has 17 components:

\[
[\text{graph} \quad G] = T + 10A_2 + 6A_4.
\]

Let us now construct a Riemann surface from this graph.

The rooted tree \( T \) has 32 vertices: the vertex \( \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \) at the first floor and 30 vertices \( c \) of period 4 (thus, \( c^4 = 1 \)) at the second floor, and thus the set of ranks is of the form \( r(T) = (1, 1, 30) \) (with respect to the root vertex 1 at the zeroth floor).
The periods of the points of the components $A_4$ are equal to 5 (for the vertices on the attracting cycles) and to 10 (for the vertices of the (unique) first floor of the equipping trees). Typical examples are given by the element $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ of period 10 and by its square $\begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix}$ of period 5.

The periods of the points of the components $A_2$ are equal to 3 (for the vertices on the attracting cycles) and to 6 (for the vertices of the (unique) first floor of the equipping trees). Typical examples are given by the element $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ of period 6 and by its square $\begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix}$ of period 3.

**Theorem 5.** The group $G = SL(2, \mathbb{Z}_5)$ acts on the finite projective line $\mathbb{P} = P^1(\mathbb{Z}_5)$ as a certain special group of 60 even permutations of the six points of this finite line.

To describe these permutations, we begin with the dodecahedron with its twelve pentagonal faces. Let us join each face to the opposite face by a segment joining the centres of the faces. The symmetry group of the dodecahedron permutes these six lines. To describe the subgroup of the 60 special even permutations (which forms a small part of the total set of $360 = 6!/2$ even permutations of six elements), let us turn to the Kepler cubes.

The construction of such a cube begins with the choice of some diagonal on one of the faces of the dodecahedron. At an endpoint of this diagonal there are two other faces joining the face under consideration, and we choose the diagonal on each of these faces that passes through the indicated endpoint.

To this end, it suffices to turn the dodecahedron about the indicated endpoint through an angle of $120^\circ$, cyclically permuting the three faces concurrent at this endpoint. Then the original diagonal of the face is taken to the orthogonal diagonal of the neighbouring face.

Continuing this process, passing from one endpoint of a diagonal to the other, we quickly construct 12 diagonals of the faces (one on each face), and these diagonals form a Kepler cube (as the edges of the cube).

This cube depends on the initial choice of one of the five diagonals on the original face. Thus, the Kepler construction gives five cubes inscribed in the dodecahedron.

The desired 60 special permutations of six elements realized by the action of $SL(2, \mathbb{Z}_5)$ on $\mathbb{P}$ are described in the above terms as 60 *rotations* of the dodecahedron, which make up half of its symmetry group. They realize all 60 even permutations of the five Kepler cubes. Therefore, the *projective group of the finite projective line* $\mathbb{P}$ (consisting of 6 points) is isomorphic to the group $S^+(5)$ of even permutations of five elements (namely, the five Kepler cubes):

$$(G = SL(2, \mathbb{Z}_5))/\{\pm 1\} \simeq S^+(5).$$

**Remark 1.** The group $G$ consists of 120 elements, like the group $S(5)$ of all permutations of five elements. These two groups of 120 elements are not isomorphic. Indeed, the matrix group $G$ has centre $\{\pm 1\}$ consisting of two elements, whereas the centre of the permutation group is trivial.
Remark 2. The group $G$ is not representable in the form of a direct product $K \times H$, where $K = \{\pm 1\}$ is the group of two elements.

Indeed, denote by $(R_0 = 1, R_1, R_2, \ldots)$ the ranks of the tree $T$ of the identity component of the graph of $H$. The ranks of the product $A_1 \ast T$ are then equal to $(1, 2R_1 + 1, 2R_2, \ldots)$ (by the formula for the ranks of a product), because the graph $A_1$ of the group $K$ has the set of ranks $(1, 1)$.

For the group $G$ the ranks of the tree of the identity component are equal to $(1, 1, 30)$. Therefore, if $G$ were isomorphic to a product $K \times H$, then we would have $2R_1 + 1 = 1, 2R_2 = 30$, that is, $R_1 = 0, R_2 = 15$, which is impossible, because the second floor is empty if the first is, and $15$ is not equal to $0$.

In a similar way one can prove that the bundle $G \rightarrow G/K$ is non-trivial for the groups $SL(2, \mathbb{Z}_p)$, $p > 5$.

