HOMEWORK 6, DUE THU MAR 11TH

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let G be a finite abelian group of order n and let $G = \{g_1, g_2, \ldots, g_n\}$. Let $g = \prod_{i=1}^{n} g_i$.

(a) Show that $g^2 = e$.

Solution. We first partition G into two sets, $G_1 = \{x \in G | x^2 = e\}$ and $G_2 = \{x \in G | x^2 \neq e\}$. So, we can write $g = hk$ where $h = \prod_{x \in G_1} x, k = \prod_{x \in G_2} x$. Next, we notice that $h^2 = e$. Notice also that if $x \in G_2$, then $x^{-1} \in G_2$ and $x \neq x^{-1}$. Thus we can pair every element in G_2 with its inverse and thus we get $k = e$. So, $g = h$ and $g^2 = h^2 = e$. □

(b) If $o(G)$ is either odd or G has more than one element of order two, show that $g = e$.

Solution. If $o(G)$ is odd, $G_1 = \{e\}$ and thus $h = e$. Now assume that G has more than one element of order 2. The G_1 above is a subgroup of G with all non-trivial elements of order 2 and contains all such elements of G. Thus, the assumption implies $o(G_1) > 2$ and so $o(G_1) = 2^m$ with $m > 1$. Proof is by induction on m. If $m = 2$, then $G_1 = \{e, a, b, ab\}$ and so the product h is just e. Now, let $m > 2$ and take $H \subset G_1$, a subgroup of index 2 (why does it exist?). Then $G_1 = H \cup aH$, the two cosets. Since $o(H) = 2^{m-1}$ and $m - 1 > 1$, by induction, the product of elements of H is just e. The product of elements in aH is just $a^{o(H)}$ multiplied by the product of elements of H and since $o(H)$ is even, this too is identity. □

(c) If G has exactly one element of order 2, say x, show that $g = x$.

Solution. In this case, $G_1 = \{e, x\}$ and then the product is just x. □

(2) Let p be a prime number.

(a) Show that for any $x \in \mathbb{Z}$, $x^p \equiv x \bmod p$. (Fermat's little theorem)

Solution. We use the fact that the non-zero elements of $\mathbb{F}_p$ is a group of order $p-1$. Thus, $x^{p-1} \equiv 1 \bmod p$ for any integer x with p not dividing it. So, we get for these $x^p \equiv x \bmod p$. If p divides x, then both x^p and x are zero modulo p and so, cearly $x^p \equiv x \bmod p$. $\square$

(b) Show that $(p-1)! \equiv -1 \bmod p$. (Wilson's theorem)

Solution. Here, we use the fact that the non-zero elements of $\mathbb{F}_p$ is in fact a cyclic group. If $p = 2$, the result is trivial and so assume p is odd. Then, this cyclic group has order $p-1$ an even number and has exactly one element (class of -1) of order 2. Thus, the product of elements in this group, which is just $(p-1)!$ must be -1 modulo p by problem (1)(c). $\square$

(c) Assume p is odd. Write

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

with $a, b \in \mathbb{Z}$. Show that $p|a$.

Solution. Again, we look at $\mathbb{F}_p^*$, the non-zero elements of $\mathbb{F}_p$. We have the natural map $\alpha : \mathbb{F}_p^* \to \mathbb{F}_p^*$, given by $\alpha(i)$, the inverse of i where $1 \le i < p$ and so are the $\alpha(i)$. This just means, $\alpha(i) \equiv 1 \bmod p$, so we write $\alpha(i)i = x_i$ with $x_i \equiv 1 \bmod p$. Thus, $\frac{1}{i} = \frac{\alpha(i)}{x_i}$. Let $x = \prod x_i$ and then our sum is just $\frac{\sum \frac{x\alpha(i)}{x_i}}{x}$. Since p does not divide x, suffices to show that the numerator is a multiple of p. But, modulo p, each of x/x_i is 1 and thus modulo p, the numerator is just $\sum \alpha(i) = \sum i = p(p-1)/2 = 0$. $\square$

(3) Find all automorphisms of S_3.

Solution. We always have the group homomorphism $S_3 \to \mathrm{Aut}(S_3)$, given by conjugation and whose kernel is the center, which in this case is just $\{e\}$ and so this map is one-to-one. Now, let $T \in \mathrm{Aut}(S_3)$. Let $a \in S_3$ be a two cycle. Then $T(a)$

can be written as product of disjoint cycles. If this contains a 3-cycle, then there are no more disjoint cycles, but since $2 = o(a) = o(T(a)) = 3$, we have a contradiction. So, this product can not contain 3-cycles and all those appearing must be 2 or 1 cycle. If it had only 1-cycles, this is just the identity again contradicting $o(a) = 2$. Thus it must have at least one 2-cycle and then it is just a two cycle. Thus, T induces a map from the set of 2-cycles to itself. There are three 2-cycles and this induced map is a bijection. So, we get a group homomorphism $\mathrm{Aut}(S_3) \to S_3$, where the latter S_3 is the set of all bijections from the set of 2-cycles to itself. I claim that this map too is one-to-one. If not, it has a kernel and let T be in the kernel. Then, $T(a) = a$ for all two cycles. Since $(123) = (13)(12)$, we see that $T(123) = T(13)T(12) = (13)(12) = (123)$, we see that T also acts as identity on a 3-cycle. Since every element in S_3 can be written as product of such cycles, we see that T must be identity. So, $o(S_3) \leq o(\mathrm{Aut}(S_3)) \leq o(S_3)$ and thus these are all the same. Thus the natural conjugation map $S_3 \to \mathrm{Aut}(S_3)$ is an isomorphism.

