Math 504: Modern Algebra, Fall Quarter 2017
Jarod Alper
Midterm Solutions

Problem 1.1. Classify all groups of order 385 up to isomorphism.

Solution: Let G be a group of order 385. Factor 385 as $385 = 5 \cdot 7 \cdot 11$. Let n_5, n_7 and n_{11} be the number of $5, 7$ and 11-Sylow subgroups. Sylow's theorem implies that $n_5 \equiv 1 (\mathrm{mod}\, 5)$ and $n_5 | 77$. This implies that $n_5 = 1$ or 11. Similarly, we have that $n_7 \equiv 1 (\mathrm{mod}\, 7)$ and $n_7 | 55$ which implies that $n_7 = 1$, and $n_{11} \equiv 1 (\mathrm{mod}\, 11)$ and $n_{11} | 35$ which implies that $n_{11} = 1$.

In particular, we have a normal 7-Sylow subgroup $N_7 \subset G$ and a normal 11-Sylow subgroup $N_{11} \subset G$. Then $N := N_7 N_{11} \subset G$ is a subgroup of order 77. Moreover, N is normal in G since for $x \in N_7$, $y \in N_{11}$ and $g \in G$, we have that $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) \in N_7 N_{11} = N$. Let K be any Sylow 5-subgroup. By considering orders of subgroups, we see that $K \cap N = 1$ and $KN = G$. By the result from lecture, we know that

$$G \cong N \rtimes_\phi K$$

where $\phi \colon K \to \mathrm{Aut}(N)$ is a group homomorphism. We know that $K \cong \mathbb{Z}/5$, $N_7 \cong \mathbb{Z}/7$ and $N_{11} \cong \mathbb{Z}/11$. Since N_7 and N_{11} are normal in G, they are also normal in N. As $N_7 \cap N_{11} = 1$, we know that $N \cong \mathbb{Z}/7 \times \mathbb{Z}/11$. We also know from lecture that $\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}/7 \times \mathbb{Z}/11) \cong \mathbb{Z}/6 \times \mathbb{Z}/10$. We need to classify group homomorphisms

$$\phi \colon K \cong \mathbb{Z}/5 \to \mathbb{Z}/6 \times \mathbb{Z}/10 \cong \mathrm{Aut}(N).$$

Since the element $\phi(1) \in \mathbb{Z}/6 \times \mathbb{Z}/10$ has order dividing 5, we know that $\phi(1) = (0, 2i)$ for $i \in \{0, 1, 2, 3, 4\}$. There are two cases:

Case 1: $i = 0$. In this case, $G \cong N \times K = \mathbb{Z}/77 \times \mathbb{Z}/5 \cong \mathbb{Z}/385$ and is clearly abelian.

Case 2: $i \neq 0$. In this case, let $\alpha_i \colon \mathbb{Z}/5 \to \mathbb{Z}/5$ be the automorphism of groups defined by $k \mapsto ki$. If $\phi_i \colon \mathbb{Z}/5 \to \mathbb{Z}/6 \times \mathbb{Z}/10$ denotes the group homomorphism determined by $\phi_i(1) = (0, 2i)$, then clearly $\phi_i = \phi_1 \circ \alpha_i$. By Homework Problem 3.1(1), we know that the two semi-direct products $\mathbb{Z}/77 \rtimes_{\phi_1} \mathbb{Z}/5$ and $\mathbb{Z}/77 \rtimes_{\phi_i} \mathbb{Z}/5$ are isomorphic. Therefore, we have only one non-trivial semi-direct product $\mathbb{Z}/77 \rtimes_{\phi_1} \mathbb{Z}/5$ up to isomorphism. Since this group is not abelian, it is not isomorphic to $\mathbb{Z}/385$ and we may conclude that there are only two groups of order 385 up to isomorphism: $\mathbb{Z}/385$ and $\mathbb{Z}/77 \rtimes_{\phi_1} \mathbb{Z}/5$.

Problem 1.2. Let $G = \mathrm{GL}_3(\mathbb{C})$ be the group of invertible 3×3 matrices with entries in $\mathbb{C}$. Let $H \subset G$ be the subgroup consisting of diagonal matrices.

