HOMEWORK 4, DUE THU FEB 25TH

All solutions should be with proofs, you may quote from the book

(1) Let G be a finite abelian group.
   (a) Let H, K be subgroups of G with $\gcd(o(H), o(K)) = 1$. Show that the natural map $f : H \times K \to G$, $f(a, b) = ab$ is a one-to-one group homomorphism.

   Solution. Since G is abelian, this is a group homomorphism is clear (and we have checked it earlier). To show that it is one-to-one, we calculate its kernel. If $f(a, b) = e$, we get $ab = e$ and so $a = b^{-1}$. Thus, $a \in H \cap K$ and so $o(a)$ should divide bot $o(H), o(K)$. But these are relatively prime and thus $o(a) = 1$ and so $a = e$ and then $b = e$. □

   (b) Show that G is isomorphic to $H_1 \times H_2 \times \cdots \times H_n$ with all H_i cyclic and $o(H_{i+1})$ dividing $o(H_i)$ for all i.

   Solution. The proof is very similar to what we did in class. Proof is by induction on $o(G)$. If $o(G) = 1$, this is trivial. So assume proved for smaller orders and pick $a \in G$ of maximal order, say n. Let $H = \langle a \rangle$, the cyclic subgroup generated by a. Then, $G/H = K_1 \times \cdots K_m$ where K_i are cyclic, $o(K_i) = r_i$ and $r_{i+1} | r_i$, by induction, since $o(G/H) < o(G)$. Main observation is for any element $x \in G$, $o(x)$ divides n, because if not, $\mathrm{lcm}(o(x), n) > n$ and we have an element of order $\mathrm{lcm}(o(x), n)$ in G, contrary to our choice.
   Now as we did in class, we lift a generator b_i of K_i to $a_i \in G$ such that $o(a_i) = b_i$. We do this for any element $b \in G/H$. So, let $x \in G$ be any lift. That is, under the natural group homomorphism $\pi : G \to G/H$, $\pi(x) = b$. Let $o(b) = r$. Since $a^n = e$, we have $\pi(a)^n = b^n = e$ and thus r divides n. Since $\pi(x)^r = b^r = e$, we see that $x^r \in H$ and so we can write $x^r = a^k$ for some k. Then, $e = (x^r)^{n/r} = a^{kn/r}$. Thus, n divides nk/r and so r divides k. Thus $k = lr$ and then, take $A = xa^{-l}$. Then $\pi(A) = b$

and $A^r = x^r a^{-lr} = e$. Easy to see that $o(A) = r$. We can do this for all the b_is above.
Then, $\pi(a_i) = b_i$ and $o(a_i) = r_i$. Letting $H_i = \langle a_i \rangle$, we get a map $H \times H_1 \times H - 2 \times \cdots H_m \to G$ as usual and easy to check that this is a group isomorphism. □

(2) We write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$ for a prime p, since we wish to use the fact that it has addition, multiplication and inverses for all non-zero elements, called a *field*.
   (a) Let $G = GL(n, \mathbb{F}_p)$. Then, we can let G act on $\mathbb{F}_p^n = \mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ (n times) as usual (recall from Math 429 how this works). If A is any $n \times n$ matrix with entries from $\mathbb{F}_p$ and $\underline{a} \in \mathbb{F}_p^n$ (written as column vectors) then $A\underline{a} \in \mathbb{F}_p^n$ makes sense. Show that such an A is in G if and only if the columns (or rows) are linearly independent. That is, if $A = [\underline{a}_1, \underline{a}_2, \cdots, \underline{a}_n]$ and $c_1\underline{a}_1 + c_2\underline{a}_2 + \cdots + c_n\underline{a}_n = \underline{0}$, with $c_i \in \mathbb{F}_p$, then $c_i = 0$ for all i.

