SOLUTIONS OF SOME HOMEWORK PROBLEMS
MATH 114

Problem set 1

4. Let D_4 denote the group of symmetries of a square. Find the order of D_4 and list all normal subgroups in D_4.

Solution. D_4 has 8 elements:

$$1, r, r^2, r^3,\ d_1, d_2, b_1, b_2,$$

where r is the rotation on 90°, d_1, d_2 are flips about diagonals, b_1, b_2 are flips about the lines joining the centers of opposite sides of a square. Let N be a normal subgroup of D_4. Note that

$$d_1 = rd_2r^{-1},\ b_1 = rb_2r^{-1},\ d_1d_2 = b_1b_2 = r^2.$$

Hence if $d_1 \in N$, then $d_2 \in N$, similarly for b_1, b_2. Note that $d_1b_1 = r$. Thus, if N contains a flip and $N \neq G$, then N either contains d_1, d_2 or contains b_1, b_2. Let N contain d_1 and d_2, then $N = \{1, d_1, d_2, r^2\}$. In the same way if N contains b_1 and b_2, then $N = \{1, b_1, b_2, r^2\}$. Finally, if N does not contain flips, then $N = \{1, r, r^2, r^3\}$ or $N = \{1, r^2\}$. Thus, D_4 have one 2-element normal subgroup and three 4-element subgroups. Then, as always, there are normal subgroups $\{1\}$ and D_4.

6. Show that the n-cycle (1...n) and the transposition (12) generate the permutation group S_n, i.e. every element of S_n can be written as a product of these elements.

Solution. Let $s = (12)$, $u = (1 \dots n)$. It is easy to check that

$$usu^{-1} = (23)\,,\ u^2su^{-2} = (34)\,, \dots, u^{n-2}su^{2-n} = (n-1, n)\,.$$

Thus, any subgroup of S_n which contains u and s must contain all adjacent transpositions. But the adjacent transpositions generate S_n. Hence s and u generate S_n.

7. Find a cyclic subgroup of maximal order in S_8.

Solution. The order of $s \in S_n$ equals the least common multiple of the lengths of the cycles of s. For $n = 8$, the possible cycle lengths are less than 9. By simple check we see that a product of disjoint 3-cycle and 5-cycle has the maximal order 15. Hence $\mathbb{Z}_{15}$ is a maximal cyclic group in S_8.

Problem set 2

1. An *automorphism* of a group G is an isomorphism from G to itself. Denote by $\operatorname{Aut} G$ the set of all automorphisms of G.

(a) Prove that $\operatorname{Aut} G$ is a group with respect to the operation of composition.

Date: February 22, 2006.

(b) Let G be a finite cyclic group. Describe $\operatorname{Aut} G$.

(c) Give an example of an abelian G such that $\operatorname{Aut} G$ is not abelian.

Solution. The part (a) is a straightforward check. For (b) let $G = \mathbb{Z}_n$. If $\phi \in \operatorname{Aut} G$, then ϕ is determined by $\phi(1)$, as

$$\phi(k) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = k\phi(1).$$

It is easy to check now that ϕ is injective if and only if $\phi(1)$ and n are relatively prime. Let

$$\mathbb{Z}_n^\times = \{s \mid 0 < s < n, (s, n) = 1\},$$

with operation of multiplication $\mod n$. The map $\operatorname{Aut} \mathbb{Z}_n \to \mathbb{Z}_n^\times$ given by $\phi \mapsto \phi(1)$ is an isomorphism.

To do (c) let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $\operatorname{Aut} G$ is isomorphic to S_3 because any permutation of (1,0), (0,1) and (1,1) defines an automorphism of G.

2. Use the same notations as in Problem 1. Let π_g be the map of G to itself defined by $\pi_g(x) = gxg^{-1}$, here $g \in G$.

(a) Show that $\pi_g \in \operatorname{Aut} G$.

(b) Let $\operatorname{Inn} G = \{\pi_g \mid g \in G\}$. Show that $\operatorname{Inn} G$ is a normal subgroup in $\operatorname{Aut} G$.

