WHEN ARE ALL GROUPS OF ORDER N CYCLIC?

D. Baranov, A. Klyachko, K. Kokhas, A. Skopenkov and M. Skopenkov

A group is a nonempty set of transformations (= permutations or rearrangements of elements) of some set such that it is closed with respect to compositions of transformations and taking the inverse transformation. (i.e., if $f,\, g \in G$ then $f \circ g \in G$ and $f^{-1} \in G$). We say that a group G is *cyclic*, if there exists a transformation $g \in G$ such that $G = \{g, g^2, \dots, g^n, \dots\}$.

This set of problems is devoted to the following intriguing question:

For which n an arbitrary group of n permutations is cyclic?

Examples of (finite) groups.

(1) The group S_n of *all* permutations of a n-element set. It is called a *symmetric group*.

(2) The group $\{\mathrm{id}, (13)(24), (1234), (1432)\}$ of transformations of a set consisting of 4 elements.

(3) Consider a square on the plane and all the transformations of the plane that map the square onto itself. These are the identity transformation, 3 rotations and 4 symmetries; 8 transformations in all. Let the group consist of 8 permutations of the set of vertices of the square induced by these 8 transformations.

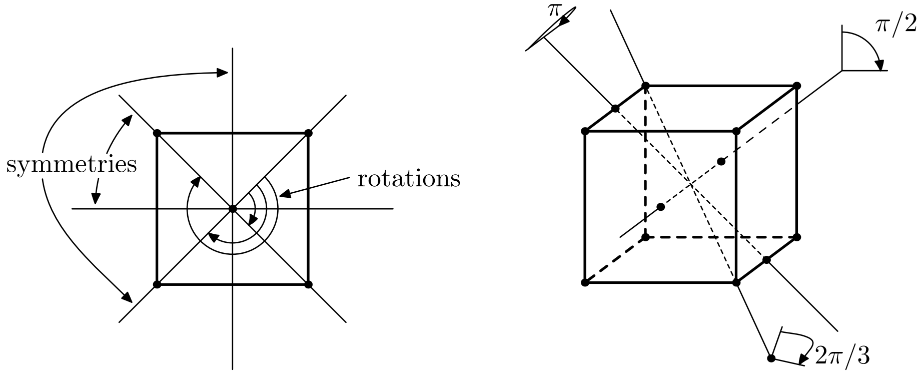

Figure: transformations of a square and a cube.

(4) Consider a cube in the 3-dimensional space and all the rotations of the space mapping the cube onto itself.

(a) Consider the group of all permutations of the set of *vertices* of the cube induced by these rotations.

(b) Consider the group of all permutations of the set of *edge midpoints* of the cube induced by these rotations.

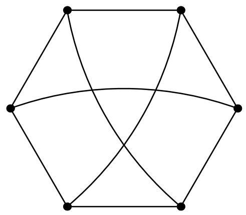

Figure: the graph $K_{3,3}$

(5) The group of all permutations of the 6-element set of vertices of the graph $K_{3,3}$ which are isomorphisms of the graph.

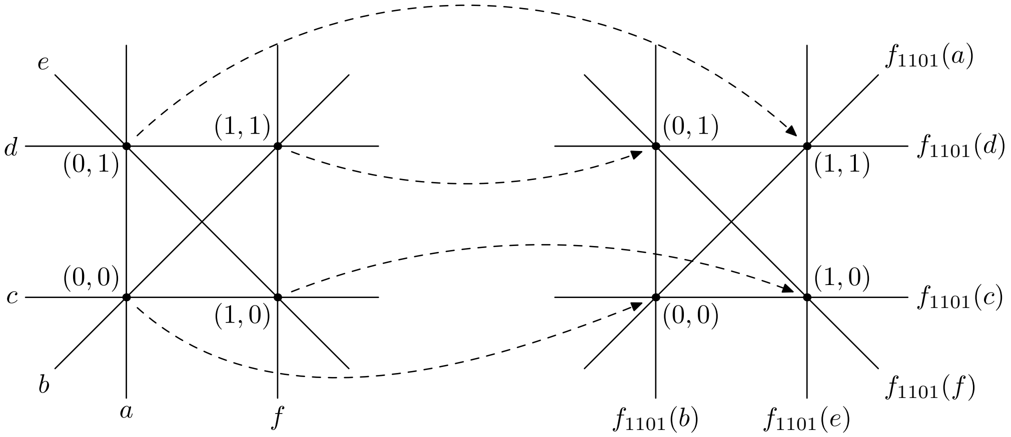

Figure: linear transformation $f_{1101} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$

