Abstract algebra. Final exam. 05.19.08.

YOUR NAME: Alexander Givental

Let F be a finite field of order 49, R be the ring $\mathbf{Z}/144\mathbf{Z}$ of residues modulo 144.

1. Show that the multiplicative groups $F^\times$ and $R^\times$ have the same order N and find this N.

$$|F^\times| = 49 - 1 = 48;\ |R^\times| = \phi(144) = \phi(3^2 2^4) = (3-1)3(2-1)2^3 = 48.$$

2. Classify all abelian groups of order N up to isomorphism. Which of these groups are isomorphic to $F^\times$?

$$\mathbf{Z}_3 \times \mathbf{Z}_{16},\ \mathbf{Z}_3 \times \mathbf{Z}_8 \times \mathbf{Z}_2,\ \mathbf{Z}_3 \times \mathbf{Z}_4^2,\ \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_2^2,\ \mathbf{Z}_3 \times \mathbf{Z}_2^4.$$

The multiplicative group of a finite filed is always cyclic, and hence $F^\times \cong \mathbf{Z}_{48} \cong \mathbf{Z}_3 \times \mathbf{Z}_1 6$.

3. Prove that the ring R is isomorphic to the cartesian product of the rings $\mathbf{Z}/9\mathbf{Z}$ and $\mathbf{Z}/16\mathbf{Z}$.

The homomorphism $\mathbf{Z}_{144} \to \mathbf{Z}_9 \times \mathbf{Z}_{16}$ of rings of the same order $144 = 9 \times 16$, defined by assigning to a residue $\bar{n}$ of an integer n modulo 144 the pair (a, b) of residues of n modulo 9 and 16 respectively, has the trivial kernel (since $(9, 16) = 1$), and is therefore an isomorphism.

4. Use **3** in order to find the place of $R^\times$ in your classification.

From **3**, we have: $\mathbf{Z}_{144}^\times = \mathbf{Z}_9^\times \times \mathbf{Z}_{16}^\times$. Furthermore, $\phi_9 = 6$, so that $\mathbf{Z}_9^\times \cong \mathbf{Z}_6$, while $\phi(16) = 8$. The group $\mathbf{Z}_{16}^\times = \{1, 3, 5, 7, -7, -5, -3, -1\}$, as it is easy to check, has no elements of oredr 8, but has elements of order 4, and hence is isomorphic to $\mathbf{Z}_4 \times \mathbf{Z}_2$. Thus $R^\times \cong \mathbf{Z}_6 \times \mathbf{Z}_4 \times \mathbf{Z}_2 \cong \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_2^2$.

5. Construct explicitly a field F of order 49 and point out a generator of the group $F^\times$. How many choices of such a generator are available in the group $F^\times$?

$F = \mathbf{Z}_7[i] \cong \mathbf{Z}_7[x]/(x^2+1)$ is a field (of order 49); indeed, $x^2 + 1$ is irreducible over $\mathbf{Z}_7$, because the integer prime $7 \cong 3 \pmod 4$. The number of generators in the cyclic group $F^\times \cong \mathbf{Z}_{48}$ is equal to $\phi(48) = \phi(3) \cdot \phi(16) = (3-1) \cdot (2-1)2^3 = 16$. One of them is $3 + i$. Indeed, $(3+i)^{24} \cong (1-i)^{12} = (-2i)^6 \cong 3^3 \cong -1 \mod 7$, i.e. the order of $3 + i$ in $F^\times$ is equal to 48.

Find all those n for which the permutation group S_n contains:

6. a subgroup of order 60;

The alternating group $A_5 \subset S_5$ has order $5!/2 = 60$ and for $n \geq 5$ is contained in any $S_n \supset S_5$. No subgroups of order 60 exist in S_n with $n < 5$ since then $|S_n| < 60$.

7. a cyclic subgroup of order 60.

Since the order of a permutation is equal to the least common multiple of the lengths of its cycles, such least common muliple is equal to $60 = 3 \times 4 \times 5$ for a permutation with three cycles of lengths $3, 4, 5$, which first occurs in $S_{3+4+5} = S_{12}$. Thus, for $n \geq 12$, the group S_n contains the required cyclic subgroup, and for $n < 12$ does not.

8. For any field F, find the greatest common divisor in $F[x]$ of the polynomials $x^m - 1$ and $x^n - 1$.

When $m \geq n$, write $m = qn + r$ where $0 \leq r \leq n$. Then, dividing $x^m - 1$ by $x^n - 1$ we find the remainder $x^r - 1$. Hence the steps of the Euclidean algorithm for the integers m and n govern the steps of the Euclidean algorithm for the polynomials $x^m - 1$ and $x^n - 1$. Thus, if $d = (m, n)$, we have: $(x^m - 1, x^n - 1) = x^d - 1$.

9. Trisect the angle $\pi/7$ using only straightedge and compass.

$$\frac{\pi}{3} - 2\frac{\pi}{7} = \frac{(7 - 2 \cdot 3)\pi}{21} = \frac{\pi}{21}.$$

10. To commemorate two centuries of Gauss' *Disquisitiones Arithmeticae* the Institute of Mathematical History is selling necklaces priced \$62.50 each and consisting of 17 identically shaped symmetrical black or white beads moving freely on a circular band. Find the price the Institute of Historical Mathematics will have to pay for a complete collection of such necklaces.

Identify the beads with vertices of a regular 17-gon and consider the set of 2^{17} possible colorings. The dihedral rotation group D_{17} of the regular 17-gon in the space acts on the set of colorings. A complete collection consists of representatives of orbits of this action. To compute the number of orbits we may use the Cauchy counting theorem which identifies the number of orbits with the average number of fixed points of the group elements. The identity element has all 2^{17} colorings fixed. The rotation of the 17-gon through the angle $2\pi k/17$ with any $k = 1, 2, ..., 16$ generates the whole rotation subgroup

(since 17 is prime) and thus has only 2 fixed points: the entire necklace has to be either black or white. The reflection about any of the 17 symmetry axes leaves one of the beads in its place and transposes 8 remaining pairs. The color within each pair has to be the same, but the 8 colors of the pairs as well as the color of the fixed bead can be arbitrary. Thus each reflection leaves 2^9 colorings fixed. Summing up the answers over all elements in D_{17} and dividing by their total number 34 we find the number of orbits:

$$\frac{2^{17} + 16 \cdot 2 \cdot + 17 \cdot 2^9}{34} = \frac{(2^{17} - 2) + 17 \cdot 2(2^8 + 1)}{34} =$$

$$(2^8 + 1)(\frac{2^8 - 1}{17} + 1) = 257(15 + 1) = 257 \cdot 16.$$

Thus the total price of the collection is $257 \times 16 \times \$62.50 = \$257,000$.