Solution.

$$(a)\, \pi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \pi_g(x)\pi_g(y).$$

(b) First check that Inn G is a subgroup

$$\pi_g \circ \pi_h(x) = g\left(hxh^{-1}\right)g^{-1} = (gh)\,x\,(gh)^{-1} = \pi_{gh}(x).$$

To check that Inn G is normal let $\phi \in \operatorname{Aut} G$, then

$$\phi \circ \pi_g \circ \phi^{-1}(x) = \phi\left(g\phi^{-1}(x)\,g^{-1}\right) = \phi(g)\,\phi\left(\phi^{-1}(x)\right)\phi\left(g^{-1}\right) = \phi(g)\,x\phi\left(g^{-1}\right).$$

Thus, $\phi \circ \pi_g \circ \phi^{-1} = \pi_{\phi(g)}$.

4. One makes necklaces from black and white beads. Let p be a prime number. Two necklaces are the same if one can be obtained from another by a rotation or a flip over. How many different necklaces of p beads one can make?

Solution. The group acting on the necklaces is D_p. We have to find the number of orbits. Possible subgroups of D_p are groups generated by one flip or the cyclic subgroup of rotations, as follows from the fact that $|D_p| = 2p$ and the Lagrange theorem.

If all rotations preserve a necklace, then its beads are all of the same color. In this case the stabilizer is the whole D_p, and we have exactly two such orbits.

Let a stabilizer of a necklace is a flip. Then the necklace is symmetric. We can choose color of $\frac{p+1}{2}$ beads, the other can be obtained by the symmetry. Thus, we have exactly $2^{\frac{p+1}{2}} - 2$ orbits. (We subtract 2 because necklaces with all beads of the same color are already counted). Each orbit has p necklaces in it. All other necklaces do not have any symmetry. To count their number we must subtract the number of necklaces which we already counted from 2^p. That gives

$$2^p - p\left(2^{\frac{p+1}{2}} - 2\right) - 2.$$

Every orbit with a trivial stabilizer has $2p$ elements. The number of such orbits is

$$\frac{2^p - p\left(2^{\frac{p+1}{2}} - 2\right) - 2}{2p} = \frac{2^{p-1} - 1}{p} - 2^{\frac{p-1}{2}} + 1.$$

The total number of orbits is

$$\frac{2^{p-1} - 1}{p} - 2^{\frac{p-1}{2}} + 1 + 2^{\frac{p+1}{2}} = \frac{2^{p-1} - 1}{p} + 2^{\frac{p-1}{2}} + 1.$$

5. Assume that N is a normal subgroup of a group G. Prove that if N and G/N are solvable, then G is solvable.

Solution. Let $K = G/N$. Consider the series

$$N \supset N_1 \supset \cdots \supset \{1\}, \; K \supset K_1 \supset \cdots \supset \{1\},$$

such that K_i/K_{i+1} and N_j/N_{j+1} are abelian. Let $p \colon G \to K$ denote the natural projection. Then for the series

$$G \supset p^{-1}(K_1) \supset \cdots \supset N \supset N_1 \supset \cdots \supset \{1\}$$

$$p^{-1}(K_i)/p^{-1}(K_{i+1}) \cong K_i/K_{i+1}$$

by the second isomorphism theorem. Thus, G is solvable.

6. For any permutation s denote by $F(s)$ the number of fixed points of s (k is a fixed point if $s(k) = k$). Let N be a normal subgroup of A_n. Choose a non-identical permutation $s \in N$ with maximal possible $F(s)$.

(a) Prove that any disjoint cycle of s has length not greater than 3. (Hint: if $s \in N$, then $gsg^{-1} \in N$ for any even permutation g).

(b) Prove that the number of disjoint cycles in s is not greater than 2.

(c) Assume that $n \geq 5$. Prove that s is a 3-cycle.

(d) Use (c) to show that A_n is *simple* for $n \geq 5$, i.e. A_n does not have proper non-trivial normal subgroups. (Hint: A_n is generated by 3-cycles, as it was proven in class).

