Math 504 HW3

Rohan Mukherjee

November 28, 2023

1. (a) We claim that the natural projection $\pi : G \to G/H$ yields the one-to-one correspondence. First, notice that for any $H \leq K \leq G$, we have that $\pi(K) = \{ kH \mid k \in K \}$. Since $H \trianglelefteq G$, $H \trianglelefteq K$ (since $K \subset G$), so $\pi(K) = K/H$. Now we claim that if $S \leq G/H$, then $H \trianglelefteq \pi^{-1}(S) \leq G$, and also that $\pi^{-1}(S)/H = S$. Note that since π is onto it has a right inverse π^{-1}, so $\pi^{-1}(S)$ is actually defined. Now, given $a, b \in \pi^{-1}(S)$,

$$(ab^{-1})H = a(b^{-1}H) = aH \cdot b^{-1}H = aH \cdot (bH)^{-1} \in S$$

Since π is surjective, we have $\pi(\pi^{-1}(S)) = S$, which proves the one-to-one correspondence.

(b) Suppose that $K \trianglelefteq G$. We want $(gH)K/H(g^{-1}H) = K/H$ for every $gH \in G/H$, so let $kH \in K/H$ be arbitrary. Notice that $(gH)kH(g^{-1}H) = gkg^{-1}H = k_2H \in K/H$ (Note: $gkg^{-1} = k_2$ for some $k_2 \in K$ by normality). Now suppose that $K/H \trianglelefteq G/H$, fix $k \in K$, and let $g \in G$ be arbitrary. One sees that, since K/H is normal in G/H,

$$k_2H = (gH) \cdot (kH) \cdot (gH)^{-1} = (gkg^{-1})H$$

So we have $gkg^{-1}k_2^{-1} \in H \leq K$, so $gkg^{-1}k_2^{-1} = k_3$, i.e. $gkg^{-1} = k_3k_2 \in K$, proving the claim.

(c) I claim we have the following commutative diagram:

$$\begin{tikzcd}
G/H \arrow[d] \arrow[dr, "gH\mapsto gK"] & \\
\frac{G/H}{K/H} \arrow[r, dashed] & G/K
\end{tikzcd}$$

First, define $f : G/H \to G/K$ by $f(gH) = gK$. We must check that f is well-defined. If $g_1H = g_2H$, then $g_1g_2^{-1} \in H \leq K$, so $g_1K = g_2K$. To verify it is a homomorphism, we see that $f(g_1Hg_2H) = f((g_1g_2)H) = (g_1g_2)K = g_1Kg_2K = f(g_1H)f(g_2H)$. Finally, if $f(gH) = K$, then $gK = K$, which says $g \in K$, i.e. that $gH \in K/H$, which completes the proof.

2. Let G be a group of order p^2. By the class equation,

$$p^2 = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Since each g_i is not in $Z(G)$, by definition we can't have $C_G(g_i) = G$. So each $|G : C_G(g_i)|$ is divisible by p (Since $C_g(g_i)$ can't be p^2). This tells us that, for some constant $d = \frac{1}{p} \sum_{i=1}^{r} |G : C_G(g_i)| \in \mathbb{Z}$,

$$p^2 - pd = |Z(G)|$$

In particular, $|Z(G)|$ is divisible by p. If $|Z(G)| = p^2$ we are done, so suppose it equals p instead. Then $G/Z(G)$ is a group of order p and hence isomorphic to $\mathbb{Z}/p$, which is cyclic. Now we claim that if $G/Z(G)$ is cyclic then G is abelian. Indeed, write $G/Z(G) = \langle xZ(G) \rangle$, and let $a, b \in G$ be arbitrary. Then $a = x^n z_1$ for some $n \in \mathbb{Z}^+, z_1 \in Z(G)$, and $b = x^m z_2$ for some $n \in \mathbb{Z}^+, z_2 \in Z(G)$. Now,

$$ab = x^n z_1 x^m z_2 = x^n x^m z_1 z_2 = x^m x^n z_2 z_1 = x^m z_2 x^n z_1 = ba$$

This covers the other case.