   Solution. Proofs are identical to what you did in linear algebra. So, firs $A \in G$, written as above. If $c_1\underline{a}_1 + c_2\underline{a}_2 + \cdots + c_n\underline{a}_n$ is the zero vector, then $A\underline{c}$ is the zero vector, where $\underline{c}$ is the column vector

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}.$$

   Multiplying by A^{-1}, we get that this vector is zero.
   Conversely, assume that $\underline{a}_i$ are linearly independent. Then, the map $A : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is onto, since these form a basis and thus A is one-to-one and onto and one can then write down an inverse. So, $A \in G$. □

   (b) Calculate the order of G for a prime p.

   Solution. If A written as above using columns, for being in G, we need them to be linearly independent. So, $\underline{a}_1 \neq 0$, thus it has $p^n - 1$ choices, the only vector to be avoided is the zero vector. What are the choices for $\underline{a}_2$ once we fix $\underline{a}_1$? The only ones to be avoided are multiples of $\underline{a}_1$ and thus it has $p^n - p$ choices. Continuing in this fashion, we

get the order of G to be.

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

□

(3) These are some problems on automorphisms.

(a) Let G be a finite group and $\phi \in \mathrm{Aut}(G)$. Assume that if $\phi(g) = g$ for $g \in G$ then $g = e$. Show that every element in $g \in G$ is of the form $g = x^{-1}\phi(x)$ for some $x \in G$. Deduce that, if in addition $\phi^2 = \mathrm{Id}$, then G is abelian.

Solution. Consider the (set) map $f : G \to G$, $f(x) = x^{-1}\phi(x)$. I claim this is one-to-one. So, as usual, we solve $f(x) = f(y)$ and that is $x^{-1}\phi(x) = y^{-1}\phi(y)$. This says, $yx^{-1} = \phi(y)\phi(x)^{-1} = \phi(yx^{-1})$. So, our hypothesis says $yx^{-1} = e$ or $x = y$, proving what we need. Since G is a finite set, any one-to-one map from G to itself must be onto and this proves the claim.
For the latter part, assume that ϕ^2 is identity. Then for any $g \in G$, write $g = x^{-1}\phi(x)$ and then, $\phi(g) = \phi(x^{-1}\phi(x)) = \phi(x)^{-1}\phi^2(x) = \phi(x)^{-1}x = g^{-1}$. (Rest we have done earlier, but let me do it again.) Since ϕ is a group homomorphism, for any $g, h \in G$, we have $\phi(gh) = \phi(g)\phi(h)$ and thus $(gh)^{-1} = g^{-1}h^{-1}$. So, $h^{-1}g^{-1} = g^1h^{-1}$, thus any two elements commute. □

(b) Show that a finite group with order greater than two has a non-trivial (not equal to identity) automorphism.

Solution. If $gx \neq xg$ for two elements $g, x \in G$, then the inner conjugation automorphism $\phi_g : G \to G$, $\phi_g(x) = gxg^{-1}$ is not the identity. So, we may assume that G is abelian. Now write G as a product of cyclic groups. If one of them has order greater than 2, say H, write $G = H \times K$, where K is the product of the remaining collection. Let $o(H) = n > 2$ and then $\phi(n) > 1$, so we have an automorphism different from identity, say f of H. Define $\phi : G = H \times K \to G$, by $\phi(a, b) = (f(a), b)$. I will leave you to check that this is indeed an automorphism of the desired kind.
Finally we are left with the case every one of the cyclic group appearing in our decomposition has order 2. Then,

$G = H_1 \times H_2 \times \cdots \times H_n$ with $o(H_i) = 2$ and then $n > 1$, since $o(G) > 2$. Now, consider $f : G \to G$, $f(a_1, a_2, \ldots, a_n) = (a_2, a_1, \ldots, a_n)$. I will let you check that is an automorphism of the desired kind. □

(c) Let $\phi(n)$ be the Euler function (the number of integers k, $1 \leq k < n$ with $\gcd(k, n) = 1$). For any integer $a > 1$, show that n divides $\phi(a^n - 1)$. (Hint: For any $m > 1$, $\phi(m)$ is the order of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$.)

