504 Homework 6

Daniel Rui - 12/1/20

Problem 1

Let G be the group with presentation $\langle a, b \mid a^4 = b^4 = 1, bab^{-1} = a^{-1}\rangle$. We want to show that $|G| = 16$.

The given relation $bab^{-1} = a^{-1}$ is equivalent to the relation $ab = ba^{-1}$; with this latter formulation, it is easy to see that for any possible word written using the alphabet $\{a, b\}$, say $a^{m_1}b^{n_1}\cdots a^{m_k}b^{n_k}$ (where the exponents are non-negative integers), we can move any a^{m_i} left of a b to its right (becoming a^{-m_i}), and thus swap by swap we can move all the a's to the right of all the b's. Thus, all words can be simplified to the form $b^n a^m$, and furthermore because we know $a^4 = b^4 = 1$, we can further restrict $n, m \in \{0, 1, 2, 3\}$. Now observe that $\langle a\rangle \trianglelefteq G$: for any $a^k \in \langle a\rangle$, and arbitrary $b^n a^m \in G$,

$$(b^n a^m)a^k(b^n a^m)^{-1} = b^n a^m a^k a^{-m} b^{-n} = b^n a^k b^{-n} = (bab^{-1})^k = (a^{-1})^k = a^{-k} \in \langle a\rangle$$

Note that $G/\langle a\rangle = \{g\langle a\rangle : g \in G\} = \{b^n a^m\langle a\rangle : n, m \in \{0, 1, 2, 3\}\} = \{b^n\langle a\rangle : n \in \{0, 1, 2, 3\}\} \simeq \langle b\rangle$. Thus, by Lagrange's theorem, we have that $\frac{|G|}{|\langle a\rangle|} = \left|\frac{G}{\langle a\rangle}\right| = |\langle b\rangle| \implies |G| = |\langle a\rangle||\langle b\rangle|$.

All the remains now is to establish that $|\langle a\rangle| = |\langle b\rangle| = 4$, i.e. that a and b both have order 4. The relation $a^4 = b^4 = 1$ means that a and b are either order 1, 2, or 4. Thus, if we can show that the relations don't force $a^2 = 1$ or $b^2 = 1$, then we will have that a and b are order 4. We *can* in fact show that, by finding some group that satisfies all the relations (i.e. it is generated by two elements a, b s.t. $a^4 = b^4 = 1$ and $bab^{-1} = a^{-1}$) that doesn't have a^2 or b^2 equal to 1.

Consider the semi-direct product $N \rtimes H$ for $H = N = C_4 = (\{0, 1, 2, 3\}, +)$ with the group homomorphism $\phi : H \to \mathrm{Aut}(N)$ defined as $\phi_h(n) := [\phi(h)](n) = hn^{-1}h^{-1}$. Recall that the group operation $\bullet$ for $N \rtimes H$ is defined as $(n_1, h_2)\bullet(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$. Define $a = (1, 0)$ and $b = (0, 1)$. We now show that $C_4 \rtimes C_4$ satisfies all the relations, and also doesn't have a^2, b^2 equal to $e := 1_{C_4\rtimes C_4} = (0, 0)$:

- $a^2, b^2 \neq e$ and $a^4 = b^4 = e$: from the definition, $a^2 = (1, 0) \bullet (1, 0) = (1 + \phi_0(1), 0 + 0)$. Note that ϕ_0 is the trivial automorphism because ϕ is a group homomorphism and hence sends the identity ($0 \in H$) to the identity ($\mathrm{id} \in \mathrm{Aut}(N)$), and so $a^2 = (1 + 1, 0 + 0) = (2, 0) \neq (0, 0) = e$. It's now easy to see that $a^4 = a^2 \bullet a^2 = (2 + \phi_0(2), 0 + 0) = (2 + 2, 0 + 0) = (0, 0)$.

  Similarly, $b^2 = (0+\phi_1(0), 1+1) = (0+0, 1+1) = (0, 2) \neq (0, 0)$ because ϕ_1 is an automorphism and hence sends the identity to the identity, and $b^4 = b^2 \bullet b^2 = (0+\phi_2(0), 2+2) = (0+0, 2+2) = (0, 0)$.

- $ab = ba^{-1}$: first, we have that $a^{-1} = (3, 0)$, because $a^{-1}\bullet a = (3+\phi_0(1), 0+0) = (3+1, 0) = (0, 0) = (1 + \phi_0(3), 0 + 0) = a \bullet a^{-1}$. Then, $b \bullet a^{-1} = (0, 1) \bullet (3, 0) = (0 + \phi_1(3), 1 + 0) = (\phi_1(3), 1) = (1, 1)$ because $\phi_1(3) = 1 + 3^{-1} + 1^{-1} = 1 + 1 + 3 = 1$, and $a \bullet b = (1 + \phi_0(0), 0 + 1) = (1, 1)$.

- Finally, a, b generate $C_4 \rtimes C_4$ because $a^m \bullet b^n = (m, 0) \bullet (0, n) = (m + \phi_0(0), 0 + n) = (m, n)$.

Thus, we are done.

Problem 2

Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the set of all 2×2 matrices with integer entries and determinant 1. Let us now define the projective special linear group over $\mathbb{Z}$, $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\mathrm{Id}, -\mathrm{Id}\}$.

We want to show that $\mathrm{PSL}_2(\mathbb{Z}) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$ (a free product). Let us first define two important matrices,

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

A quick calculation yields

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad B^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

Obviously, $\mathbb{Z}_2$ and $\mathbb{Z}_3$ respectively have presentations $\langle A \mid A^2 = \mathrm{Id} \rangle$ and $\langle B \mid B^3 = \mathrm{Id} \rangle$, and so by the definition of free product, $\mathbb{Z}_2 * \mathbb{Z}_3 \simeq \langle A, B \mid A^2 = B^3 = \mathrm{Id} \rangle$. To show that this is isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$, we show that A, B generate $\mathrm{SL}_2(\mathbb{Z})$, and each word $A^{0,1}B^{1,2}A^1B^{1,2}\cdots B^{1,2}A^1B^{1,2}A^{0,1}$ is a unique matrix (once evaluated) in $\mathrm{PSL}_2(\mathbb{Z})$.