(6) Consider the set $\mathbb{Z}_2^2 = \{(0,0),(0,1),(1,0),(1,1)\}$ of ordered pairs of residues modulo 2. For any 4 residues a, b, c, d consider a transformation $f_{abcd} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ defined by the formula $f_{abcd}(x,y) = (ax+by, cx+dy)$. The set of invertible transformations of this form is a group.

General remarks. If the condition of the problem consists of a single statement, you have to prove this statement. If the problem looks like too difficult, try to solve the neighboring problems, they can contain hints.

Star-mining. A team gets a star for each correct ($\geqslant +$.) written solution. Jury may also award stars for elegant solutions, for solutions of difficult problems and for (some) solutions written in TEX. The jury has infinite number of stars. A team may present the solution orally paying 1 star for each attempt.

BEFORE. 1st series

1.1. (a) A combination lock can be opened by a 9-digit combination. It happens that if two combinations A and $B = b_1 b_2 \dots b_9$ open the lock ($A = B$ is allowed), then the combination obtained from A by replacing its every digit k (simultaneously for all k) with the digit b_k opens the lock too. It is known that the lock can be opened by the combination 856291473 and the combinations obtained by (multiple) applying the above rule only. How many combinations open the lock?

(b) The same question for the following rule. If the combination A opens the lock and B is an arbitrary combination ($A = B$ is allowed), then the combination obtained from A by replacing (simultaneously for each k) the digit in the combination A that equals the number of the position of the digit k in combination B with b_k.

1.2. (a) Prove that the set in the example 6 is indeed a group.

(b) What groups in the examples above are cyclic?

(c) Every group contains the identity transformation. It is called *unity* and is denoted by e.

1.3. (a) Construct a group that contains two permutations a and b such that $ab = b^{-1}a$.

(b) The alphabet of Ababa tribe consists of two letters «a» and «b». No word change the sense if we insert or delete at any place in this word the fragments «aab» or «bba». 4 words of Ababa language are scratched on the rock. Prove that two of them have the same sense.

1.4. (a) Construct a group of 17 permutations numbered by numbers 0, 1, ..., 16, such that the number of composition of any two permutations equals the sum of the numbers of these permutations modulo 17.

(b) Construct a group of 16 permutations numbered by numbers 1, 2, ..., 16, such that the number of composition of any two permutations equals the product of the numbers of these permutations modulo 17.

(c) Does there exist a group of 8 permutations, that can be numbered by numbers 1, 2, 4, 7, 8, 11, 13, 14 so that the number of composition of any two permutations equals the product of the numbers of these permutations modulo 15?

1.5. Determine for the following values of n whether every group of n permutations is cyclic.
(7) 1,2,3,4,5,6,7; (8) 8; (9) 9; (10) 10; (12) 12; (15) 15; (21) 21; (1001) 1001.

> Denote by $|X|$ the number of elements in the set X. The group G is called *commutative* if $xy = yx$ for each x, $y \in G$. *The order* of an element $a \in G$ is the minimal positive integer n such that $a^n = e$ (where e is the identity). If the order exists then it is denoted by $\operatorname{ord} a$.

1.6. (a) *Fermat–Euler theorem.* If G is a commutative group, e is its unity, then $a^{|G|} = e$ for each $a \in G$.
(b) Every cyclic group is commutative.
(c) Is the opposite statement true?

1.7. If the number of elements of a group is prime then the group is cyclic.

1.8. (a) Find the order of each element in the group S_4.
(b) The order is well-defined for each element of a finite group.
(c) If a group contains an element of order 2 then the number of elements in the group is even.
(d) If a group contains an element of order 3 then the number of elements in the group is divisible by 3.
(e) *Lagrange theorem.* The number of elements of a finite group is divisible by the order of every its element.
(f) If the number of elements in G is even then G contains an element of order 2.