The components of the graph of the monad of squaring for the group $G = SL(2, \mathbb{Z}_5)$ can be described in terms of permutations of points of a finite projective line by Young diagrams of special even permutations of the Kepler cubes, namely,

$$A_1 \sim (5), \quad A_2 \sim (3 + 1 + 1), \quad T_r \sim (1 + 1 + 1 + 1 + 1)$$

at the floors $r = 0$ and $r = 1$, and $T_2 \sim (2 + 2 + 1)$.

Geometrically, the component of type $A_2$ is represented by four non-trivial rotations of the dodecahedron that preserve one of its faces (and hence also the opposite face). There are six pairs of faces of this kind, six components, and the total number of such non-trivial rotations of the dodecahedron is $24$.

The rotations realized by the components of type $A_2$ preserve a vertex of the dodecahedron (and hence the opposite vertex). There are $10$ pairs of vertices of this kind, $10$ components, and the total number of such non-trivial rotations of the dodecahedron is $20$.

The rotations realized by the element of the second floor $T_2$ preserve an edge (and hence the opposite edge). There are $15$ pairs of edges of this kind, $15$ elements, and, together with the identity transformation (realized by the floors $T_0$ and $T_1$), we obtain all $24 + 20 + 15 + 1 = 60$ rotations of the dodecahedron.

Let us consider the group $G = SL(2, \mathbb{Z}_p)$, where $p$ is odd, from the same point of view. This group permutes $(p + 1)$ points of the finite projective line

$$\mathbb{P} = P^1(\mathbb{Z}_p).$$

**Theorem 6.** All these permutations are even.

Indeed, the generators $g = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ and $h = \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)$ of the group $G$ have odd order $p$ in $G$ (that is, $g^p = b^p = 1$). This implies that the permutations corresponding to the generators are even, because an odd iterate $f^p$ of an odd permutation $f$ would be an odd permutation and cannot be the identity transformation.

Thus, the group $G/\{\pm 1\}$ of special (projective) permutations of $(p+1)$ elements (consisting of some $p(p^2 - 1)/2$ even permutations) is much smaller than the entire group of $(p+1)!/2$ even permutations of $(p+1)$ elements.

The simplest example here is the case $p = 7$ in which the projective group $G/\{\pm 1\}$ consists of $168$ special even permutations of eight points of the finite projective line $\mathbb{P}$. 
In this example the dodecahedron is replaced by the ‘regular polyhedron of genus $g = 3$’ that has 24 heptagonal faces meeting three at a time at 56 vertices and bordered by 84 edges. This polyhedron is connected with the singularity $K_{12}$ of the holomorphic function $z^2 + y^3 + z^7$ in $\mathbb{C}^3$ and with the reflection group for the triangle with angles $(\pi/2, \pi/3, \pi/7)$ in the Lobachevskii plane.

The amusing combinatorics of these special even permutations merits a thorough investigation.

The projective structure on the set of $p + 1$ points is preserved by these permutations and is fixed by a choice of a cyclic order on a subset of $p − 1$ points. The choice of this subset is inessential, but it must be fixed to obtain a one-to-one correspondence between the projective structures and the cyclic orders.

If $p = 5$, then there are six structures, because a set of $p − 1 = 4$ elements has six cyclic orders (the number of cyclic orders on a set of $m = p − 1$ elements is equal to $(m − 1)! = (p − 2)!$). Each of these six structures is preserved by the 360/6 = 60 special permutations of the six points (the class of special permutations depends on the structure).

If $p = 7$, then the number of cyclic orders on a fixed subset of $p − 1 = 6$ elements among the $p + 1 = 8$ points of the line $\mathbb{P}$ is equal to $(p − 2)! = 5! = 120$. Each of these 120 structures is preserved by special even permutations of the $p + 1 = 8$ points of the finite projective line, and the number of these special permutations is

$$\frac{(p + 1)!/2}{(p − 2)!} = \frac{p(p^2 − 1)}{2} = 168.$$  

To generalize the interpretation for $p = 5$ of this projective group $G/\{±1\}$ by means of Kepler cubes, we must construct an analogue of the surface of the dodecahedron and an analogue of the construction of the Kepler cubes for $p > 5$.

Below we find that that a certain Riemann surface generalizes the dodecahedron, and Hamiltonian subgroups supply analogues of the Kepler cubes.