Part 1: A, B generate $\mathrm{SL}_2(\mathbb{Z})$. First, let us define $C = AB = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. One can check that $C^{-1} = \left[\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right]$ and verify by induction that for $n \in \mathbb{N}$, $C^n = \left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$ and $C^{-n} = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ (so in fact $C^n = \left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$ holds for all $n \in \mathbb{Z}$).

Now let's say that we're given a matrix $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. If $c = 0$, we know that because $\det(M) = 1$, M must look like $\left[\begin{smallmatrix} \pm 1 & m \\ 0 & \pm 1 \end{smallmatrix}\right]$ for some $m \in \mathbb{Z}$. That is, we know that matrices in $\mathrm{SL}_2(\mathbb{Z})$ of this form ($c = 0$) can be written as $\pm T^{\pm m}$, i.e. a product of A's and B's (recall that $A^2 = -\mathrm{Id}$, and $T = AB$).

Thus, for a matrix $M \in \mathrm{SL}_2(\mathbb{Z})$ with $c \neq 0$, if we can multiply by some A's and B's and get it to the $c = 0$ case, then we'll be done (because we can just move all the A's and B's to the other side by multiplying by inverses, resulting in $M =$ some product of A's and B's). The key to this reduction lies in the following identities:

$$AM = \begin{bmatrix} c & d \\ -a & -b \end{bmatrix} \quad \text{and} \quad C^n M = \begin{bmatrix} a + cn & b + dn \\ c & d \end{bmatrix}$$

With these identities, we can iterate the division algorithm and get the lower left corner to be 0, as follows: as long as the lower left entry c is non-zero, we can write the upper left entry a as $a = cq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < |c|$ (by the division algorithm), and so multiplying by C^{-q} (on the left) we get that the new upper left entry is r, where $r < |c|$. Multiplying this (on the left) by A makes the new lower left entry $c' = -r$. Iterating this process, we see that we get a sequence of integers $c, c', c'', \ldots$ s.t. $|c| > |c'| > |c''| > \ldots$. Since any strictly decreasing chain of non-negative integers must end, and since the process can continue as long as the lower left entry is non-zero, we see that the process MUST reach a matrix with lower left entry $= 0$. This finishes the proof.

Part 2: each word $A^{0,1}B^{1,2}A^1B^{1,2}\cdots B^{1,2}A^1B^{1,2}A^{0,1}$ is a unique matrix (once evaluated) in $\mathrm{PSL}_2(\mathbb{Z})$. The map $\phi : \langle A, B \mid A^2 = B^3 = \mathrm{Id}\rangle \to \mathrm{PSL}_2(\mathbb{Z})$ (maybe think of $\mathrm{PSL}_2(\mathbb{Z})$ as subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with upper-left entry positive) defined by evaluating the word is a group homomorphism, and showing that it is injective is equivalent to showing that $\ker\phi$ is trivial. Surjectivity is given by **Part 1**, so by the end of this part we'll have shown that ϕ is an isomorphism, so indeed $\mathrm{PSL}_2(\mathbb{Z}) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$.

Let us associate each matrix $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with the map φ_M defined by $x \mapsto \frac{ax+b}{cx+d}$ (that acts only the irrationals to avoid any issues with the denominator being 0) — the only requirement is that c, d are not both 0, which is guaranteed by $\det(M) = 1$. Note that for matrices $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $N = \left[\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right]$,

$$\varphi_M \circ \varphi_N = \frac{a(\frac{ex+f}{gx+h}) + b}{c(\frac{ex+f}{gx+h}) + d} = \frac{(ae+bg)x + (af+bh)}{(ce+dg)x + (cf+dh)} = \varphi_{MN}.$$

If we can show that for any non-trivial word, the associated φ is not trivial, i.e. that there is some irrational x s.t. $\varphi(x) \neq x$, then we will have that $\ker\phi$ is just the empty word, because then only the empty word would correspond to Id, which has associated map φ_{Id} that maps $x \mapsto x$.

The associated maps of A, B, and B^2 are $\varphi_A(x) = \frac{1}{-x}, \varphi_B(x) = \frac{-1}{x+1}$, and $\varphi_{B^2}(x) = \frac{-x-1}{x} = -1 - \frac{1}{x}$. Let us define the four sets $\mathscr{P}^+, \mathscr{P}^-, \mathscr{N}^-, \mathscr{N}^+$ to be respectively the irrationals in the sets $(1,\infty)$, $(0,1)$, $(-1,0)$, and $(-\infty,-1)$. Observe the following facts:

- $\varphi_A(\mathscr{P}^\pm) = \mathscr{N}^\mp$ (shorthand for "$\varphi_A(\mathscr{P}^+) = \mathscr{N}^-$ and $\varphi_A(\mathscr{P}^-) = \mathscr{N}^+$"); and $\varphi_A(\mathscr{N}^\mp) = \mathscr{P}^\pm$.
- $\varphi_B(\mathscr{P}^\pm) = \mathscr{N}^-$ (in this context $\mathscr{P}^\pm = \mathscr{P}^+ \cup \mathscr{P}^-$); $\varphi_B(\mathscr{N}^-) = \mathscr{N}^+$; and $\varphi_B(\mathscr{N}^+) = \mathscr{P}^\pm$.
- $\varphi_B(\mathscr{P}^\pm) = \mathscr{N}^+$; $\varphi_B(\mathscr{N}^-) = \mathscr{P}^+$; and $\varphi_B(\mathscr{N}^+) = \mathscr{N}^-$.

A bit of casework concludes the problem: in each case, we input an irrational from one or two of the four sets, and show that the output is in a different set, thus showing that φ can not possibly be φ_{Id}.