1.9. (a) If $n > 2$ is even then there exists a noncyclic group of n permutations.
(b) If n is divisible by the square of a prime number then there exists a noncyclic group of n permutations.

1.10. (a) Each commutative group of 10 elements is cyclic.
(b) The same is true for each 21-element group.
(c) The same is true for each 1001-element group.
(d) For which n every commutative group of n elements is cyclic?

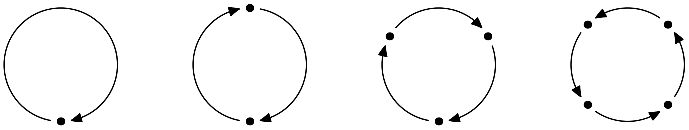

Figure: a permutation of type $\langle 1, 2, 3, 4\rangle$

1.11. If a permutation of a $(n_1+\ldots+n_k)$-element set is a composition of nonintersecting cycles of order n_1, $\ldots$, n_k, we call it a permutation *of type* $\langle n_1, \ldots, n_k\rangle$.
(a) Prove that any two permutations f and g of the same type are conjugate in the group S_n, that means that $g = b^{-1}fb$ for a suitable permutation $b \in S_n$.
(b) Prove the opposite statement.
(c) The conjugate permutations have the same orders.

1.12. Let G be a group of 15 elements.
(a) G contains an element of order 3.
*(b) Each element of order 5 in G can be conjugate with its powers only.

2. BEFORE. 2nd series.

Solution of Problem 1.2. $f \in G \quad\Rightarrow\quad f^{-1} \in G \quad\Rightarrow\quad ff^{-1} = e \in G.$

Solution of Problem 1.5-7 for $n = 3$. Assume the converse: there is a noncyclic group G consisting of 3 permutations. Denote by a one of the permutations distinct from the identity. If $a^2 \neq e$ then the permutations a, a^2, a^3 are distinct and hence the group G is cyclic. If $a^2 = e$ then take a permutation $b \in G$ distinct from e and a. Then the permutation ab is distinct from e, a, b. (Indeed, obviously $ab \neq a$ and $ab \neq b$. If $ab = e$ then $b = a^2b = a$, a contradiction.) This contradiction proves the problem.

Solution of Problem 1.5-10. Answer: the group is not necessarily cyclic.

Consider a regular pentagon in the plane and all the isometries of the plane that map the pentagon onto itself. These motions are the identity, 4 rotations and 5 symmetries, 10 transformations at all. Consider permutations of the vertices of the pentagon under these transformations. These 10 permutations form a noncyclic group, and for any two symmetries s and t we have $st \neq ts$. That means that the group is noncyclic, because if $s = g^k$ and $t = g^l$ for some g, then $st = ts = g^{k+l}$.

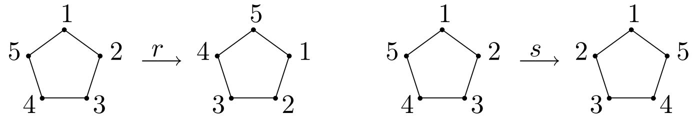

Figure: transformations of a regular 5-gon

Another solution of Problem 1.5-10. (It can be useful for solving Problem 2.1.) Let r be a rotation by $2\pi/5$ of the regular pentagon, s be a symmetry (see fig. 2). Then $r^5 = e = s^2$ and $sr = r^{-1}s$. Consider 10 transformations $r^k s^l$, $k = 0, 1, 2, 3, 4$ and $l = 0, 1$. Due to the relation $sr = r^{-1}s$ one can obtain that this set of transformations is a group. (This step is the main difference with the previous solution. We check that the set is a group algebraically but not geometrically. Therefore we can use the similar ideas when the objects have no geometrical interpretations.) The same relation allows to establish that the group is noncyclic.

2.1. (a) There exists a noncyclic group of 21 elements.

(b) There exists a noncyclic group of 55 elements.

(c) If p and q are primes and $q - 1$ is divisible by p, then there exists a noncyclic group of pq elements.

Hint to the problem 2.1a. Choose the relations for elements r and s that provide the set $r^k s^l$, $k, l \in \mathbb{Z}$ to be a noncyclic group of 21 element, then construct the suitable permutations.

A subgroup of the group G is a subset of G that is a group itself.