§ 8. Kepler cubes and Hamiltonian subgroups

The classical Hamiltonian group consists of 8 quaternion units, $\{±1, ±i, ±j, ±k\}$. It is isomorphic to the connected identity component for the monad of squaring for the group $SL(2, \mathbb{Z}_3)$ (which is the only group $SL(2, \mathbb{Z}_n)$ for which the identity component of the monad of squaring forms a subgroup).

The Kepler cubes inscribed in the dodecahedron and their $K_{12}$-generalizations described below are connected with subgroups isomorphic to the classical Hamiltonian group in the identity component of the monad of squaring in the group $G = SL(2, \mathbb{Z}_p)$.

Among the 30 elements of order 4 forming the second floor $T_2$ of the identity component for the monad of squaring for the group $G = SL(2, \mathbb{Z}_3)$, one can single out five disjoint sextets each forming, together with the elements 1 and $−1$ of the zeroth and first floors of $G$, a subgroup isomorphic to the classical Hamiltonian group.

All five Hamiltonian subgroups of $G$ thus defined are conjugate in $G$.

To identify a sextet, one can use the relations $\{r^2 = −1, s^2 = −1, t^2 = −1\}$ for the anticommuting generators $r$ and $s$ of it and their product $t = rs$. 
To prove the above properties of the sextets, it suffices to verify them for a single example, for instance, for the sextet \( \{ \pm r, \pm s, \pm t \} \) with

\[
\begin{align*}
    r &= \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}, \\
    s &= \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \\
    t &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}
\end{align*}
\]

by computing the conjugations preserving this sextet.

These conjugations generate 12 automorphisms of the corresponding Hamiltonian subgroup. The 120 elements of the group \( G \) act as 60 conjugation operations, because \( axa^{-1} = (-a)x(-a)^{-1} \).

The 60 elements conjugate to a given sextet give \( 60/12 = 5 \) distinct sextets (we thus obtain 5 Hamiltonian subgroups of \( G \)) which are conjugate to one another.

The product of two elements of order 4 in \( G \) is itself of order 4 (and satisfies the relation \( (rs)^2 = -1 \)) for exactly the pairs \((r, s)\) generating a Hamiltonian subgroup. In particular, the two elements of this pair anticommute (which enables one to readily identify these elements, because these are the only anticommuting pairs of elements of order 4).

The manipulations described above give the following 5 sextets I–V (we write out only three elements in each sextet; the other three are \((-r, -s, -t)\)):

| sextet | I | II | III | IV | V |
|--------|---|----|-----|----|---|
| \( r \) | 01 | 11 | 20  | 13 | 14|
|        | 40 | 34 | 33  | 14 | 24|
| \( s \) | 02 | 20 | 12  | 20 | 20|
|        | 20 | 13 | 44  | 23 | 43|
| \( t = rs \) | 20 | 33 | 24  | 34 | 32|
|        | 03 | 02 | 03  | 02 | 02|

The five Kepler cubes are generated by these five Hamiltonian subgroups \( H \) in the following way (which simulates the computation of the matrix \( A^h \) for a matrix \( h \in H \)).

Let us choose an element \( A \) of order 3 in the group \( G \). Conjugation by \( A \) takes every Hamiltonian subgroup of \( G \) to a Hamiltonian subgroup. For a given Hamiltonian subgroup \( H \) of \( G \) there are 8 elements \( A \) of order three which preserve \( H \) under conjugation by \( A \): \( AHA^{-1} = H \).

**Definition.** These 8 elements of order three are the eight vertices of the Kepler cube connected with the chosen Hamiltonian subgroup \( H \).

The above computations give the following quadruples \((a, b, c, d)\) of vertices of the Kepler cubes (the other four elements of the group \( G \) are their inverses,
that is, \((a^2, b^2, c^2, d^2)\):

\[
\begin{array}{c|ccccc}
\text{sextet} & \text{I} & \text{II} & \text{III} & \text{IV} & \text{V} \\
\hline
a & 12 & 04 & 04 & 44 & 44 \\
 & 13 & 14 & 14 & 10 & 10 \\
b & 32 & 02 & 03 & 02 & 03 \\
 & 11 & 24 & 34 & 24 & 34 \\
c & 34 & 32 & 34 & 14 & 12 \\
 & 31 & 11 & 37 & 33 & 13 \\
d & 14 & 24 & 23 & 23 & 24 \\
 & 33 & 22 & 12 & 12 & 22 \\
\end{array}
\]

Each of the ten vertices of the Kepler cubes indicated in the table occurs in the table exactly twice, and exactly two cubes pass through each vertex of a Kepler cube. This gives, together with the inverses, the 20 vertices of the dodecahedron (which are precisely the twenty third-order elements in the group \(G\)).

