# Math 504 HW2

Rohan Mukherjee

December 3, 2023

1. First we prove that $(a, b) = (a, b + ax)$ for all $x \in \mathbb{Z}$. Let $d_1 = (a, b)$. Then as $d_1 \mid a$ and $d_1 \mid b$, we have that $d_1 \mid b + ax$, so $d_1 \mid (a, b + ax)$. Now letting $d_2 = (a, b + ax)$, we also have $d_2 \mid b + ax - ax = b$, so $d_2 \mid (a, b) = d_1$, which shows that $d_2 = d_1$. Now we see that,

$$\binom{p^\alpha m}{p^\alpha} = \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha(m-1)+1)}{p^\alpha \cdot (p^\alpha - 1)\cdots 1}$$

From the previous part, we have that, for any $k$, $(p^\alpha m - k, p^\alpha) = (k, p^\alpha)$ (We also used that $-k$ has the same divisors as $k$). Now, since $(m, p) = 1$, $(m, p^\alpha) = 1$, so $(p^\alpha m - k, p^\alpha)$ is the highest power of $p$ dividing $p^\alpha m - k$ (most importantly, it can not be any higher than $p^\alpha$). Since the highest power of $p$ dividing $p^\alpha - k$ is exactly the same as the one dividing $p^\alpha m - k$, we cancel all the powers of $p$ on the top and bottom, and are left with none. Thus, $p$ does not divide $\binom{p^\alpha m}{p^\alpha}$.

2. Let $\langle p_1/q_1, \ldots, p_n/q_n \rangle \subset \mathbb{Q}$ be a nontrivial subgroup of $\mathbb{Q}$. By making a common denominator of $\prod q_i$, we get (we haven't done anything yet)

$$\left\langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} \right\rangle = \left\langle \frac{\prod_{i \neq 1} q_i p_1}{\prod q_i}, \ldots, \frac{\prod_{i \neq n} q_i p_n}{\prod q_i} \right\rangle$$

We have reduced our problem to the following: Show that $\langle p_1/q, \ldots, p_n/q \rangle = \langle (p_1, \ldots, p_n)/q \rangle$. First notice that $p_i/q = (p_i/(p_1, \ldots, p_n) \cdot (p_1, \ldots, p_n))/q$, so we have $\langle p_1/q, \ldots, p_n/q \rangle \leq \langle (p_1, \ldots, p_n)/q \rangle$. I claim that we can find $x_1, \ldots, x_n$ so that $(p_1, \ldots, p_n) = \sum_i p_i x_i$. This follows by induction: the base case is the definition of the gcd, so suppose its true for some $k \geq 3$. Now we prove the lemma that $(p_1, \ldots, p_{k+1}) = ((p_1, \ldots, p_k), p_{k+1})$. This follows since $(p_1, \ldots, p_{k+1}) \mid (p_1, \ldots, p_k)$ (since it is a common divisor of $p_1, \ldots, p_k$) so $(p_1, \ldots, p_{k+1}) \mid ((p_1, \ldots, p_k), p_{k+1})$. Similarly, $((p_1, \ldots, p_k), p_{k+1})$ divides all of $p_1, \ldots, p_{k+1}$, so it divides $(p_1, \ldots, p_{k+1})$. Now we can inductively find $x_1, \ldots, x_k$ so that $(p_1, \ldots, p_k) = \sum_{i=1}^k x_i p_i$. Now finding $y$ and $z$ so that $((p_1, \ldots, p_k), p_{k+1}) = y(p_1, \ldots, p_k) + z p_{k+1} = \sum_{i=1}^k y x_i p_i + z p_{k+1}$, completing the proof.

   Then,

$$\frac{(p_1, \ldots, p_n)}{q} = \sum_i \frac{p_i x_i}{q}$$

And thus $\langle (p_1, \ldots, p_n)/q \rangle \subset \langle p_1/q, \ldots, p_n/q \rangle$. Next notice that every nonzero element of $\mathbb{Q}$ has infinite order: for if $p, q \neq 0$, we would need an $n > 0$ so that $np/q = 0$, which is true iff $np = 0$ which can't happen. So, $\langle (p_1, \ldots, p_n)/q \rangle$ is a cyclic group of infinite order and hence isomorphic to $\mathbb{Z}$, which completes the proof.

3. We first prove that $H$ is in fact normal in $N_G(H)$–letting $n \in N_G(H)$, by definition we have that $nHn^{-1} = H$. Next, suppose that $H \trianglelefteq K \leq G$. By definition we have $kHk^{-1} = H$ for every $k \in K$. But this just says $K \leq N_G(H)$, so we are done.