2.2. (a) Can a commutative group of 10 elements contain two elements of order 2? (This is a hint to the problem 1.10a.)

(b) *Lagrange theorem.* The number of elements of a finite group is divisible by the number of elements of any its subgrouop.

2.3. (Hint to the problem 1.12b.) Let G be a group of 15 elements and f, $g \in G$ be its elements of order 5.

(a) The sets $\{f, f^2, f^3, f^4\}$ and $\{g, g^2, g^3, g^4\}$ either coincide or do not intersect.

(b) One of the elements f, g is a power of the other.

2.4. Let G be a group of 15 elements, $f \in G$ be an element of order 5, $b \in G$, $b^{-1}fb = f^m$ and $k \in \mathbb{Z}$, $k > 0$. Then $b^{-1}f^k b = f^{km}$ and $b^{-k}fb^k = f^{m^k}$.

2.5. Let G be a group of 15 elements such that all its elements (except the unity) have order 3. Let f, $g \in G \setminus \{e\}$.

(a) The sets $\{f, f^2\}$ and $\{g, g^2\}$ either coincide or do not intersect.

(b) If $\{f, f^2\} \neq \{g, g^2\}$, then $fg \neq gf$.

(c) Every $f \in G$, $f \neq e$, has exactly 4 conjugate elements.

(d) This group does not exist.

2.6. (a) If the number of elements of G equals pq, where p and q are primes, $p < q$ and $q - 1$ is not divisible by p, then the group is cyclic.

(b) Let G be a group of 1001 elements and $f \in G \setminus \{e\}$ is an element that is conjugate with its powers only. Prove that G is cyclic.

3. BEFORE. Series 3

These funny problems in an abstract way describe the idea that was given in the hint to Problem 2.1a. Formally we do not need them for our main goal.

3.1. [1] There are two letters in Cyclists' language: a and a^{-1}. They are called *opposite.*

A *Word* in Cyclists' and other considered languages is defined as an ordered collection of letters; in particular, there is an *empty* word – word with no letters (silence haves a sense).

The word that consists of eight letters a is *indecent.* The word that consists of two opposite letters is named *stumble.*

In Cyclists' and other languages that we consider sense of a word does not change after

- inserting an indecent word or a stumble or
- deleting an indecent word or a stumble.

(Scientifically, sense is equivalence class of words with respect to inserting and deleting indecent words and stumbles operations.)

For example, words $aaaa^{-1}a$ and aaa are different but have the same sense.

(a) There are only 8 senses in Cyclists' language.

(b) Cyclists speak about residue classes modulo 8. In other words, the set of all senses with operation of concatenation is *isomorphic* to the set of all residue classes modulo 8 with sum operation.

Exact wording of this statement is as follows. We may concatenate words: X and Y gives XY. (For example, aa and $aa^{-1}a$ gives $aaaa^{-1}a$.) The operation of concatenation of words sets operation of concatenation of senses. So, there is a correspondence between residue classes to senses such that residue class of XY is the sum of residue classes of words X and Y.

3.2. In order to provide secrecy the Pentagon's workers created a language. There are four letters a, b, a^{-1} and b^{-1}. Letters a and a^{-1} are called *opposite.* Letters b and b^{-1} are opposite too. Five a letters or two b letters form an indecent word. ... is an indecent word too. It consists of 4 letters, first three letters are first three letters of $abab$ and last three letters of this word are last three letters of $a^{-1}bbab^{-1}$.

(a) The Pentagon's workers language has 10 senses.

(b) They speak about isometries of regular Pentagon. Give an exact wording of this statement.

3.3. Connoisseurs' of Perfection language has 4 letters a, b, a^{-1} and b^{-1}. Three a letters or two letters b form an indecent word. ... is an indecent word too. It has 10 letters and it is a concatenation of 5 copies of ba.

(a) Connoisseurs' of Perfection language has a finite number of senses.

(b) Connoisseurs of Perfection speak about a group. Give an exact wording of this statement.

3.4. (a) In Algebraists' language there are 4 letters a, b, a^{-1} and b^{-1}. We will not describe indecent words or even tell if there is a finite number of indecent words or not because they are indecent. Prove that algebraists speak about a group. Give an exact wording of this statement. (This group is able to be infinite even if there is a finite number if indecent words.)

