HOMEWORK 2, DUE WED FEB 10TH

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

(1) In the following problem, we are given a set and a suggested binary operation. Check whether it is indeed a binary operation and then check whether the set is a group with respect to this operation.

(a) Let $\mathbb{R}/\mathbb{Z}$ denote the set of equivalence classes of $\mathbb{R}$ with the relation $a \sim b$ if $a - b \in \mathbb{Z}$ (which you checked is indeed an equivalence relation in the first homework). Define an operation by $[a] + [b] = [a + b]$.

Solution. To check this operation is well defined, we must check that if $[a] = [a']$, $[b] = [b']$, then $[a + b] = [a' + b']$. The assumption gives, $a - a' = m, b - b' = n$ for integers m, n and thus $a + b = a' + b' + m + n$. Since $m + n \in \mathbb{Z}$, we see that $[a + b] = [a' + b']$.
Checking that this makes it into a group is straight forward. For example, associativity:

$$\begin{aligned}
[a] + ([b] + [c]) &= [a] + [b + c] \\
&= [a + (b + c)] \\
&= [(a + b) + c] \quad \text{associativity of addition for } \mathbb{R} \\
&= [a + b] + [c] \\
&= ([a] + b]) + [c]
\end{aligned}$$

Similarly, one checks $[0]$ is the identity element and $[-a]$ is the inverse of $[a]$. □

(b) Let U be the set of 2×2 matrices of the form $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$ for all $\theta \in \mathbb{R}$, with the operation being the usual matrix multiplication.

Solution. If $A(\theta)$ is the above matrix, one checks $A(\theta)A(\phi) = A(\theta + \phi)$ by using the addition formula from trigonometry. So, the operation is defined on this set.

Now, associativity is again clear, using $\theta + (\phi + \psi) = (\theta + \phi) + \psi$, in $\mathbb{R}$. Identity is $A(0)$ and inverse of $A(\theta)$ is $A(-\theta)$. □

(c) Let G, H be two groups and let the set be $G \times H$ and the binary operation is defined as $(g, h)(g', h') = (gg', hh')$.

Solution. This is easy. □

(2) Let G be a group such that for any $a, b \in G$, $(ab)^2 = a^2b^2$. Show that G is abelian.

Solution. One has $a^2b^2 = (ab)^2 = abab$. Multiplying on the left by a^{-1} and on the right by b^{-1}, we get,

$$\begin{aligned} a^{-1}(a^2b^2)b^{-1} &= a^{-1}(abab)b^{-1} \\ ab &= (a^{-1}a)ba(bb^{-1} \\ ab &= ba \end{aligned}$$

Since a, b were arbitrary, we see that G is abelian. □

(3) Let G be a group and let $\{H_\alpha\}$ be a collection (possibly infinite) of subgroups of G.

(a) Show that $\cap_\alpha H_\alpha$ is a subgroup of G.

Solution. We check the two conditions for subgroups. If we write $K = \cap_\alpha H_\alpha$, and $a, b \in K$, then $a, b \in H_\alpha$ for all α and since these are subgroups, $ab \in H_\alpha$ for all α and thus ab is in their intersection, K. The proof for a^{-1} is equally trivial. □

(b) Now, let the above collection be the set of *all* subgroups of G different from the trivial subgroup $\{e\}$. If $\cap_\alpha H_\alpha \neq \{e\}$, show that every element of G has finite order.

Solution. Assume that G has an element a of infinite order. Then, $H = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of G and $a^n \neq e$ if $n \neq 0$. Then, we have subgroups $H_p \subset H$, $H_p = \{a^{pm} | m \in \mathbb{Z}\}$ for any prime number p. Also, $H_p \neq \{e\}$ for any p, but $\cap_p H_p = \{e\}$, contradicting our hypothesis. □

(4) Let G be a group and H a subgroup.

(a) Show that for any $a \in G$, $aHa^{-1} = \{aha^{-1} | h \in H\}$ is a subgroup of G (called a *conjugate* of H).

Solution. As usual, we check the two conditions for a subgroup. If $aha^{-1}, ah'a^{-1} \in aHa^{-1}$, then their product is $(aha^{-1})(ah'a^{-1}) = ahh'a^{-1}$ and since $hh' \in H$, this belongs to aHa^{-1}. Similarly, the inverse of aha^{-1} is $ah^{-1}a^{-1}$, again in aHa^{-1}. □

(b) Let $N = \cap_{a \in G} aHa^{-1}$. Show that for any $x \in G$, $xNx^{-1} = N$.