(1) Find the centralizer $C_G(H)$ of H in G.
(2) Find the normalizer $N_G(H)$ of H in G.
(3) Determine the quotient $N_G(H)/H$; that is, identify this group with a familiar group.

Solution: For (1), first observe that as H is abelian $H \subset C_G(H)$. The centralizer $C_G(H)$ consists of 3×3 matrices

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

such that $AD = DA$ for every diagonal matrix

$$D = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3. \end{pmatrix}$$

The condition that $AD = DA$ translates into

$$AD = \begin{pmatrix} d_1 a_{1,1} & d_2 a_{1,2} & d_3 a_{1,3} \\ d_1 a_{2,1} & d_2 a_{2,2} & d_3 a_{2,3} \\ d_1 a_{3,1} & d_2 a_{3,2} & d_3 a_{3,3} \end{pmatrix} = \begin{pmatrix} d_1 a_{1,1} & d_1 a_{1,2} & d_1 a_{1,3} \\ d_2 a_{2,1} & d_2 a_{2,2} & d_2 a_{2,3} \\ d_3 a_{3,1} & d_3 a_{3,2} & d_3 a_{3,3} \end{pmatrix} = DA.$$

Since this must hold for every non-zero choice of d_1, d_2 and d_3, we conclude that $a_{i,j} = 0$ if $i \neq j$, that is, $A \in H$ is diagonal.

For (2), the normalizer $N_G(H)$ consists of 3×3 matrices $A = (a_{i,j})$ such that for every diagonal matrix $D = \operatorname{diag}(d_1, d_2, d_3)$ we have that $DA = AD'$ for another diagonal matrix $D' = \operatorname{diag}(d_1', d_2', d_3')$. The condition that $AD = D'A$ translates into

$$AD = \begin{pmatrix} d_1 a_{1,1} & d_2 a_{1,2} & d_3 a_{1,3} \\ d_1 a_{2,1} & d_2 a_{2,2} & d_3 a_{2,3} \\ d_1 a_{3,1} & d_2 a_{3,2} & d_3 a_{3,3} \end{pmatrix} = \begin{pmatrix} d_1' a_{1,1} & d_1' a_{1,2} & d_1' a_{1,3} \\ d_2' a_{2,1} & d_2' a_{2,2} & d_2' a_{2,3} \\ d_3' a_{3,1} & d_3' a_{3,2} & d_3' a_{3,3} \end{pmatrix} = D'A.$$

Since this must hold for each d_1, d_2 and d_3, we see that A must have precisely one non-zero element in each row and each column. Indeed, if $a_{i,j} \neq 0$, then $d_j = d_i'$. If $a_{i,j'} \neq 0$ for $j' \neq j$, then $d_{j'} = d_i' = d_j$ which certainly doesn't hold for all d_1, d_2, d_3. Similarly, if $i' \neq i$, then $d_{i'}' = d_j = d_i'$ which also can't hold.

Let $P_3 \subset \mathrm{GL}_3(\mathbb{C})$ be the subgroup consisting of permutations matrices. Then

$$\begin{aligned} P_3 H = & \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 0 & * & 0 \\ * & 0 & 0 \\ 0 & 0 & * \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 0 & 0 & * \\ 0 & * & 0 \\ * & 0 & 0 \end{pmatrix} \right\} \\ & \bigcup \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & * \\ 0 & * & 0 \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 0 & * & 0 \\ 0 & 0 & * \\ * & 0 & 0 \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{pmatrix} \right\} \end{aligned}$$

where $*$ could be any non-zero complex number. We have verified that $N_G(H) \subset P_3 H$. It is a simple calculation to conclude that each of these matrices normalizes H, that is, $P_3 H \subset N_G(H)$. We conclude that $N_G(H) = P_3 H$.