(b) If we add 2 new letters c and c^{-1} to the Algebraists' language and some new indecent words, they will all the same speak about a group.

[1] This is an example of an *ugly* mathematical problem. Understanding it's conditions is more difficult then solving it. However, this problem is necessary because it helps us to introduce an important construction.

4. AFTER. Series 4

Some Solutions.

1.8. (e) *The proof of the Lagrange Theorem.* For $x \in G$ consider the set $\{x, xf, xf^2, \dots, xf^{\operatorname{ord} f - 1}\}$. These elements are different by definition of order. Thus this set has $\operatorname{ord} f$ elements. If $xf^k = yf^l$ then $y = xf^{k-l}$. Thus for different x these sets either are equal or do not intersect. So $\operatorname{ord} f$ divides $|G|$.

1.10. (a) Denote by p the order of a nonidentity element f. If $p = 10$ then the group is cyclic. Assume that $p < 10$. By Lagrange's Theorem $p \in \{5, 2\}$. If there exists an element g of order $10/p$ then $G = \{fg, (fg)^2, \dots, (fg)^{10}\}$. Else there is an element $g \notin \{f, f^2, \dots, f^p\}$ of order p. Then $\{f^k g^l\}_{k,l\in\mathbb{Z}}$ is a subgroup of order p^2. Contradiction to Lagrange's Theorem.

1.11. *Hint.* Change the numeration of the elements of the set to transform f into g. The change of numeration determines the required permutation b.

2.3. (a) Suppose that the two given sets intersect. Then there are integers $1 \le k, l \le 4$ such that $f^k = g^l$. Since $\mathrm{GCD}(k, 5) = 1$ it follows that there is an integer m such that $5 \,|\, km - 1$. Then $f = f^{km} = (f^k)^m = (g^l)^m = g^{lm}$. This implies that the two given sets are equal.

(b) Consider 25 elements $f^k g^l$, where $1 \le k, l \le 5$. Since the entire group has only 15 elements, it follows that there are $1 \le k, l, m, n \le 5$ such that $(k, l) \ne (m, n)$ and $f^k g^l = f^m g^n$. Multiplying by f^{-m} from the left and by g^{-l} from the right, we get $f^{k-m} = g^{n-l}$. Since f and g have order 5 it follows that the sets $\{f, f^2, f^3, f^4\}$ and $\{g, g^2, g^3, g^4\}$ intersect. Then by assertion (a) the sets coincide, and the problem follows.

2.5. (c) *Hint.* Take an element $f \ne e$. Let $c(f)$ be the number of elements conjugate to f (including the element f itself). Consider the set $Z(f) := \{g \in G : fg = gf\}$. By assertion (b) it follows that this set is $\{e, f, f^2\}$. Now apply the following general result: $c(f) \cdot |Z(f)| = |G|$. Thus $c(f) = 15/3 = 5$.

2.1. (a) *New hint.* This group is a group of some permutations of the (49-element) set $\mathbb{Z}_7^2$. In order to define this group let us represent such elements as pairs (x, y) of residue classes modulo 7. For non-negative integers k, l define a map

$$f_{k,l} : \mathbb{Z}_7^2 \to \mathbb{Z}_7^2 \quad \text{by} \quad f_{k,l}(x, y) := (2^k x, lx + y).$$

Check that

- there are exactly 21 such maps;
- they form a group;
- this group is not cyclic.

2.1. (b) *Hint.* Observe that $2^5 = 33 - 1$. For nonnegative integers k, l define a map $f_{k,l} : \mathbb{Z}_{11}^2 \to \mathbb{Z}_{11}^2$ by $f_{k,l}(x, y) := (4^k x, lx + y)$.

3.3. *Hint.* Use that Connoisseurs of Perfection are Algebraists.

3.4. *Hint.* Map each sense to the transformation of the set of senses defined as «left concatenation».

New problems

4.1. There exists a noncyclic group of 39 elements.

4.2. Let G be a group with 1001 elements and $f \in G - \{e\}$. Suppose that f is conjugated only with its exponents. Let $g \notin \langle f\rangle := \{f, f^2, \dots, f^n, \dots\}$. Denote by q the smallest positive integer n such that $g^n \in \langle f\rangle$.