- Case 1: begins and ends with B's, i.e. our word looks like $W = B^{1,2}A^1B^{1,2}\cdots B^{1,2}A^1B^{1,2}$. Then $\varphi_W = \varphi_{B^{1,2}} \circ \varphi_A \circ \cdots \circ \varphi_{B^{1,2}} \circ \varphi_A \circ \varphi_{B^{1,2}}$ applied to a positive irrational will output a negative, because $B^{1,2}$ (both B^1 and B^2) turns a positive into a negative, and A turns a negative back to positive, and so on until the leftmost $B^{1,2}$ turns a positive into a negative.
- Case 2: begins and ends with A's, i.e. our word looks like $W = A^1B^{1,2}A^1B^{1,2}\cdots B^{1,2}A^1$. If φ_W takes in a negative, the rightmost A turns it into a positive, and so we can apply Case 1 (which outputs a negative), and then the apply the leftmost A to output a positive.
- Case 3: begins with a B and ends with an A, i.e. our word looks like $W = B^{1,2}A^1\cdots B^{1,2}A^1$. If the leftmost $B^{1,2}$ is B^1, we know that $\varphi_B(\mathscr{P}^\pm) = \mathscr{N}^-$, so if we input a negative irrational in $\mathscr{N}^+$, we can apply Case 2 so that the input to the leftmost φ_{B^1} is a positive, forcing it to output a negative irrational in $\mathscr{N}^-$.

  If the leftmost $B^{1,2}$ is instead B^2, we know that $\varphi_B(\mathscr{P}^\pm) = \mathscr{N}^+$, so it's just like the B^1 case except we input a negative in $\mathscr{N}^-$ and get an output in $\mathscr{N}^+$.

- Case 4: begins with an A and ends with a B, i.e. our word looks like $W = A^1B^{1,2}A^1 \cdots B^{1,2}$. If φ_W were indeed φ_{Id}, then we would have that $\varphi_{AWA} = \varphi_A \circ \varphi_W \circ \varphi_A = \varphi_A \circ \varphi_A = \varphi_{AA} = \varphi_{\mathrm{Id}}$. But AWA is a word of the type covered by Case 3, and so this is impossible.

Problem 2b

We want to show that $\mathrm{SL}_2(\mathbb{Z}) \simeq \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$ (an amalgamated product). Recall that in general for $A = \langle X_A \mid W_A \rangle$ (where X_A is a set of generators and W_A is a set of relations), $B = \langle X_B \mid W_B \rangle$, and $H = \langle X_H \mid W_H \rangle$, then $A *_H B := \langle X_A \cup X_B \mid W_A \cup W_B \cup \{\varphi(x) = \psi(x)\}_{x \in X_H} \rangle$ where $\varphi : H \to A$ and $\psi : H \to B$ are injective group homomorphisms (assuming no notational doubling; if there is, think of the unions as disjoint unions). Thus in particular, $\mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6 \simeq \langle A \mid A^4 = \mathrm{Id} \rangle *_{\langle x \mid x^2 = 1 \rangle} \langle B \mid B^6 = \mathrm{Id} \rangle$ is $\langle A, B \mid A^4 = B^6 = \mathrm{Id}, \varphi(x) = \psi(x) \rangle$ where $\varphi(x^n) = A^{2n}$ and $\psi(x^n) = B^{3n}$; that is to say, $\mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6 \simeq \langle A, B \mid A^4 = B^6 = 1, A^2 = B^3 \rangle$.

We want to show that this is isomorphic to $\mathrm{SL}_2(\mathbb{Z})$. Like we did in **Part 2** of Problem 2a above, we define a group homomorphism $\Phi : G \to \mathrm{SL}_2(\mathbb{Z})$ ($G := \langle A, B \mid A^4 = B^6 = \mathrm{Id}, A^2 = B^3 \rangle$) by evaluating the word. As above, surjectivity is given by **Part 1** of Problem 2a, so we just need to prove injectivity.

Notice first that $A^2A^m = A^mA^2$ and $A^2B^n = B^3B^n = B^nB^3 = B^nA^2$, which means that for any word $W \in G$, $A^2W = WA^2$ because we can swap A^2 to the right of any A^m and B^n over and over until A^2 is all the way to the right. This means two important things: $N := \{\mathrm{Id}, A^2\}$ is central (hence normal) subgroup of G, and $G/N = \{WN : W \in G\} \simeq \langle A, B \mid A^2 = B^3 = \mathrm{Id} \rangle \simeq \mathrm{PSL}_2(\mathbb{Z})$ (because for any word W, if that word contains $A^{2,3}$ or $B^{3,4,5}$, we can move those A^2 or B^3 all the way to the right to merge with N, leaving a reduced word W' with only A^1 and $B^{1,2}$, i.e. a word in $\langle A, B \mid A^2 = B^3 = \mathrm{Id} \rangle$).

Now consider the induced map $\phi : G/N \to \mathrm{PSL}_2(\mathbb{Z})$ (thinking of $\mathrm{PSL}_2(\mathbb{Z})$ as $\mathrm{SL}_2(\mathbb{Z})/\{\mathrm{Id}, -\mathrm{Id}\}$), defined by $\phi(WN) = \Phi(W)\{\mathrm{Id}, -\mathrm{Id}\}$. This is well defined (and a homomorphism), because if $W_1N = W_2N$, then $W_1 = W_2n$ where n is either Id or A^2 (so $\Phi(n)$ is either Id or $-\mathrm{Id}$), and so $\phi(W_1N) = \Phi(W_1)\{\mathrm{Id}, -\mathrm{Id}\} = \Phi(W_1)\Phi(n)\{\mathrm{Id}, -\mathrm{Id}\} = \Phi(W_2)\{\mathrm{Id}, -\mathrm{Id}\} = \phi(W_2N)$. The choice of name for this map was no coincidence; it can be thought of as the same map as ϕ from **Part 2** of Problem 2a. Thus ϕ is an isomorphism.