4. We notice that the proof of Langrange's theorem works exactly the same if "left" was replaced with "right", and in particular the number of left cosets equals the number of right cosets, and in our case, both equal 2. Write $\{ H, gH \}$ to be the set of left cosets and $\{ H, Hg \}$ to be the set of right ($g$ is necessarily not in $H$). We claim that $gH \cap H = \emptyset$. If not, $gh = h_2$ for some $h_2$, so $g = h_2 h^{-1} \in H$ a contradiction. Since cosets partition the entire group and are all disjoint, we must have $Hg = G \setminus H = gH$, which completes the proof.

5. We show that if $\varphi : G \to H$ is a homomorphism, then $|\varphi(G)| \mid |G|$ and $|\varphi(G)| \mid |H|$. The latter is clear since $\varphi(G) \leq H$. The former is not as obvious. By the first isomorphism theorem, we have that $\varphi(G) \cong G/\ker(\varphi)$. In particular, they have the same order, so $|\varphi(G)| = |G|/|\ker(\varphi)|$. This is clearly a divisor of $|G|$ (it has a subset of $|G|$'s factors, not exceeding their power in $|G|$), so we have proven the second claim. Third, we claim that if $\varphi : G \to H$ and $N \leq G$, then we can restrict this to a homomorphism $\varphi_N : N \to H$. We can restrict these as *functions*, so now we just have to show that this preserves the homomorphism structure. Letting $n_1, n_2 \in N \leq G$, we have that $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$, which completes the third subclaim. Now, we have the natural projection $\pi : G \to G/N$. Restricting this to a homomorphism $\pi_H : H \to G/N$, we now have that $\pi_H(H) \mid |G/N|$ and $\pi_H(H) \mid |H|$. Since $(|G/N|, |H|) = 1$, we have that $|\pi_H(H)| = 1$, i.e. that $\pi_H(H) = gN$ for some $g \in G$. Since $e \in H$, $g = e$ ($N$ is the only coset with $e$), so we have proven that $\pi_H(H) = N$. In particular, this tells us that $hN = N$ for every $h \in H$, and that tells us that $H \subseteq N$. Our last claim is that if $H, N \leq G$ and $H \subset G$, then $H \leq N$. This follows immediately by the subgroup criterion, so we are done. □

P1. (a) We claim that the orbits are just $\{ 0 \}$, and $\mathbb{R}^n \setminus 0$. First notice that the orbit of $0 \in \mathbb{R}^n$ is just 0 (since $A \cdot 0 = 0$ for any matrix). In particular we shall show the orbit of $e_1$ is $\mathbb{R}^n \setminus 0$. Geometrically, for any $x \neq 0$ in $\mathbb{R}^n$, we can find a rotation matrix $R$ rotating $e_1$ to $x/\|x\|$. Then, we can use the diagonal matrix $\|x\| I_n$ to see that $\|x\| I_n (x/\|x\|) = x$, so our matrix sending $e_1$ to $x$ is just $(\|x\| I_n R)$. Since the orbits form a partition and are disjoint, we have classified all of them. The isotropy groups are just the stabilizers–i.e., $G_x = \{ A \in \mathrm{GL}_n(\mathbb{R}) \mid Ax = x \}$. One can see by definition this is just the set of invertible matrices with $x$ as an eigenvector with eigenvalue 1.

(b) Two matrices are in the same orbit if they have the same eigenvalues. Notice that, for a matrix $A \in \mathrm{Mat}_n(\mathbb{C})$, an $B \in \mathrm{GL}_n(\mathbb{C})$,

$$\begin{aligned}\det\Big(BAB^{-1} - \lambda I\Big) &= \det\Big(BAB^{-1} - B\lambda B^{-1}\Big) \\ &= \det\Big(B(AB^{-1} - \lambda B^{-1})\Big) = \det\Big(B(A - \lambda I)B^{-1}\Big) \\ &= \det(A - \lambda I)\det(B)\det\Big(B^{-1}\Big) = \det(A - \lambda I)\end{aligned}$$

So every conjugate of $A$ has precisely the same eigenvalues as $A$. Similarly, let $\{ v_1, \ldots, v_n \}$ be the collection of eigenvectors of $A$, with corresponding eigenvectors $\{ \lambda_1, \ldots, \lambda_n \}$. We have that,

$$BAB^{-1}Bv_i = BAv_i = \lambda_i Bv_i$$

Now we claim the reverse is true. If $C$ is a matrix with the same eigenvalues as $A$, and if there is an invertible matrix $B$ such that

$$\left\{ \begin{array}{l} \text{eigenvectors } B^{-1}u_1, \ldots, B^{-1}u_n \\ \text{of } C \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{eigenvalues } v_1, \ldots, v_n \\ \text{of } A \end{array} \right\}$$