(a) $\operatorname{ord} g$ is divisible by q. (b) If $g^{-1}fg = f^k$ then $g^{-n}fg^n = f^{k^n}$.

(c) $g^{-1}fg = f$. (d) $\{fg, (fg)^2, (fg)^3, \dots, (fg)^{q \operatorname{ord} f}\}$ is a subgroup of G.

4.3. Let G be a noncyclic group of 1001 elements.

(a) Each element of G is contained in a subgroup maximal by inclusion and different from G.

Such subgroups are called *maximal.*

(b) Each maximal subgroup is cyclic.

4.4. The *commutativiser* of a group G is the set

$$Z = Z(G) := \{a \in G \ : \ ga = ag \text{ for any } g \in G\}$$

of elements that commute with all elements.

(We hope that the word "commutativiser" is more accessible for beginners than *center.*)

(a) Find $Z(S_n)$ for each $n = 2, 3, 4, \dots$

(b) The commutativiser is a subgroup.

4.5. Let G be a noncyclic group of 1001 elements. Assume that the generator of each maximal subgroup is conjugate not only to its powers.

(a) Every maximal subgroup contains the commutativiser.

(b) Find the number $a(F)$ of elements that are conjugate to some element of given maximal subgroup F, if $|F|$ and $|Z|$ are known.

5. AFTER. Series 5

Hint to the problem 1.4c. Try to choose a suitable subgroup in the group of permutations of the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

5.1. (a) For any group G and an element $g \in G$ the set

$$N(g) = N_G(g) := \{a \in G \ : \ ga = ag^k \text{ for some } k\}$$

is a subgroup.

(b) Determine $N_{S_3}(g)$ for each $g \in S_3$.

(c) The number of subgroups conjugated to $\langle g\rangle$ equals $|G|/|N(g)|$.

A *generator* of a finite cyclic group G is any element g such that G consists of powers of g. (A generator needs not to be unique.)

5.2. Let G be a noncyclic group of 1001 elements. Assume that certain generator of each maximal subgroup is conjugated not with its powers only.

(a) The intersection of any two maximal subgroups is exactly the center of the group.

(b) The number of subgroups conjugated to maximal subgroup F equals $1001/|F|$.

(c) Denote by $\widehat{F}$ the number of elements of G conjugate to elements of a maximal subgroup F and not contained in the commutativizer. Prove that $500 < \widehat{F} \le 1000 - |Z|$.

Primitive root theorem. For any prime p there exists a non negative integer g such that all the residues modulo p of g^1, g^2, g^3, …, $g^{p-1} \equiv 1$ are distinct.

5.3. *Proof of the theorem.* Let p be a prime and let a be a non negative integer that is not divisible by p.

(a) $p - 1$ is divisible by the minimal $k > 0$ for which $a^k \equiv 1 \bmod p$.

(b) for any two positive integers n and a the congruence $x^n \equiv a \bmod p$ has at most n solutions.

(c) If $p - 1$ is divisible by d, then the congruence $x^d \equiv 1 \bmod p$ has exactly d solutions.

(d) Prove the primitive root theorem for $p = 2^m + 1$.

(e) Prove the primitive root theorem for $p = 2^m \cdot 3^n + 1$.

(f) Prove the primitive root theorem for an *arbitrary* prime p.

(g)* Is it true that the number 3 is a primitive root modulo $p = 2^m + 1$?

5.4. For which n any group of n elements is commutative?

6. Solutions

1.8. (d) Let a be the element of order 3. Make a list of all the elements of the finite group. Let us cross out the elements from the list as follows. At each step, choose an element x which has not been crossed out yet, and cross out each of the 3 elements x, xa, and xa^2. This procedure never leads to crossing out an element more than once. Indeed, assume that, say, xa has already been crossed out. This implies that for element y chosen before we have either $xa = y$, or $xa = ya$, or $xa = ya^2$. But then either $x = ya^2$, or $x = y$, or $x = ya$, respectively. Thus x must also have been crossed out before according to our rule, a contradiction. Thus exactly 3 elements are removed at each step. Since the group is finite, the process ends in a finite time. This implies that the number of elements in the list (and hence in the group) is divisible by 3.

1.12. *Hint.* See Problem 2.3.