Solution. Let $s = c_1 \dots c_k$ and c_1 be one of the longest cycles. Assume that the length of c_1 is greater than 3. Let

$$c_1 = (x_1, x_2, \dots, x_l), \; u = (x_1, x_2, x_3).$$

Then

$$sus^{-1}u^{-1} = (x_1, x_4, x_2) \in N.$$

But $F(sus^{-1}u^{-1}) = 3 < F(s)$. Contradiction. That proves (a).

Assume now that $k \geq 3$. Since all cycles of s have the length 2 or 3. One can find two cycles of the same length. Say

$$c_1 = (a, b, c), \; c_2 = (d, e, f).$$

Let $u = (b, c)(e, f)$. Then

$$s^{-1}usu^{-1} = c_1c_2 \in N.$$

Again $F(s^{-1}usu^{-1}) < F(s)$. Contradiction. If we assume that

$$c_1 = (a, b), \; c_2 = (c, d),$$

put $u = (a, b, c)$. Then

$$s^{-1}usu^{-1} = (a, c)(b, d) \in N.$$

We obtain $F(s^{-1}usu^{-1}) < F(s)$. Contradiction. Hence (b) is proven.

Now let $n \geq 5$. Assume that s is not a 3-cycle. Then

$$s = c_1c_2,$$

where c_1 and c_2 are either both transpositions or both 3-cycles. First, assume that c_1 and c_2 are both transpositions. In this case

$$c_1 = (a, b), \; c_2 = (c, d).$$

Since $n \geq 5$, there is $e \neq a, b, c, d$. Let $u = (a, b, e)$. Then

$$s^{-1}usu^{-1} = (b, e, a),$$

again $F(s^{-1}usu^{-1}) = 3 < 4 = F(s)$. Finally, let

$$c_1 = (a, b, c)(d, e, f).$$

Play the same game with $u = (b, c, e)$. Get

$$sus^{-1}u^{-1} = (a, f, c, b, e).$$

Obtain contradiction again.

If N contains one 3-cycle, then N must contain all 3-cycles, because all 3-cycles are conjugate in A_n for $n \geq 5$. Therefore $N = A_n$. Done.

Problem set 3

2. If p is prime and p divides $|G|$, then G has an element of order p.

Solution. By Sylow theorem G has a subgroup P of order p^n. Let $g \in P$. Then the order of g is p^k, and the order of $g^{p^{k-1}}$ is p.

3. Let p and q be prime and $q \not\equiv 1 \mod p$. If $|G| = p^n q$, then G is solvable.

Solution. By the second Sylow theorem there is only one Sylow p-subgroup. Denote it by P. Then P is normal since $gPg^{-1} = P$ for any $g \in G$. As we proved in class P is solvable, the quotient G/P is solvable. Hence G is solvable by Problem 5 homework 2.

4. Suppose that $|G| < 60$ and $|G| = 2^m 3^n$. Check that G is solvable. Hint: prove by induction on $|G|$. First, show that the number of Sylow 2-subgroups is 3 or the number of Sylow 3-subgroups is 4. Then construct a homomorphism $f : G \to S_3$ or S_4. By induction the kernel and the image of f are solvable. Hence G is solvable.

Solution. First, assume that $m \leq 3$. The number of Sylow 3-subgroups is 1 or 4 by the second Sylow theorem. If it is 1, proceed as in Problem 3. If it is 4, then G acts on the 4-element set of Sylow 3-subgroups by conjugation. Thus, we have a non-trivial homomorphism $f : G \to S_4$. $\operatorname{Im} f$ is solvable as a subgroup of a solvable group, $\operatorname{Ker} f$ is solvable by induction assumption. Hence G is solvable.

Now let $m \geq 4$. Recall that $|G| < 60$. The case $n = 0$ is known. Therefore $m = 4, n = 1$, $|G| = 48$. The number of Sylow 2-subgroups is 1 or 3. If it is 1 we can proceed as in Problem 3. If it is 3, then G acts on the 3-element set of Sylow 2-subgroups, there is a non-trivial homomorphism $f : G \to S_3$ and we can finish the argument as in the previous paragraph.