For (3), observe that $P_3 \cap H = 1$. We also know that the subgroup P_3 of 3×3 permutation matrices is isomorphic to the symmetric group S_3. We may use the 2nd isomorphism theorem to conclude that

$$N_G(H)/H \cong P_3 H/H \cong P_3/P_3 \cap H \cong P_3 \cong S_3.$$

Alternatively, you can simply write down a surjective group homomorphism $P_3 H \to P_3$ which replaces an element in the normalizer with the matrix where each non-zero entry is replaced with a 1. The kernel of this homomorphism is clearly H. Therefore, $N_G(H)/H \cong P_3 H/H \cong P_3$.

Problem 1.3. Find *all* possible composition series for the dihedral group D_{12} of order 12.

Solution: We write $D_{12} = \langle r, s \,|\, r^6 = s^2 = 1, rs = sr^{-1}\rangle$. We first observe that $1 \trianglelefteq \langle r^3 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_{12}$ is a composition series with factors $\mathbb{Z}/3, \mathbb{Z}/2$ and $\mathbb{Z}/2$. By the Jordan–Hölder theorem, any composition series will have these factors up to reordering. Therefore, if $1 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq D_{12}$ is a composition series, then N_2 is a normal subgroup of order 4 or 6. We claim that there are no normal subgroups of order 4. Since $12 = 2^2 \cdot 3$, a subgroup of order 4 is a 2-Sylow. The subgroup $\langle r^3, s\rangle$ is a 2-Sylow but it is not normal since $rsr^{-1} = sr^4 \notin \langle r^3, s\rangle$. Since all 2-Sylow's are conjugate, there are no normal 2-Sylow subgroups.

We now classify all subgroups of D_{12} of order 6. Let $N_2 \trianglelefteq D_{12}$ be a subgroup of order 6, which is necessarily normal. By Cauchy's theorem, N_2 has a subgroup $H \subset N_2$ of order 3. Then $H \subset D_{12}$ is a 3-Sylow subgroup. Observe that $\langle r^2 \rangle \subset D_{12}$ is a 3-Sylow subgroup and that it is normal: indeed, $sr^2s = r^4 \in \langle r^2 \rangle$. It follows that $\langle r^2 \rangle \subset D_{12}$ is the unique subgroup of order 3. Thus $H = \langle r^2 \rangle \subset N_2$ and N_2 is obtained from $\langle r^2 \rangle$ by adjoining an element of order 2. We can enumerate all elements of D_{12} of order 2: $s, sr, sr^2, sr^3, sr^4, sr^5, r^3$. Adjoining these creates 3 distinct subgroups of order 6: $\langle r \rangle$, $\langle r^2, s\rangle$ and $\langle r^2, sr\rangle$. Observe that $\langle r \rangle \cong \mathbb{Z}/6$, which has 2 composition series: $1 \trianglelefteq \langle r^3 \rangle \trianglelefteq \langle r \rangle$ and $1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle$. Also, both $\langle r^2, s\rangle$ and $\langle r^2, sr\rangle$ are isomorphic to S_3 which has a unique composition series $1 \trianglelefteq \langle (123) \rangle \trianglelefteq S_3$. Putting these observations together, we have four distinct composition series:

$$\begin{array}{llll}
1 & \trianglelefteq \langle r^3 \rangle & \trianglelefteq \langle r \rangle & \trianglelefteq D_{12} \\
1 & \trianglelefteq \langle r^2 \rangle & \trianglelefteq \langle r \rangle & \trianglelefteq D_{12} \\
1 & \trianglelefteq \langle r^2 \rangle & \trianglelefteq \langle r^2, s \rangle & \trianglelefteq D_{12} \\
1 & \trianglelefteq \langle r^2 \rangle & \trianglelefteq \langle r^2, sr \rangle & \trianglelefteq D_{12}.
\end{array}$$

Problem 1.4. Prove that a group of order p^2q is solvable, where p and q are distinct primes. (Recall from HW Problem 2.2 that a finite group is *solvable* if and only if there exists a composition series with abelian factors.)

Solution: Let G be a group of order p^2q. Let n_p and n_q be the number of p and q-Sylow subgroups, respectively. Sylow's theorem implies that $n_p \equiv 1 (\bmod\, p)$ and $n_p | q$, and that $n_q \equiv 1 (\bmod\, q)$ and $n_q | p^2$. Therefore, $n_p \in \{1, q\}$ and $n_q \in \{1, p, p^2\}$.