Let W_0 be some arbitrary element in $\ker \Phi$ was not trivial, i.e. $\Phi(W_0) = \mathrm{Id}$. Then we would have that $\phi(W_0N) = \Phi(W_0)\{\mathrm{Id}, -\mathrm{Id}\} = 1_{\mathrm{PSL}_2(\mathbb{Z})}$. That would mean that $W_0N \in \ker \phi$, but $\ker \phi$ is trivial, so it must be that $W_0N = N \iff W_0 \in N$. We can explicitly calculate Φ for the elements of N: $\Phi(\mathrm{Id}) = \mathrm{Id}$, and $\Phi(A^2) = -\mathrm{Id}$. Thus, we've just shown that W_0 must be Id. Thus, Φ is injective, and we are done.

Problem 3

Let us denote by E_{ij} an $n \times n$ matrix with entry (i, j) as 1 and all other entries as 0. Let I_n be the identity matrix, B_n be the group of upper triangular matrices over a field F ($\mathbb{R}$ or $\mathbb{F}_p$), $U_n \leq B_n$ be the the subgroup of matrices with 1's on the diagonal, and $U_n^{(k)} \leq U_n$ be the subgroup of all matrices with the first k super diagonals being 0. Let us assume that $n > 1$ and $p > 2$.

(a) We want to show that the matrices in $\mathscr{S} := \{(I_n + aE_{i,j}) : a \in F, 1 \leq i < j \leq n\}$ generate U_n. We proceed by downward induction; i.e. the base case is verifying that indeed $\mathscr{S}$ generates $U_n^{(n-1)} = \{I_n\}$, and the induction step is using the assumption that $\mathscr{S}$ generates $U_n^{(k)}$ to prove that $\mathscr{S}$ generates $U_n^{(k-1)}$. The conclusion of the induction is that $\mathscr{S}$ generates $U_n^{(0)} = U_n$.

Note that for any matrix M, $ME_{i,j}$ is the matrix whose jth column is the ith column of M. Thus, $M(1+aE_{i,j})$ is the result of adding the ith column of M, scaled by a, to the jth column of M. Now suppose we have some $M = (m_{i,j})_{i,j=1}^n \in U_n^{(k-1)}$. We will now construct some matrix $M' \in U_n^{(k)}$ s.t. M is M' times some product of the $(I_n + aE_{i,j})$.

Consider the sequence of matrices $A_1 = M'(I_n + m_{1,1+k}E_{1,1+k})$, $A_2 = A_1(I_n + m_{2,2+k}E_{2,2+k})$, $\ldots$, $A_{n-k} = A_{n-k-1}(I_n + m_{n-k,n}E_{n-k,n})$ (we'll set $A_0 = M'$ for ease of notation). For each $x \in \{0, \ldots, n-k-1\}$, A_x has $(A_x)_{i,i+k} = 0$ for $i \in \{x+1, \ldots, n-k\}$. Then when we multiply A_x by $(I_n + m_{x,x+k}E_{x,x+k})$, we get the xth column of A_x (which we know has a 1 in the xth row), scale it by $m_{x,x+k}$, and add it to the $(x+k)$th column of A_x (this process only impacts the $(x+k)$th column of A_x; all other columns don't change). That is to say, we have now guaranteed that $(A_{x+1})_{x,x+k} = m_{x,x+k}$.

Unfortunately, rows $1, \ldots, (x-1)$ of the $(x+k)$th column of A_{x+1} may no longer be rows $1, \ldots, (x-1)$ of the $(x+k)$th column of A_x, since we might have added some "mess" from the xth column of A_x. However, this is not a problem, since we can just set M' at the beginning to have $(x+k)$th column such that it becomes the $(x+k)$th column of M only after adding the "mess". In this way, we've written the arbitrary matrix $M \in U_n^{(k-1)}$ as a product of M' and some $(I_n + aE_{i,j})$, where $M' \in U_n^{(k)}$, and so the induction step is complete.

(b) We show that $\mathscr{T} = \{(I_n + aE_{i,i}) : 1 \leq i \leq n\}$ generates the group of diagonal matrices T_n. If we have a diagonal matrix D, with entries $d_{i,i}$, $i \in \{1, \ldots, n\}$, then as we said above in (a), $D(I_n + aE_{i,i})$ takes the ith column of D, scales it by a, and adds it to the ith column of D. This allows us to easily see that $D = (I_n + (d_{1,1}-1)E_{1,1})(I_n + (d_{2,2}-1)E_{2,2}) \cdots (I_n + (d_{n,n}-1)E_{n,2=n})$, and so we are done.

(c) We compute the product $(I_n + aE_{i,i})(I_n + bE_{j,\ell})(I_n + aE_{i,i})^{-1}$: first observe that $(I_n + aE_{i,i})^{-1} = (I_n + (-\frac{a}{a+1})E_{i,i})$. Then the product (we'll denote it B) becomes

$$\begin{aligned}
B &= (I_n + aE_{i,i} + bE_{j,\ell} + abE_{i,i}E_{j,\ell})(I_n + \tfrac{-a}{a+1}E_{i,i}) \\
&= I_n + aE_{i,i} + bE_{j,\ell} + abE_{i,i}E_{j,\ell} + \tfrac{-a}{a+1}E_{i,i} + a\tfrac{-a}{a+1}E_{i,i}E_{i,i} + b\tfrac{-a}{a+1}E_{j,\ell}E_{i,i} + \tfrac{-a}{a+1}abE_{i,i}E_{j,\ell}E_{i,i} \\
&= I_n + (a + \tfrac{-a}{a+1} + a\tfrac{-a}{a+1})E_{i,i} + bE_{j,\ell} + abE_{i,i}E_{j,\ell} + b\tfrac{-a}{a+1}E_{j,\ell}E_{i,i} + \tfrac{-a}{a+1}abE_{i,i}E_{j,\ell}E_{i,i} \\
&= I_n + bE_{j,\ell} + abE_{i,i}E_{j,\ell} + b\tfrac{-a}{a+1}E_{j,\ell}E_{i,i} + \tfrac{-a}{a+1}abE_{i,i}E_{j,\ell}E_{i,i}
\end{aligned}$$

where we used that $E_{i,i}^2 = E_{i,i}$. We now split into a couple cases:

- If $j, \ell = i$, then things simplify further to $B = I_n + (b + ab + b\frac{-a}{a+1} + \frac{-a}{a+1}ab)E_{i,i} = I_n + bE_{i,i}$ (because $E_{i,i}^2 = E_{i,i} \implies E_{i,i}^3 = E_{i,i}$).
- If $j = i$ but $\ell \neq i$, then $B = I_n + bE_{i,\ell} + abE_{i,\ell} + b\frac{-a}{a+1}E_{i,\ell}E_{i,i} + \frac{-a}{a+1}abE_{i,i}E_{i,\ell}E_{i,i}$, but $E_{i,\ell}E_{i,i} = \mathbf{0}$ because $\ell \neq i$, so we can further simplify: $B = I_n + (b + ab)E_{i,\ell}$
- If $\ell = i$ but $j \neq i$, then $B = I_n + bE_{j,i} + abE_{i,i}E_{j,i} + b\frac{-a}{a+1}E_{j,i}E_{i,i} + \frac{-a}{a+1}abE_{i,i}E_{j,i}E_{i,i}$, but $E_{i,i}E_{j,i} = \mathbf{0}$ because $j \neq i$, so we can further simplify: $B = I_n + (b + b\frac{-a}{a+1})E_{j,i} = I_n + \frac{b}{a+1}E_{j,i}$
- If both $j, \ell \neq i$, then $E_{j,\ell}E_{i,i} = \mathbf{0}$ and $E_{i,i}E_{j,\ell} = \mathbf{0}$, so all that's left is $B = I_n + bE_{j,\ell}$.

(d) We want to show that $[B_n, U_n] = U_n$. We can show that $[B_n, U_n] \subseteq U_n$ very easily if we have that $U_n \trianglelefteq B_n$, because then for any $B \in B_n, U \in U_n$, $(BUB^{-1})U^{-1} = U'U^{-1} \in U_n$ for some $U' \in U_n$. It is indeed true that $U_n \trianglelefteq B_n$, because U_n is the kernel of the homomorphism taking B_n to its diagonal (it is a homomorphism because for upper triangular matrices, $(B_1B_2)_{i,i} = (B_1)_{i,i}(B_2)_{i,i}$.

Now for $[B_n, U_n] \supseteq U_n$. From (c), we know that for any $1 \leq i < \ell \leq n$, $(I_n + aE_{i,i})(I_n + bE_{i,\ell})(I_n + aE_{i,i})^{-1} = I_n + (b+ab)E_{i,\ell}$. It is also easy to see that $(I_n + bE_{i,\ell})^{-1} = (I_n + (-b)E_{i,\ell})$ (indeed $(I_n + bE_{i,\ell})(I_n + (-b)E_{i,\ell}) = I_n + bE_{i\ell} - bE_{i,\ell} - b^2E_{i,\ell}E_{i,\ell} = I_n = (I_n + (-b)E_{i,\ell})(I_n + bE_{i,\ell})$), so

$$\begin{aligned}(I_n + aE_{i,i})(I_n + bE_{i,\ell})(I_n + aE_{i,i})^{-1}(I_n + bE_{i,\ell})^{-1} &= (I_n + (b + ab)E_{i,\ell})(I_n + (-b)E_{i,\ell}) \\ &= I_n + abE_{i,\ell}\end{aligned}$$

Note that $(I_n + aE_{i,i}) \in B_n$ and $(I_n + bE_{i,\ell}) \in U_n$, and so (by taking $b = 1$) we've just shown that $\mathscr{S} := \{(I_n + aE_{i,\ell}) : a \in F, 1 \leq i < \ell \leq n\} \subseteq [B_n, U_n]$. From (a), we know that $\mathscr{S}$ generates U_n, and so it must be that $U_n \subseteq [B_n, U_n]$, as desired.

(e) B_n therefore can not be nilpotent, because the elements of its lower central series $B_n, [B_n, B_n] \supseteq [B_n, U_n] = U_n, [B_n, [B_n, B_n]] \supseteq [B_n, U_n] = U_n, \ldots$ always remain $\supseteq U_n$, and hence can never terminate.

Problem 4

Let G be a group generated by two elements, and such that any element in G has order 1 or 3. We want to show that (a), $|G| \leq 27$, and (b), that this bound can not be improved.

Part 1: $|G| \leq 27$. Because we know that all elements are either order 1 or 3, we definitely have that $a^3, b^3, (ab)^3, (ab^2)^3, (a^2b)^3, (a^2b^2)^3$ are all 1. a^3, b^3 being 1 in particular implies that $a^{-1} = a^2, b^{-1} = b^2$. To bound the order of G, we need to somehow show that all words can be reduced to a small set of words (say for example the set of all words of length 3 or less, where the words of length 3 are described by $a^{1,2}b^{1,2}a^{1,2}$ or $b^{1,2}a^{1,2}b^{1,2}$).
We can show that all words can be reduced to words of length 3 or less if we show that all words of length 4 can be reduced to length 3 (or less); this suffices because given any word of length longer than 3, we can take a length-4 chunk and reduce it to length 3 (or less), thus shaving down the length

by one (at least). Let us now try to reduce the 16 words of the form $a^{1,2}b^{1,2}a^{1,2}b^{1,2}$ (the cases where b is at the beginning are symmetric):

- $abab = b^2a^2$
- $ab^2ab^2 = ba^2$
- $a^2ba^2b = b^2a$
- $a^2b^2a^2b^2 = ba$
- $abab^2 = (b^2a^2)b$
- $ab^2ab = (ba^2)b^2$
- $a^2ba^2b^2 = (b^2a)b$
- $a^2b^2a^2b = (ba)b^2$
- $a^2bab = a(b^2a^2)$
- $a^2b^2ab^2 = a(ba^2)$
- $aba^2b = a^2(b^2a)$
- $ab^2a^2b^2 = a^2(ba)$