The vertices of the Kepler cubes can readily be computed by using the following properties of these elements of the group \(G\).

Let us choose an orientation of the cube and the corresponding orientation of each face. Let \(P, Q, R, S\) be the sequence of vertices of a single face (ordered in accordance with the orientation). Then

\[PQ = QR = RS = SP\]

is the corresponding element of the Hamiltonian subgroup (all 4 edges of the same face give the same product).

The resulting correspondence between the six elements of the sextet and the six faces of the cube has the following property (which could be regarded as either the definition of a Kepler cube if the sextets are defined, or the definition of a sextet if the cubes are defined):

*The product of the three elements of the group \(G\) that correspond to the three faces coalescent at a vertex of the cube (equipped with the regular orientations of the faces) is always equal to 1.*

There are 12 colourings of the faces of the cube by the elements of a sextet, and all these colourings are transformed to one another by rotations of the cube.

Another description of the same correspondence between the Hamiltonian subgroups and the Kepler cubes is as follows:

*Four vertices of the Kepler cube are obtained from one of them (say, from \(A\)) by conjugating this vertex by the eight elements of the Hamiltonian subgroup, \(\{A, rAr^{-1}, sAs^{-1}, tAt^{-1}\}\) (the conjugation defined by \(-r\) coincides with that defined by \(r\)).

The other four vertices of the Kepler cube are inverse to those described above, that is, they are \(\{A^2, rA^2r^{-1}, \ldots\}\). The vertices of the Kepler cube are joined by edges in the same way as the elements of the Hamiltonian group placed at the
vertices of the cube are joined to one another: the vertices \((s, t, r)\) are neighbours of the vertex \(1\), and the vertex \((-u)\) is opposite to the vertex \(u\).

The above construction of the vertices of a Kepler cube from the elements of a Hamiltonian subgroup extends the map

\[1 \mapsto A, \quad (-1) \mapsto A^{-1}\]

by giving a definite meaning to the matrices \(A^r, A^s, A^t\).

Let us return to the surface of the dodecahedron. We can obtain it from the combinatorics of the group \(G\) by choosing the elements of order three as the vertices. Then one can choose one of the two conjugacy classes of elements of order five in the group \(PSL(2, \mathbb{Z}_5)\) (or of order ten in the group \(SL(2, \mathbb{Z}_5)\)).

In dependence on this choice of a conjugacy class, we obtain some dodecahedron surface from the group \(G = SL(2, \mathbb{Z}_5)\). The situation here is similar to the relation between a regular pentagon and the five-pointed star with the same vertices.

A permutation of vertices of the dodecahedron is said to be symmetric if it takes every symmetry of the dodecahedron to a (generally different) symmetry. The symmetries themselves define permutations of this kind. However, apart from these permutations, there is a non-trivial symmetric permutation (which is unique up to a symmetry). This very non-trivial symmetric permutation of the vertices transforms the dodecahedron obtained under one of the choices of a conjugacy class to a dodecahedron corresponding to another choice.

In terms of the group \(G = SL(2, \mathbb{Z}_5)\) the passage from one dodecahedron surface to another can also be described as a \(GL(2, \mathbb{Z}_5)\)-conjugation (by a matrix whose determinant is not a quadratic residue, for example, by the matrix \(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\)).

When a conjugacy class is chosen, two vertices \(A\) and \(B\) (of order three in \(G\)) are joined by an edge if the product belongs to the chosen class. This supplements the set of vertices to form a graph. The three edges issuing from a single vertex are cyclically permuted by a conjugation determined by this vertex, and the graph thus obtained turns out to be planar with respect to the resulting cyclic order of the edges issuing from every vertex. This graph divides the plane, or the sphere \(S^2\) in which the graph is embedded, into pentagons. This gives the desired dodecahedron.

It would be of interest to know to what extent this construction can be extended to other groups \(G\) (for instance, whether it gives surfaces as smooth or even holomorphic as in the case of \(G = SL(2, \mathbb{Z}_5)\) for \(SL(2, \mathbb{Z}_n)\) or for the group \(GL(2, \mathbb{CZ}_p)\) of matrices whose elements are complex numbers \(x+iy\), where \(x\) and \(y\) are residues modulo \(p\)).