Solution. Take $N = a^n - 1$ and $G = \mathbb{Z}/N\mathbb{Z}$. Then, $\gcd(a, N) = 1$ and thus $[a] \in \mathrm{Aut}(G)$ (which from class, are all the elements of G which are relatively prime to N, under multiplication). Clearly, $[a]^n = [a^n] = [1]$. Easy to see that $[a]^k \neq [1]$ for any positive integer $k < n$ and thus $o([a]) = n$ and then by Lagrange, n divides $\phi(N)$. □

(4) These are some problems on semi-direct products.

(a) Construct a non-abelian group of order 55 and one of order 203.

Solution. Start with $G = \mathbb{Z}/11\mathbb{Z}$ and $H = \mathbb{Z}/5\mathbb{Z}$. Then $\mathrm{Aut}(G)$ is an abelian group of order 10 and thus has a cyclic subgroup of order 5. Thus, we have an inclusion $\phi : H \to \mathrm{Aut}(G)$ and so the semidirect product of G, H using ϕ gives one such example.
Again, $203 = 7 \times 29$. So, again we start with $G = \mathbb{Z}/29\mathbb{Z}$ and $H = \mathbb{Z}/7\mathbb{Z}$. One notes $\mathrm{Aut}(G)$ is an abelian group of order 28 and hence has an element of order 7 and the rest is identical. □

(b) Can you do the same for 35?

Solution. So, let G be a group of order 35. Since $35 = 5 \times 7$, any element of G must have order $1, 5, 7$ or 35. If it had an element of order 35, then it is cyclic and thus abelian. So, let us assume we have none of order 35. Can it have all non-identity elements of order 7? If so, let $H_1, \ldots, H_n$ be all the order 7 subgroups. Then $H_i \cap H_j = \{e\}$ and since we are assuming, $\cup H_i = G$, we see that $35 = o(G) = 6n + 1$, which is absurd. So, not all non-identity elements can have order 7. Can they all have order 5? Again, this will lead to an equation $35 = 4n + 1$,

which too is not possible. So, G must have t least an element of order 7 and another of order 5.
So, let $o(a) = 7, o(b) = 5$ and let $H = \langle a \rangle$. First assume that H is normal. Then, we get a homomorphism by conjugation, $\langle b \rangle \to \mathrm{Aut}(H)$. But $\mathrm{Aut}(H)$ is a group of order 6 and thus all such maps must be trivial. Thus, G is the direct product of H with $\langle b \rangle$ and in particular abelian.
Now, let H be non-normal. Then, $H_i = b^i H b^{-1}$ are all distinct for $0 \leq i < 5$ and they have only the identity in common. So, they cover exactly $5 \times 6 + 1 = 31$ elements. Then, it is clear that the remaining elements are precisely $b^i, 0 < i < 5$. Thus, these are the only elements of of order 5. So, we get $K = \langle b \rangle$ is normal. Again, the conjugation map $H \to \mathrm{Aut}(K)$ is trivial, since $o(H) = 7, o(\mathrm{Aut}(K) = 4$. So, again the group is abelian. So, all groups of order 35 are abelian (and then cyclic). □

(5) Show that $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group for any prime p.

Solution. We will use a result from previous homework (hw 3), which said that an abelian group with the property the number of solutions to $x^n = e$ is at most n for any n, is cyclic.

Remember that $G = \{[1], \ldots, [p-1]\}$ and we will drop the brackets for convenience and just write $1, 2$ etc. In this group the identity element is just 1. If $p(X)$ is a monic polynomial with integer coefficients in X then for any $a \in \mathbb{Z}/p\mathbb{Z}$, $p(a)$ makes sense and if $p(a) = 0$ for some $a \in \mathbb{Z}/p\mathbb{Z}$, then it is easy to see that $p(X) = (X - a)q(X)$ where $q(X)$ is a monic polynomial of degree $\deg p - 1$ in X. By an easy induction, one sees that $p(X)$ can have at most $\deg p(X)$ roots in $\mathbb{Z}/p\mathbb{Z}$ and this is true for $p(X) = X^n - 1$ and thus, the number of solutions to $x^n = 1 (= e)$ is at most n for any n. □