3. (a) Notice first that vectors $\{ x_1, \ldots, x_n \} \subset \mathbb{F}_p^n$ are linearly independent iff every subset of $\{ x_1, \ldots, x_n \}$ are linearly independent. Since an invertible matrix is just an array of n vectors who are linearly independent, we can instead count this quantity. The first vector can be anything except 0, of which there are $p^n - 1$ possibilities. The second vector needs to be linearly independent from the first–so, it can't be any of the p multiples of the first, which gives $p^n - p$ possibilities. The third can't be a linear combination of the first or second–of which, we have p coefficients for the first vector, and p for the second vector, so we have $p^n - p^2$ remaining possibilities. Continuing this process, the last vector can't be any of the p^{n-1} linear combinations of the first $n - 1$ vectors. This yields our final answer of:

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

(b) Note first that $U_n(\mathbb{F}_p)$ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ because the determinant of a matrix in $U_n(\mathbb{F}_p)$ is just the product of the diagonals which is 1. We have $\binom{n}{2}$ degrees of freedom, so there are $p^{\binom{n}{2}}$ possibilities. Notice that the order of $\mathrm{GL}_n(\mathbb{F}_p)$ is equivalently,

$$(p^n - 1)p(p^{n-1} - 1)p^2(p^{n-2} - 1) \cdots p^{n-1}(p - 1) = p^{\sum_{i=1}^{n-1} i} \cdot \prod_{i=1}^{n} (p^i - 1)$$

We see that $\sum_{i=1}^{n-1} i = \binom{n}{2}$, and also that $p^i - 1 \equiv -1 \mod p$ for every $1 \leq i \leq n$, and in particular, is not divisible by p. So the largest power of p appearing in this factorization is just $\binom{n}{2}$, so the order of the largest p-group is at most $\binom{n}{2}$, which shows that $U_n(\mathbb{F}_p)$ is maximal. This subgroup is not unique: the set of all "strictly lower triangular" matrices is also of order $p^{\binom{n}{2}}$. Notice that this is a subgroup because of the following: let A, B be strictly lower triangular matrices. Then,

$$A \cdot B = (B^T A^T)^T$$

And since B^T, A^T are strictly upper triangular matrices, so is their product, and the transpose of a strictly upper triangular matrix is a strictly lower diagonal one. Similarly, since $(A^{-1})^T = (A^T)^{-1}$, this also shows that strictly lower diagonal matrices are closed under inverses.

(c) We claim that $\langle A, AB \rangle$ is a p-group. Notice that $[A, AB] = A^{-1}B^{-1}A^{-1}BAA = A^{-1}[B, A]A = A^{-1}A = 1$, since $[B, A] = [A, B]^{-1} = 1$. So, every element of $\langle A, AB \rangle$ can be written in the form $A^{\alpha}(AB)^{\beta}$ for some α, β. Next, notice that $(A^{\alpha}(AB)^{\beta})^p = A^{\alpha p}(AB)^{\beta p}$. Since both A, B have order p, and since $AB = BA$, AB has order dividing $\operatorname{lcm}(p, p) = p$ so $A^{\alpha p}(AB)^{\beta p} = 1$. If $|\langle A, AB \rangle|$ were not a power of p, by Cauchy's theorem it would have an element of order q for some prime $q \neq p$. But this is a contradiction–for $q \nmid p$, since the only divisors of p are 1 and p neither which are q. By Sylow's theorem, $\langle A, AB \rangle \leq SU_nS^{-1}$ for some $S \in \mathrm{GL}_n(\mathbb{F}_p)$. Thus,

$$S^{-1}AS = U \in U_n$$
$$S^{-1}ABS = V \in U_n$$

At last, we see,

$$S^{-1}ASS^{-1}BS = US^{-1}BS = V$$

That is, $S^{-1}BS = U^{-1}V \in U_n$, which completes the proof.

(d) The claim is not true if A, B do not commute. Consider $G = \mathrm{GL}_2(\mathbb{F}_2)$, $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Notice that both A, B have order 2. Also notice that $U_2(\mathbb{F}_2)$ is the set of all upper triangular matrices, since by necessity we need 1s along the main diagonals because entries are drawn from $\mathbb{F}_2$. So, if there was a matrix $S \in G$ such that $SAS^{-1}, SBS^{-1} \in U_2(\mathbb{F}_2)$, then $A, B \in S^{-1}U_2(\mathbb{F}_2)S$, and since all Sylow p-groups are conjugate, this would mean that A, B are in the same Sylow subgroup of G. We showed above that the set of strictly lower triangular matrices was also a Sylow 2-subgroup of G, and since A is in that Sylow 2-subgroup and B is in $U_2(\mathbb{F}_2)$, they are not in the same Sylow 2-subgroup, which means that such a matrix S cannot exist.