§ 9. Riemann surface of heptagons and its Kepler cubes

Extending the dodecahedron investigations to the case of the group \(G = SL(2, \mathbb{Z}_7)\), we obtain the following conclusions.

**Theorem 7.** In the part \(T_0 + T_1 + T_2\) of the tree of the monad of squaring in the group \(G\) there are 14 Hamiltonian subgroups. Seven of them are conjugate to one of them and the other seven to another. These two Hamiltonian subgroups are not conjugate to each other in \(G\), although they are conjugate in the larger group \(GL(2, \mathbb{Z}_7)\).
The generators \((r, s)\) of seven Hamiltonian subgroups of this kind and their products \(t = rs\) are

| subgroup | I   | II  | III | IV  | V   | VI  | VII |
|----------|-----|-----|-----|-----|-----|-----|-----|
| \(r\)   | 01  | 24  | 32  | 02  | 03  | 16  | 13  |
|          | 60  | 45  | 24  | 30  | 20  | 26  | 46  |
| \(s\)   | 23  | 15  | 34  | 26  | 25  | 14  | 12  |
|          | 35  | 16  | 14  | 55  | 65  | 36  | 66  |
| \(t\)   | 35  | 66  | 46  | 33  | 41  | 55  | 56  |
|          | 54  | 21  | 33  | 64  | 43  | 62  | 52  |

The other seven Hamiltonian subgroups are obtained from these by the group automorphism

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}
\]

(the subgroup \(\tilde{I}\) dual to the subgroup \(I\) contains the matrices \(\begin{pmatrix} 0 & 6 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}\), and so on).

The 14 sextets of these 14 Hamiltonian subgroups give \(6 \cdot 14 = 84\) elements of order 4, whereas the second floor \(T_2\) of the monad of the group \(G\) contains 42 elements altogether.

Therefore, the sextets described have non-trivial intersections. These intersections are related to the four-colour problem by the following construction.

Let us form a graph whose 14 vertices are the 14 Hamiltonian subgroups of the group \(G\) and whose edges join vertices whose sextets intersect. The resulting graph can be described as a subset of the two-dimensional torus that partitions the torus into seven hexagons meeting three at a time at the 14 vertices. Each hexagon has a common edge with each of the others. Therefore, the map of seven countries that is obtained on the torus cannot be regularly coloured by fewer than seven colours.

The seven subgroups conjugate to the subgroup \(A\) are shown in the figure below by circles.

A covering of the torus by the seven hexagons is obtained from the regular hexagon on the Euclidean plane \(\mathbb{R}^2\). The union of this hexagonal domain with its six reflections in the sides covers a plane polygon which is a fundamental domain of the group \(\mathbb{Z}^2\) of parallel translations preserving the partition of the plane into congruent hexagons. As mentioned above, the quotient torus \(T^2 = \mathbb{R}^2/\mathbb{Z}^2\) is partitioned into seven hexagonal domains (the group of parallel translations is generated by the vectors \(AA'\) and \(AA''\)).

The fact that the pattern of intersections of the 14 sextets is isomorphic to this toric graph can be verified by a straightforward (though tedious) computation of the 84 matrices \(\{\pm r, \pm s, \pm t\}\).

The construction of the Kepler cubes from these 14 Hamiltonian subgroups repeats the \(SL(2,\mathbb{Z}_5)\)-construction carried out above and gives 14 Kepler cubes,
among which seven cubes are conjugate to one of them and the other seven to another, with the conjugations acting on each cube as rotations of it.

All these cubes could be drawn on a surface \( M \) which generalizes the dodecahedron and is covered by 24 heptagons meeting along 84 edges and forming a surface of genus 3 with 56 vertices, where three faces are coalescent at each vertex. The vertices of \( M \) are the elements of order three in the group \( G \), and the faces are defined by the elements of order 14, \( c = ab \), where \( c^7 = -1 \) and \( a^3 = b^3 = 1 \).

Instead of the surface \( M \), it is convenient to draw its quotient surface determined by the following ‘folding’.

The map assigning to each matrix \( A \) the transposed inverse matrix \( \tilde{A} \) is an automorphism of the group \( Q = SL(2, \mathbb{Z}_7) \) (namely, conjugation by means of the matrix \( \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \)). This automorphism takes an element of order three (of order 14) to an element of order three (of order 14, respectively), and therefore acts on the surface \( M \).