2.1c. This group is a group of some permutations of the (q^2-element) set $\mathbb{Z}_q^2$. In order to define this group let us represent such elements as pairs (x, y) of residue classes modulo q. By the primitive root theorem there exists an element $a \in \mathbb{Z}_q$ of order p. For nonnegative integers k, l define a map $f_{k,l} : \mathbb{Z}_q^2 \to \mathbb{Z}_q^2$ by $f_{k,l}(x, y) := (a^k x, lx + y)$ Check that

- there are exactly pq such maps;
- they form a group;
- this group is not cyclic.

3.1. *Hint.* Given a word, define the *number of its meaning* to be the difference between the quantities of letters a and a^{-1} in the word modulo 8.

3.2. *Hint.* The bijection between the meanings and isometries of the regular pentagon is constructed as follows. Assign to the letter a a counterclockwise rotation through 72° about the center of the pentagon. To the letter b assign a suitable reflection so that the relation $a \circ b \circ a \circ b^{-1} = id$ holds. Now interpret each word as the composition of the corresponding isometries.

3.3b. *First solution.* This follows from problem 3.4a.

3.3b. *Second solution.* Connoisseurs of Perfection talk about the group of those permutations of the vertices of a regular icosahedron which are obtained from the isometries of 3-space taking the icosahedron into itself. That is, about the group A_5.

4.2. (b) This follows by induction over n.

5.3. *Hints.* (b) Let us prove the following more general statement: a polynomial of degree n cannot have more than n roots in $\mathbb{Z}_p$. Here by a polynomial we mean the collection of coefficients but not the function.

Assume that a polynomial $P(x)$ of degree n has in $\mathbb{Z}_p$ different roots $x_1, \dots, x_n, x_{n+1}$. Represent $P(x)$ as

$$P(x) = b_n(x - x_1) \dots (x - x_n) + b_{n-1}(x - x_1) \dots (x - x_{n-1}) + \dots + b_1(x - x_1) + b_0$$

('*the Newton interpolation*'). Put in the congruence $P(x) \equiv 0\ (p)$ residues $x = x_1, \dots, x_n, x_{n+1}$ in this order. We obtain $b_0 \equiv b_1 \equiv \dots \equiv b_{n-1} \equiv b_n \equiv 0\ (p)$.

The same solution can be presented in the following way. Let P be a polynomial. Then polynomial $P - P(a)$ is divisible by $x - a$, i.e. $P - P(a) = (x - a)Q$ for some polynomial Q such that $\deg Q < \deg P$. Since $P(a) = 0$, it follows that $P = (x - a)Q$ for some polynomial Q of degree less than $\deg P$. Now the required statement can be proved by induction over the degree of the polynomial P.

(c) Obviously, polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p$ has exactly $p - 1$ roots and is divisible by $x^d - 1$. Prove that if a polynomial of degree a has a roots and is divisible by a polynomial of degree b, then the polynomial of degree b has exactly b roots.

(d) If there are no primitive roots, then by problem 2a the congruence $x^{2^{m-1}} \equiv 1\ (p)$ has $p - 1 = 2^m > 2^{m-1}$ solutions.

(e),(f) Similarly to (d).

5.4. *Hint.* All groups of order n are abelean if and only if the prime decomposition of this number $n = p_1^{k_1} \dots p_l^{k_l}$ has the following properties:

- $k_i < 3$;
- p_i does not divide $p_j^{k_j} - 1$.

You can prove this by the same way, but in the case 1 you need the following fact: any finite abelean group is a direct product of cyclic subgroups.

The remaining problems are covered by the supplied paper [BKS].

References

[A] V.I. Arnold, Ordinary differential equations, M, Nauka, 1984.

[B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/ kbrown/4340/cyclic_only_orders.pdf

[BKS] V. Bragin, Ant. Klyachko, A. Skopenkov, When any group of n elements is cyclic?

[KS] L.A. Kaluzhnin, V.I. Sluschanskiy, Transformations and permutations. M.: 1979, 112 pages.

[KM] M.I. Kargapolov, Yu.I. Merzlyakov, Foundations of group theory. M.: Nauka, 1982. http://arhivknig.com/obrazovanie/87077-osnovy-teorii-grupp.html

[K] A.I. Kostrikin, Introduction to algebra. Foundations of algebra, 1994.