5. Show that any group of order less than 60 is solvable. Hint: use the previous problems to eliminate most of numbers below 60.

Solution. Let p be the maximal prime factor of $|G|$. First, assume that $p > 7$. Then $|G| = pk$, with $k < p$. Then the number of Sylow p-subgroups of G is 1, and we can go to the quotient and proceed by induction on $|G|$.

Let $p = 7$. As above we have to check only the case when the number of 7-subgroups is more than 1. Due to the second Sylow Theorem that is is possible only for $|G| = 56$. However, in this case the number of 7-subgroups should be 8. That gives 48 elements of order 7. Thus, we can have only one 8-subgroup, since only 8 elements remains after excluding of all elements of order 7. Hence there is a normal 8-subgroup, and G is solvable.

Let $p = 5$. As above we have to check the cases when there is a possibility for more than one Sylow 5-subgroups. That leaves the case $|G| = 30$. Assume that there is six Sylow 5-subgroups, that gives 24 elements of order 5. The remaining set of elements can not contain four or more 3-subgroups. Thus, there is a normal 3-subgroup and again we can prove that G is solvable by induction argument.

The case $p = 3$ is done in Problem 4.

6. Let H be a p-subgroup of G, in other words $|H|$ is a power of a prime p. Prove that there is a Sylow p-subgroup P containing H. Hint: consider the action of H on the set of all Sylow p-subgroups. Check that there is a 1-element H-orbit $\{P\}$. Prove that H is a subgroup of P.

Solution. Let Ω be the set of all Sylow p-subgroups. Any H-orbit has p^k elements for some k. In particular, if an orbit has more than 1 element, then p divides the order of the orbit. Since $|\Omega| \equiv 1 \mod p$, there is at least one orbit $\{P\}$ of order 1. Then $H \subset N(P)$. Then HP is a subgroup of G and by the third isomorphism theorem

$$HP/P \cong H/(H \cap P).$$

Then $|HP| = |P||H/(H \cap P)|$. Therefore $|HP|$ is a power of p. But P is a maximal p-subgroup of G. Hence $HP = P$, $H \cap P = H$, the latter implies $H \subset P$.

Problem set 4

1. Let F be a field, and $F[i]$ denote the set of all expressions $a+bi$, with $a,b \in F$. Define addition and multiplication in $F[i]$ by

$$(a+bi)+(c+di)=(a+c)+(b+d)\,i,$$

$$(a+bi)(c+di)=ac-bd+(ad+bc)\,i.$$

Determine if $F[i]$ is a field for $F=\mathbb{Q},\mathbb{R},\mathbb{Z}_3,\mathbb{Z}_5$.

Solution. All axioms of a field are obvious except the existence of a multiplicative inverse. We are going to use the formula

$$(a+bi)=\frac{a-bi}{a^2+b^2}.$$

If $a^2+b^2=0$ implies $a=b=0$, then $F[i]$ is a filed. For $F=\mathbb{Q}$ or $\mathbb{R}$ the statement is obvious as $a^2+b^2>0$ whenever a or b is not zero. If $F=\mathbb{Z}_3$

$$a^2+b^2=0$$

implies $a=b=0$ as one can check directly by substituting $a=1,2, b=1,2$. But in $\mathbb{Z}_5$ there is a solution $a=1,b=2$. Indeed, in this case

$$(1+2i)(1-2i)=0,$$

therefore $\mathbb{Z}_5[i]$ is not a field.

2. Assume that $\operatorname{char} F=p$. Prove that $(a+b)^p=a^p+b^p$. Hint: use binomial formula.

Solution.

$$(a+b)^p=a^p+\tbinom{p}{1}a^{p-1}b+\tbinom{p}{2}a^{p-2}b^2+\cdots+\tbinom{p}{p-1}ab^{p-1}+b^p.$$

But

$$\tbinom{p}{k}\equiv 0 \mod p,$$

if $k=1,\dots,p-1$. Therefore $(a+b)^p=a^p+b^p$.