If $n_p = 1$, then there exists a normal subgroup $N \trianglelefteq G$ of order p^2. From lecture, we know that N is isomorphic to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$ and, in particular, N is abelian. In this case, G is solvable.

If $n_q = 1$, then there exists a normal subgroup $N \trianglelefteq G$ of order q, and G/N is a group of order p^2, which (as above) is abelian as it is isomorphic to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$. In this case, G is again solvable.

If $n_p = q$ and $n_q \in \{p, p^2\}$. Then $q \equiv 1 (\bmod\, p)$ so that $q > p$. Observe that $n_q \neq p$ as this would imply that $q < p$. We are left with the case that $n_p = q$ and $n_q = p^2$. In this case, we have p^2 Sylow subgroups of order q, and therefore $p^2(q-1)$ distinct elements of order q. There are only p^2 remaining elements in G which necessarily must form a p-Sylow subgroup. Since all p-Sylow's are conjugate, we see that this p-Sylow is normal and that $n_p = 1$, a contradiction.

Problem 1.5.

(1) Find a Sylow 7-subgroup of $\mathrm{GL}_3(\mathbb{F}_2)$.

(2) Show that $\mathrm{GL}_3(\mathbb{F}_2)$ is isomorphic to the subgroup of S_7 generated by the permutations (1234567) and $(15)(23)$.

Hint: Consider the action of $\mathrm{GL}_3(\mathbb{F}_2)$ on the set $\mathbb{F}_2^3 \setminus 0$ containing 7 elements and the induced homomorphisms $\mathrm{GL}_3(\mathbb{F}_2) \to S_7$.

Solution: Let us first observe that $|\,\mathrm{GL}_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3 \cdot 3 \cdot 7$ by a simple counting argument: the first column has to be non-zero, the second column can't be a multiple of the first and the third column has to be linearly independent to the first 2.

For (1), we simply want to find a matrix $A \in \mathrm{GL}_3(\mathbb{F}_2)$ of order 7 as this will generate a 7-Sylow. This can be found by trial and error. (In fact, it turns out that the number of 7-Sylows is 8 so there are 68 elements of order 7 so a random element has roughly a 28% chance of being an element of order 7.)

Consider

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

This element has order 7. One way to see this (other than laboriously computing the powers of A) is to think about how it acts on $\mathbb{F}_2^3 \setminus 0$:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \overset{A}{\longmapsto} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

This shows that A has an element of order 7. (In fact, the way I found the matrix A was by playing around with the coefficients so that A would cycle through the 7 elements of $\mathbb{F}_2^3 \setminus 0$.)

Order the elements of $\mathbb{F}_2^3 \setminus 0$ by defining $v_i = A^{i-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

For (2), the action of $\mathrm{GL}_3(\mathbb{F}_2)$ on the set $\mathbb{F}_2^3 \setminus 0 = \{v_1, \dots, v_7\}$ induces a group homomorphism $\pi\colon \mathrm{GL}_3(\mathbb{F}_2) \to S_7$ which is necessarily injective since a matrix that fixes every element of $\mathbb{F}_2^3 \setminus 0$ must be the identity. Define the matrix

$$B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

so that B swaps v_1 and v_5, swaps v_2 and v_3, and fixes all other vectors. The matrix B was constructed so that $\pi(B) = (15)(23) \in S_7$.

Since $\mathrm{GL}_3(\mathbb{F}_3) = \mathrm{im}(\pi)$, it suffices to show that the matrices A and B generate $\mathrm{GL}_3(\mathbb{F}_3)$, or alternatively that the permutations (1234567) and $(15)(23)$ generate a subgroup of order 168. This can be proven in a variety of ways. The solution here is a variant of the clever solutions of Kristine Hampton and Thomas Lou. Let $H = \langle A, B\rangle \subset \mathrm{GL}_3(\mathbb{F}_3)$, then we only need to show $|H| = 168 = 2^3 \cdot 3 \cdot 7$. We know H has an element of order 7 and 2. This implies that H has order $2^i \cdot 3^j \cdot 7$ for $i = 1, 2, 3$ and $j = 0, 1$. Also $\langle A\rangle \subset H$ is not normal since one can check that $BAB^{-1} \notin \langle A\rangle$. This implies that the number n_7 of 7-Sylows in H is greater than 1. But in fact $n_7 = 8$ since $n_7 \cong 1 (\mathrm{mod}\, 7)$ and n_7 must divide $2^i 3^j$, which in turn divides 24. Looking at the condition that 8 divides $2^i 3^j$ implies that $i = 3$ and $j = 1$, which shows that $|H| = 2^3 \cdot 3 \cdot 7$.