Unfortunately, the last four cases, $A = a^2bab^2$, $B = a^2b^2ab$, $C = aba^2b^2$, $D = ab^2a^2b$ don't seem to simplify. It should be noted though that $A = a(abab)b = D$ and $B = a(ab^2ab^2)b^2 = C$. This breaks our original strategy, though no worries: we can bump up to reducing length-5 words to length 4 or less (and this does end up working). We'll look at length-5 words of the form $b^{1,2}a^{1,2}b^{1,2}a^{1,2}b^{1,2}$ (the cases where a is at the beginning are symmetric like before). If the last length-4 chunk is one of the 12 reducible length-4 words, then obviously that length-5 word can be reduced to length 4 or less. Thus, it remains to tackle the 4 cases $b^{1,2}A$ and $b^{1,2}B$:

- $bA = (ba^2ba)b^2 = ((ab^2)a^2)b^2 = a^2ba$
- $b^2B = (b^2a^2b^2a)b = ((ab)a^2)b = a^2b^2a$
- $b^2A = b(bA) = b(a^2ba) = ab^2a^2$
- $bB = b^2(b^2B) = b^2(a^2b^2a) = aba^2$

Thus we have that all words can be reduced to length 4 or less, and most length-4 words can be reduced to length 3 or less. Thus, we can bound the number of length-1,2,3,4 words that start with a by $2^1 + 2^2 + 2^3 + 2 = 16$ (2^1 choices for $a^{1,2}$, 2^2 choices for $a^{1,2}b^{1,2}$, 2^3 choices for $a^{1,2}b^{1,2}a^{1,2}$, and only 2 choices for length-4 words beginning with a: A and B). By symmetry, we have another 16 for length-1,2,3,4 words that start with b, and 1 more word for the empty word (length-0), and so we have that $|G|$ must be $\leq 16 + 16 + 1 = 33$.
Finally, because $|G|$ must be a pure power of 3, because otherwise, we would have by Cauchy's theorem that there would be some element with order $p \neq 3$, which contradicts the assumption. Thus, we have our bound $|G| \leq 27$.

Part 2: there is a group, generated by 2 elements with all elements having order 1 or 3, with order 27. Consider $U_3(\mathbb{F}_3)$ (the group of 3×3 upper triangular matrices over $\mathbb{F}_3$ with 1's on the diagonal), which does in fact have $3^{1+2} = 3^3 = 27$ elements (see Homework 3 Problem 4(b)). First, a quick calculation yields that indeed all elements have order 1 or 3:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 3a & 3(ac+b) \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}.$$

Furthermore, we can verify by induction that

$$M^x := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^x = \begin{bmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad N^y := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix},$$

and so we have that

$$M^x N^y M^z N^y = \begin{bmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & z & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+z & y(x+z)+xy \\ 0 & 1 & 2y \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus we can set $y = 2^{-1}c = 2c$, $x = (b - ya)y^{-1}$, and $z = a - x$ to get the arbitrary matrix

$$M^x N^y M^z N^y = \begin{bmatrix} 1 & x+z & y(x+z)+xy \\ 0 & 1 & 2y \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & ya + \big((b-ya)y^{-1}\big)y \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

in $U_3(\mathbb{F}_3)$. Thus, we now know that $U_3(\mathbb{F}_3)$ is generated by 2 elements M, N, has all elements order 1 or 3, and has order 27, so we are done.

Problem 5

Consider the group G with presentation $\langle a, b, c \mid a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}ac = a^2 \rangle$. We want to show that G is trivial.

First, notice that all the relations can be rephrased into statements about commutators: $[a^{-1}, b] = a^{-1}bab^{-1} = b$, $[b^{-1}, c] = b^{-1}cbc^{-1} = c$, and $[c^{-1}, a] = c^{-1}aca^{-1} = a$. This means that the commutator subgroup $[G, G]$ is exactly G (i.e. G is perfect), since $[G, G]$ contains a, b, c which we know generate G. With this in mind, we now have a lead on proving that G is trivial: if we can show that G is solvable, then G must be trivial because only the trivial group can be both solvable and perfect.

It is relatively easy to see that $\langle a, b \rangle$ is solvable. We first establish that $\langle b \rangle \trianglelefteq \langle a, b \rangle$: we know that $b^{-1}b^k b = b^k \in \langle b \rangle$ and $a^{-1}b^k a = (a^{-1}ba)^k = b^{2k} \in \langle b \rangle$, and for any arbitrary element in $\langle a, b \rangle$, we can apply these two rules again and again to reduce down to some element of $\langle b \rangle$. We now show that $\langle a, b \rangle / \langle b \rangle \simeq \langle a \rangle$, which is abelian, thus proving that $\langle a, b \rangle$ is solvable: we know that $b\langle b \rangle = \langle b \rangle$, $a^k\langle b \rangle = a^k\langle b \rangle$, and $ba^k\langle b \rangle = (ba)a^{k-1}\langle b \rangle = (ab^2)a^{k-2}\langle b \rangle = a(b^2a)a^{k-2}\langle b \rangle = a(ab^{2\cdot 2})a^{k-2}\langle b \rangle = \ldots = a^k b^{2^k} a^{k-k}\langle b \rangle = a^k\langle b \rangle$; then any element $\langle a, b \rangle$ in front of $\langle b \rangle$ can be reduced to some $a^k\langle b \rangle$ ($k \in \mathbb{Z}$) by just using these three rules over and over.