3. Prove the little Fermat's theorem

$$a^p\equiv a \mod p$$

for any prime p and integer a. Hint: use the previous problem.

Solution. Start from $a=1$ and use $(a+1)^p=a^p+1=a+1$.

4. Let V be a vector space of dimension n and $A:V\to V$ be a linear map such that $A^N=0$ for some integer $N>0$. Prove that $A^n=0$. Hint: check that $\operatorname{Im}A^k$ is a proper subspace in $\operatorname{Im}A^{k-1}$.

Solution. Note that $\operatorname{Im}A^k\subset\operatorname{Im}A^{k-1}$ for all k. If $\operatorname{Im}A^k\neq\operatorname{Im}A^{k-1}$, then $\dim\operatorname{Im}A^k\le\dim\operatorname{Im}A^{k-1}-1$. Therefore, one can find $k\le n+1$ such that $\operatorname{Im}A^k=\operatorname{Im}A^{k-1}$.

Choose the minimal k such that $\operatorname{Im}A^k=\operatorname{Im}A^{k-1}$. Then

$$A:\operatorname{Im}A^{k-1}\to\operatorname{Im}A^{k-1}$$

is surjective and therefore A is non-degenerate when restricted to the subspace $\operatorname{Im} A^{k-1}$. But then

$$A^l\left(\operatorname{Im} A^{k-1}\right) = \operatorname{Im} A^{k-1}$$

for any $l > 0$. Take $l = N - k + 1$. Then

$$A^l\left(\operatorname{Im} A^{k-1}\right) = \operatorname{Im} A^{k-1} = \operatorname{Im} A^N = 0,$$

hence $A^{k-1} = 0$.

5. Find a formula for a general term of the Fibonacci sequence
1,1,2,3,5,8,13,. . .
Hint: write the Fibonacci sequence as a linear combination of

$$1, \alpha, \alpha^2, \alpha^3, \dots \text{ and } 1, \beta, \beta^2, \beta^3, \dots,$$

where

$$\alpha = \frac{1+\sqrt{5}}{2}, \ \beta = \frac{1-\sqrt{5}}{2}.$$

Solution. Let

$$f = 1, 1, 2, 3, 5, 8, 13, \dots, \ u = 1, \alpha, \alpha^2, \alpha^3, \dots, v = 1, \beta, \beta^2, \beta^3, \dots,$$

and $f = xu + yv$. Then

$$x + y = 1 \text{ and } x\alpha + y\beta = 1.$$

Solve these two equations

$$x = \frac{1-\beta}{\alpha-\beta}, y = \frac{\alpha-1}{\alpha-\beta}.$$

Use $\alpha + \beta = 1$, $\alpha - \beta = \sqrt{5}$. So

$$x = \frac{\alpha}{\sqrt{5}}, \ y = \frac{-\beta}{\sqrt{5}}.$$

Therefore

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

6. Let $F = \mathbb{Z}_p$.
(a) Prove that the number of one dimensional subspaces in F^n equals $\frac{p^n-1}{p-1}$;
(b) (Extra credit) Find the number of 2-dimensional subspaces in F^n.

Solution. A one-dimensional subspace is determined by a non-zero vector in F^n. Two non-zero vectors define the same subspace if and only if they are proportional. There are $p^n - 1$ non-zero vectors, each vector is proportional to $p - 1$ vectors. Hence the formula.

Now we proceed similarly for two-dimensional subspaces. A pair of linearly independent vectors v, w defines a two dimensional subspace, as the subspace generated by v and w. The number of linearly independent pairs is $(p^n - 1)(p^n - p)$. To find the number of two-dimensional subspaces we have to divide the number of linearly independent pairs on the number of bases in a two-dimensional subspace (F^2). Hence the answer is

$$\frac{(p^n - 1)(p^n - p)}{(p^2 - 1)(p^2 - p)}.$$