□

(4) This is a long problem, but most cases are easy. Show that any group of order at most 30 is either of prime order or has a non-trivial normal subgroup, by analyzing each order. (In fact, you should be able to do this for groups of order less than 60. We have seen A_5, whose order is 60, is simple.)

Solution. Since every group with prime power order has a non-trivial center, it is easy to see that they have a non-trivial normal subgroup, unless it is of prime order. We have also dealt with groups of order pq, p^2q where p, q are distinct primes in last homework.

So, the first number which does not fall into these categories is 24. So, let G be one such. If the 3-Sylow subgroup is not normal, there are $1 + 3k > 1$ of them and this should divide 8. Only such is 4. If S is the set of these, one has a natural map $G \to A(S)$, given by conjugation action and this map is not trivial. So, the kernel is a normal subgroup and we are done if it is non-trivial. If it is trivial, both G and $A(S) = S_4$ have 24 elements and thus $G \cong S_4$. Then, A_4 is a proper normal subgroup.

Next number not falling into the above group of numbers is 30. By Sylow theorem, one sees that the 3-Sylow subgroup must be normal or there are ten of them. So, there are 20 elements of order 3. If the 5-Sylow subgroup is also not normal, there must be six of them and then there are 24 elements of order 5 which means the group has more than $20 + 24 + 1$ elements, which is absurd.

$\square$

(5) Let $G = SL(2, \mathbb{F}_p)$, and Z be the center of $SL(2, \mathbb{F}_p)$. Let $P = PGL(2, \mathbb{F}_p) = SL(2, \mathbb{F}_p)/Z$, the projective linear group. Calculate $o(G)$ and $o(P)$.

Solution. We have seen in an earlier home work that

$$o(GL(2, \mathbb{F}_p)) = (p^2 - 1)(p^2 - p)$$

$SL(2, \mathbb{F}_p)$ is the kernel of the surjective homomorphism $\det : GL(2, \mathbb{F}_p) \to \mathbb{F}_p^*$ and thus its order is $\frac{(p^2-1)(p^2-p)}{p-1} = p(p^2 - 1)$. The center consists of scalar matrices aI, with $a \in \mathbb{F}_p^*$ (do you know why?) . Since $aI \in SL(2, \mathbb{F}_p)$, we must have $a^2 = 1$. So, if $p = 2$, we only have identity in the kernel and if p is odd, $o(Z) = 2$. Thus, if $p = 2$, $GL(2, \mathbb{F}_p) = SL(2, \mathbb{F}_p) = P$ and its order is 6. If p is odd, we see that $o(P) = \frac{p(p^2-1)}{2}$. $\square$

(6) Let notation be as in the previous problem and assume that $p = 5$. Further assume that in this case, we know P is simple. We will as usual denote elements of $\mathbb{F}_p$ as $\{0, 1, 2, 3, 4\}$.
   (a) Let

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, B = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}.$$

   Show that $\det A = \det B = 1$ and then we identify these with their images in P.

   Solution. This is just an easy calculation by the usual formula for determinant. $\square$

   (b) Show that A, B generate a 2-Sylow subgroup H of P and $EHE^{-1} \neq H$, where ,

$$E = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

So H is not normal.

Solution. One easily checks that $o(A) = o(B) = 2$ (in P) and $AB = BA$, so that the group generated by A, B is just $\{Id, A, B, AB\}$. So, it is a 2-Sylow subgroup.
One easily checks $EAE^{-1} \notin H$.

$\square$

(c) Let $C = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$. Show that $\det C = 1$ and $o(C) = 3$. Show that $C \in N(H)$, the normalizer of H. Deduce that $o(N(H)) = 12$.

Solution. The first part is just a checking. For the last part, notice that $N(H)$ contains H and C. So its order is a multiple of 4 and 3 and thus a multiple of 12. So, $o(N(H)) = 12$ or 60. If it is 60, then H would be normal, which we have seen is not the case.

$\square$

(d) Prove that $P \cong A_5$.

Solution. Since the number of conjugates of H is the index of $N(H)$ in P, it is 5. So, let S be the set of 2-Sylow subgroups. We have a homomorphism $P \to A(S) = S_5$ as usual, conjugating the Sylow subgroups. This map is not trivial, since all 2-Sylow subgroups are conjugate and since we are assuming P is simple, this map must be injective. Thus the image is a subgroup K of S_5 of index 2 and thus normal. If $K \neq A_5$, then $K \cap A_5$ would be an index 2 normal subgroup of A_5, but A_5 is simple. So, $K = A_5$. $\square$