The final piece of the puzzle lies in noticing that $c \in \langle a, b \rangle$: some manipulation yields

$$\begin{aligned} c^4 &= b^{-1}c^2b = b^{-1}(b^{-1}cb)b = b^{-2}cb^2 = (a^{-1}b^{-1}a)c(a^{-1}ba) = a^{-1}b^{-1}(aca^{-1})ba \\ &= a^{-1}b^{-1}(ca)ba = a^{-1}(b^{-1}c)aba = a^{-1}(c^2b^{-1})aba = (a^{-1}c^2)b^{-1}aba \\ &= c^2(c^{-2}a^{-1}c^2)b^{-1}aba = c^2(c^{-2}a^{-1}c^2)b^{-1}aba = c^2(c^{-2}ac^2)^{-1}b^{-1}aba = c^2a^{-4}b^{-1}aba \end{aligned}$$

implying that $c^2 = a^{-4}b^{-1}aba \implies b^{-1}cb = a^{-4}b^{-1}aba \implies c = ba^{-4}b^{-1}abab^{-1} \implies c \in \langle a, b \rangle$. This proves that $G = \langle a, b \rangle$, and since we just proved that $\langle a, b \rangle$ is solvable, G is too. As stated before, this shows that G must be trivial.

504 Homework 3

Daniel Rui - 10/27/20

Problem 3

Sylow subgroups of symmetric groups:

(a) We want to find the order of a Sylow 2-subgroup of S_{2^n}. Recall that a Sylow p-subgroup of a group G with order $p^n m$ where $\gcd(m, p) = 1$ is just any subgroup of G with order p^n. In other words, this problem is asking us to find the number of 2's in the factorization of $(2^n)!$. Well, there is one 2^n, two 2^{n-1}'s, four 2^{n-2}'s, and so on until 2^{n-1} many 2's. Adding this all up, we have a total of $1 + 2 + 4 + \ldots + 2^{n-1} = 2^n - 1$ many 2's, and so the order of a Sylow 2-subgroup of S_{2^n} is 2^{2^n-1}.

(b) We are asked to give an explicit description of one of these Sylow 2-subgroups, i.e. we need to give a description of a subgroup of S_{2^n} that has order 2^{2^n-1}. We take inspiration from the decomposition above: $2^{2^n-1} = 2^1 \cdot 2^2 \cdot 2^4 \cdots 2^{2^{n-1}}$ — if we had some sort of subset of $\{1, \ldots, 2^n\}$ that we could break down into around $n - 1$ levels, where at the first level there were 2 options, and at the second level there were 2 sets of 2 options, and at the 3rd level there were 4 sets of 2 options, and so on, a Sylow 2-subgroup could potentially be the subgroup consisting of all these arrangements.

The doubling of the sets of options at each level, and the fact that there are only 2 options brings to mind the picture of a binary tree (let's picture it growing left to right): if we have a binary tree with $2^n - 1$ nodes and levels $\{0, 1, \ldots, n - 1\}$ (i.e. 2^i nodes on level i), then at level 1 you have 2 arrangements (if we label the two nodes on level 1 "N2" and "N3", then the two arrangements are N2 above N3, or N3 above N2). Keep in mind that by rearrangements I just mean a "representation" of the binary tree; the tree itself does not change when we put N2 above N3 or vice versa (to be clear, all the descendants of the nodes move with them).

In general, if you have a node on level i (where $i \in \{0, \ldots, n - 2\}$), then its two children on level $i + 1$ can be arranged in two ways, and because there are a total of 2^i nodes on level i, the total number of arrangements of the nodes on level $i + 1$ are $2^i \cdot 2 = 2^{i+1}$.

Thus in fact the number of arrangements of this binary tree is $2^{0+1} \cdot 2^{1+1} \cdot 2^{2+1} \cdots 2^{(n-2)+1} = 2^{2^n-1}$. To make its group structure obvious, fix an arrangement of the binary tree to be the "standard representation", and for each of the 2^{2^n-1} arrangements consider instead the function ("the set of swaps one needs to do") going from the "standard representation" to the arrangement in question. In other words, the Sylow 2-subgroup we are currently describing is the automorphism group of a binary tree with $2^n - 1$ nodes (which is obviously a subgroup of S_{2^n}, the automorphism group of the set of 2^n elements).

Problem 4

Let $\mathbb{F}_p$ (which we can think of as $\{0, 1, \ldots, p-1\}$ with addition and multiplication mod p) be a finite field of p elements (p prime). Due to the operations and structure available in a field, we can construct matrices over $\mathbb{F}_p$ analogously to how we do it over $\mathbb{R}$, and preserve some properties we know from $\mathbb{R}$ such as "linearly independent columns" $\iff$ "determinant $\neq 0$" $\iff$ "invertible".

(a) We want to find the order of the finite group $\mathrm{GL}_n(\mathbb{F}_p)$ (i.e. the set of invertible $n \times n$ matrices over $\mathbb{F}_p$). As stated in the introduction above, we can answer this by finding the number of $n \times n$ matrices over $\mathbb{F}_p$ s.t. their columns are linearly independent.

The first column c_1 can be literally anything, EXCEPT a column of zeroes; thus we have $p^n - 1$ choices for the first column.

The second column c_2 can be anything as long as it is not some scalar multiple of the 1st column (note that this condition already ensures that c_2 is not the zero vector), where there are p such multiples (no two multiples can coincide, because if $ic_1 = jc_1 \implies (j-i)c_1 = 0$, and c_1 is not the zero vector, then $(j-i)$ must be 0 because $\mathbb{F}_p$ is a field and hence integral domain); thus there are $p^n - p$ choices for c_2.

The third column c_3 can be anything as long as it is not some linear combination of c_1 and c_2, where there are p^2 such linear combinations (no two linear combinations can coincide, because $i_1c_1 + i_2c_2 = j_1c_1 + j_2c_2 \implies (j_1 - i_1)c_1 + (j_2 - i_2)c_2 = 0$, and because we already ensured that c_1, c_2 were linearly independent this forces $i_1 = j_1, i_2 = j_2$; note that this argument can be extended to linear combinations of more than just two vectors); thus there are $p^n - p^2$ choices for c_3.