(Alternatively, one could directly construct elements of order 3 (e.g., AB has order 3) and a subgroup of order 8. This requires playing around with elements a bit either in $\mathrm{GL}_3(\mathbb{F}_2)$ or S_7.)

Problem 1.6. Let k be a field.

(1) Show that the ideal $(xy - zw) \subset k[x, y, z, w]$ is prime.
(2) Show that the element $x \in k[x, y, z, w]/(xy - zw)$ is irreducible but not prime.

Solution: For (1), let $R = k[y, z, w]$ and consider the degree 1 polynomial $f = xy - zw \in R[x]$. The ideal $\mathfrak{p} = (w) \subset R$ is prime. The leading coefficient of f is y which is not in $\mathfrak{p}$ and the constant coefficient is zw which is in $\mathfrak{p}$ but not in $\mathfrak{p}^2$. By Eisenstein's criterion $xy - zw \in R[x] = k[x, y, z, w]$ is irreducible. Since $k[x, y, z, w]$ is a UFD, it follows that $(xy - zw)$ is a prime ideal.

For (2), we will use the following lemma:

Lemma: Let $f \in k[x_1, \ldots, x_n]$ be an irreducible homogeneous polynomial in n variables and $R = k[x_1, \ldots, x_n]/(f)$. Then there is a function $\deg\colon R \setminus 0 \to \mathbb{Z}_{\geq 0}$ which is defined as follows: for $g + (f) \in R$, then $\deg(g + (f))$ is defined as the smallest degree of a polynomial of the form $g + fh$ for any $h \in k[x_1, \ldots, x_n]$. For $g_1, g_2 \in R \setminus 0$, we have that $\deg(g_1 g_2) = \deg(g_1) + \deg(g_2)$.

Proof of Lemma: Let $S = k[x_1, \ldots, x_n]$ and $S_d \subset S$ be the homogeneous elements of degree d. Then $S \cong \oplus_{d\geq 0} S_d$ as abelian groups with the property that for $x \in S_d$ and $y \in S_e$ non-zero, the product xy is in S_{d+e} (in other words, S is a graded ring). Let $\pi\colon S \to R$ be the canonical surjection onto the quotient. Define $R_d = \pi(S_d)$. Then it is easy to check that $R \cong \oplus_{d\geq 0} R_d$ as abelian groups and that the multiplication of a non-zero element in R_d by a non-zero element in R_s is in R_{d+s}. The degree (as we've defined it above) of an element $g = g_0 + \cdots + g_d \in R$, with $g_i \in R_i$ and $g_d \neq 0$, is precisely d. Finally, since f is an irreducible element, the ideal (f) is prime and therefore R is an integral domain. It follows that for non-zero elements $g_1, g_2 \in R$ that $\deg(g_1 g_2) = \deg(g_1) + \deg(g_2)$. $\square$

If it is possible to write $x = q_1 q_2$ with $q_1, q_2 \in R = k[x, y, z, w]/(xy - zw)$, then by the Lemma, we know that $\deg(q_1) + \deg(q_2) = \deg(x) = 1$. Therefore $\deg(q_1)$ or $\deg(q_2)$ has to be zero in which case it is a non-zero constant and thus a unit. Therefore, x is irreducible.

To see if x is prime, the quotient $R/(x) \cong k[x, y, z, w]/(xy-zw, x) \cong k[y, z, w]/(zw)$ which is not an integral domain. Therefore $x \in R$ is not prime.