Solution. As often the case, two show two sets are equal, we show the first is contained in the second and the second is contained in the first. In this case, if we show $xNx{-}1 \subset N$ for all $x \in G$, then, multiplying on the left with x^{-1} and the right by x, one gets $N \subset x^{-1}Nx$ and since x is arbitrary, we would have shown both the required inclusions.
So, to show one way inclusion, take xyx^{-1} with $y \in N$. Since $y \in aHa^{-1}$, we see that $xyx^{-1} \in xaH(xa)^{-1}$. As a is varied in G, xa varies over all of G and thus $xyx^{-1} \in \cap_{a \in G} aHa^{-1} = N$. □

(5) Let G be a group, H a subgroup of G of finite index.

(a) Show that the set $\{aHa^{-1} | a \in G\}$ is finite.

Solution. Since H is of finite index, it has only finitely many distinct right cosets, say $Ha_1, \ldots, Ha_n$. We have seen in class, then it has the same number of left cosets, say $b_1H, \ldots, b_n$. Then, $aHa^{-1} = b_iHa^{-1}$, since $aH = b_iH$ for some i. Again, $b_iHa^{-1} = b_iHa_j$, since $Ha^{-1} = Ha_j$ for some j. Thus, $aHa^{-1} = b_iHa_j$ and so there are at most n^2 of these. □

(b) Show that there is a subgroup $N \subset H$ of finite index such that $aNa^{-1} = N$ for all $a \in G$.

Solution. Again, easier to prove something more general. If $H, K \subset G$ are subgroups of finite index, so is $H \cap K$. We have $H \cap K \subset H \subset G$.

First, we show that $H \cap K \subset H$ is of finite index. It is easy to see that for any $h \in H$, $(H \cap K)h = H \cap Kh$. Since there are only finitely distinct Kh, one gets that there are only finitely many distinct $(H \cap K)h$ proving what we need.
So, let $(H \cap K)h_i$, $h_i \in H$ be these finitely many distinct cosets and let Ha_i be the finitely many cosets of H in$G$. Then, we have cosets $(H \cap K)h_i a_j$, finitely many cosets for $H \cap K$ in G and I claim these are all the cosets. So, it suffices to show that any $g \in G$ is in one of these. But $g \in Ha_j$ for some j and thus $g = ha_j$, $h \in H$. Then, $h \in (H \cap K)h_i$ for some i and thus $g \in (H \cap K)h_i a_j$.
Finally, we consider $N = \cap_{a \in G} aHa^{-1}$. Since there are only finitely many distinct aHa^1 from part a) this is a finite intersection. Since H is of finite index in G, it is clear, so are aHa^{-1} for any $a \in G$ and thus this is a finite intersection of subgroups of finite index and using the previous paragraph and easy induction, N is of finite index in G. This N satisfies $aNa^{-1} = N$ for any $a \in G$ is immediate. □

(6) Let G be an abelian group.
   (a) If $a, b \in G$ with $o(a) = m, o(b) = n$. Show that there exists a $c \in G$ with $o(c) = \mathrm{lcm}(m, n)$, the lowest common multiple of m, n.

Solution. Write $m = \prod_i p_i^{\alpha_i}, n = \prod p_i^{\beta_i}$ with $\alpha_i, \beta_i \geq 0$ and p_i distinct prime numbers. Let $M = \prod_{\alpha_i \geq \beta_i} p_i^{\alpha_i}, N = \prod_{\alpha_i < \beta_i} p_i^{\beta_i}$. Then M divides m, N divides n and $\gcd(M, N) = 1$ and $MN = \mathrm{lcm}(m, n)$. Then it is easy to check that $A = a^{m/M}$ has order M and $B = b^{n/N}$ has order N. We will use A, B to construct an element of order MN.
Take $c = AB$. Then, $c^{MN} = (AB)^{MN} = (A^M)^N (B^N)^M = e$. So, $o(c)$ divides MN. If $o(c) = d$, we get $c^d = A^d B^d = e$ or $A^d = B^{-d}$. Then, $e = (A^M)^d = (A^d)^M = (B^{-d})^M = B^{-dM}$. Since $o(B) = N$, we see that N divides dM and since $\gcd(M, N) = 1$, we see that N divides d So, $B^{-d} = e$ and thus $A^d = e$ which says M divides d. Since $\gcd(M, N) = 1$, this says MN divides d. □

(b) Assume G is finite. If the number of solutions in G to the equation $x^n = e$ is at most n for any positive integer n, show that G must be cyclic.

Solution. Since G is finite, we know that every element has order dividing the order of the group, so we can pick an $a \in G$ of maximal order, say n. Now, let $b \in G$ with order m. Then from the previous part, we have an element of order $\text{lcm}(m, n)$, but n was the maximal order, so $n \geq \text{lcm}(m, n)$. This implies $n = \text{lcm}(m, n)$ and thus m divides n.Then $b^n = e$. Since this is true for all $b \in G$, our hypothesis implies $o(G) \leq n$. Since G has an element a of order n, this says a generates G as a cyclic group. $\square$