The quotient surface \( M' \) is obtained from \( M \) by identifying each matrix \( A \) with \( \tilde{A} \), and we obtain the folding map \( M \to M' \). The surface \( M' \) has only 28 vertices and only 12 heptagonal faces shown in Fig. 1. It is of genus 1 (homeomorphic to the torus).

The map \( M \to M' \) is a two-sheeted ramified covering with four branch points that are topologically of the type of the complex function \( \sqrt{z} \). The branch points are the mid-points of some four edges rather than vertices of the polygons constructed above.

The vertices of the surface \( M \) are the 28 matrices \( \tilde{A} \) listed below and their 28 squares, \( \tilde{A} = (\tilde{A})^2 \) (these are all the elements of order three in the group \( G \)): the
Figure 1. Fundamental domain of the quotient surface $M'$

index $i$ of a matrix takes values from 1 to 13 and from 15 to 29.
Figure 2. Averaged dependence of the period on the modulus in the bilogarithmic scale

Figure 3. Kolmogorov’s bilogarithmic graph, which led to the discovery of the $5/3$ law in turbulence theory
In Fig. 1 we show 12 heptagonal faces of the fundamental domain of the surface \( M' \) on \( M \) and their neighbours; the folding consists in gluing \( A \) and \( \tilde{A} \) together along the thick line bounding the fundamental domain. The branch points of the folding \( M \to M' \) are the central points of the segments \((A\tilde{A})\), where the segments are \((3, 11)\) in the domain XI, \((23, 22)\) in the domain I, \((6, 9)\) in the domain XII, and \((15, 16)\) in the domain V.

It would be also of interest to determine the complex structures of the surfaces \( M \) and \( M' \) in terms of the combinatorics of the group \( G \), because in this case the combinatorics could be related to the geometry and arithmetics of elliptic functions.

§ 10. Statistics of the Fermat–Euler periods

We describe here the dependence on the modulus \( n \) for the least period \( T(n) \) of the arithmetic progression

\[
\{2^t \pmod n, \ t = 1, 2, \ldots, T\}
\]

for odd numbers \( n \leq 2001 \). The calculations were carried out by F. Aicardi by using a computer.

To smooth the chaotic deviations from the averaged behaviour, the graph shows the value of the sum

\[
S(n) = \sum_{k=1}^{n} T(k),
\]

which is proportional to the Cesàro mean, rather than the rapidly oscillating value of the period \( T(n) \), and this is shown in the bilogarithmic scale (in the axes \( \log n \) and \( \log S \)).

Figure 2 is a number-theoretic analogue of the technique used by Kolmogorov to discover the ‘5/3 law’ in turbulence theory. Kolmogorov’s original graph is shown in Fig. 3.

Bibliography

[1] V. I. Arnol’d, The Euler groups and arithmetics of geometric progressions, Moscow Centre of Continuous Math. Education, Moscow 2003. (Russian)

[2] V. I. Arnol’d, “Fermat–Euler dynamical systems and the statistics of the arithmetics of geometric progressions”, Funktsional. Anal. i Prilozhen. 37:1 (2003), 1–18; English transl., Funct. Anal. Appl. 37 (2003), 1–15.

[3] V. I. Arnol’d, “Ergodic arithmetical properties of geometric progressions dynamics”, Moscow Math. J. (2004) (to appear).

[4] V. I. Arnol’d, “The topology of algebra: combinatorics of squaring”, Funktsional. Anal. i Prilozhen. 37:3 (2003), 3–16; English transl., Funct. Anal. Appl. 37 (2003), 177–190.
[5] V. I. Arnol’d, *Arithmetics of binary quadratic forms, symmetry of their continued fractions, and geometry of their de Sitter world*, Moscow Centre of Continuous Math. Education, Moscow, Dubna 2002; *Bol. Soc. Brasil. Mat. (N.S.)* **34**:1 (2003), 1–41.

[6] V. I. Arnol’d, “Weak asymptotics of the numbers of solutions of Diophantine problems”, *Funktsional. Anal. i Prilozhen.* **33**:4 (1999), 65–66; English transl. in *Funct. Anal. Appl.* **33** (2000), 292–293.

Steklov Institute of Mathematics,
Russian Academy of Sciences

*E-mail address*: arnold@ceremade.dauphine.fr

Received 5/JAN/03
Translated by IPS(DoM)