Continuing this argument, we see that there are $p^n - p^{i-1}$ choices for column c_i, for $i \in \{1, \ldots, n\}$, and so in total we have $\prod_{i=1}^{n}(p^n - p^{i-1})$ choices for an $n \times n$ linearly independent matrix, and so

$$\begin{aligned} |\,\mathrm{GL}_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}) \\ &= p^0(p^n - 1)\cdot p^1(p^{n-1} - 1)\cdots p^{n-1}(p-1) = p^{0+1+2+\ldots+(n-1)}\prod_{i=1}^{n}(p^i - 1) \end{aligned}$$

(b) Because $|\,\mathrm{GL}_n(\mathbb{F}_p)| = p^{n(n-1)/2}\prod_{i=1}^{n}(p^i - 1)$, and obviously all of the $(p^i - 1)$ are not divisible by p, the order of a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ is $p^{n(n-1)/2}$. Now consider the subgroup $U_n(\mathbb{F}_p)$ of upper triangular matrices with 1's along the main diagonal (subgroup because identity matrix is obvious an element, associativity is inherited, and it's fairly easy to see that products are also of this form, and by the Gauss-Jordan method it's also fairly easy to see that inverses are of this form).

No matter how you fill in the strictly upper triangular part you will end up with a matrix with linearly independent columns, because c_i can not possibly be written as a linear combination of $c_1, \ldots, c_{i-1}$ because all of those have 0's in the ith row, whereas c_i has a 1 in the ith row. Thus, there are a total of $p^0 \cdot p^1 \cdot p^2 \cdots p^{n-1} = p^{n(n-1)/2}$ such matrices. Thus, $U_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

For a different Sylow p-subgroup, one can take the subgroup of lower triangular matrices with 1's on the main diagonal instead, a situation completely analogous to the $U_n(\mathbb{F}_p)$ situation we just talked about.

(c) Let A, B be two commuting matrices in $\mathrm{GL}_n(\mathbb{F}_p)$ of order p (i.e. p is the minimum natural number s.t. $A^p = B^p = \mathrm{Id}_n$). We want to show that there is a matrix $S \in \mathrm{GL}_n(\mathbb{F}_p)$ s.t. SAS^{-1} and SBS^{-1} are in $U_n(\mathbb{F}_p)$, i.e. there is some matrix $S \in \mathrm{GL}_n(\mathbb{F}_p)$ s.t. $A, B \in SU_n(\mathbb{F}_p)S^{-1}$. The second Sylow theorem tells us that any p-subgroup H is a subgroup of some Sylow p-subgroup, where all Sylow p-subgroups are conjugate, and so we can prove that A, B are in some conjugate of $U_n(\mathbb{F}_p)$ by proving that A, B are in some p-subgroup.

In fact, we will prove that $\langle A, B\rangle$ (the subgroup of all products of A's and B's) is a p-subgroup. Because A, B commute, we only need to consider products of the form A^iB^j, and because A, B have order p we only need to consider $i, j \in \{0, \dots, p-1\}$. That is to say, $\langle A, B\rangle = \{A^iB^j : i, j \in \{0, \dots, p-1\}\}$. It is now clear that

$$\begin{aligned}\langle A, B\rangle &= \{A^iB^j : i, j \in \{0, \dots, p-1\}\} \\ &= \{A^i : i \in \{0, \dots, p-1\}\}\{B^j : j \in \{0, \dots, p-1\}\} = \langle A\rangle\langle B\rangle.\end{aligned}$$

Proposition 3.13 in Dummit & Foote gives that for subgroups $H, K \leq G$, $|HK| = \frac{|H||K|}{|H\cap K|}$, or in particular $|HK|$ divides $|H||K|$. Applying this to $\langle A, B\rangle = \langle A\rangle\langle B\rangle$, we have that $|\langle A, B\rangle|$ divides $|\langle A\rangle||\langle B\rangle| = p \cdot p = p^2$. Because p is prime, $|\langle A, B\rangle|$ must either be p or p^2 (can't be 1 because $\langle A, B\rangle$ contains $\langle A\rangle$, which has size p), and either way, $\langle A, B\rangle$ is a p-subgroup.

Thus, as stated in the end of paragraph 1, we have a p-subgroup $\langle A, B\rangle$ that contains A, B, and so by the second Sylow theorem, A, B are elements are elements in some conjugate of $U_n(\mathbb{F}_p)$, i.e. there is some $S^{-1} \in \mathrm{GL}_n(\mathbb{F}_p)$ s.t. $A, B \in S^{-1}U_n(\mathbb{F}_p)(S^{-1})^{-1} \implies SAS^{-1}, SBS^{-1} \in U_n(\mathbb{F}_p)$.

(d) We show that (c) is not necessarily true if A, B do not commute: consider $\mathrm{GL}_2(\mathbb{F}_2)$; from (a) we know that there are $(2^2-1)(2^2-2) = 6$ such matrices, which we list here:

$$\begin{bmatrix}1&0\\0&1\end{bmatrix}, \quad \begin{bmatrix}1&1\\0&1\end{bmatrix}, \quad \begin{bmatrix}0&1\\1&1\end{bmatrix}, \quad \begin{bmatrix}1&0\\1&1\end{bmatrix}, \quad \begin{bmatrix}1&1\\1&0\end{bmatrix}, \quad \begin{bmatrix}0&1\\1&0\end{bmatrix}.$$

Of these 6, only 3 have order 2:

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}, \quad \begin{bmatrix}1&0\\1&1\end{bmatrix}, \quad \begin{bmatrix}0&1\\1&0\end{bmatrix}$$

Because we want to show that for all six $S \in \mathrm{GL}_2(\mathbb{F}_2)$, at least one of SAS^{-1} and SBS^{-1} is not upper triangular, it might make things easier if we try the two of the three above that aren't upper triangular. First we check if they do not commute:

$$AB := \begin{bmatrix}1&0\\1&1\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix} = \begin{bmatrix}0&1\\1&1\end{bmatrix} \neq \begin{bmatrix}1&1\\1&0\end{bmatrix} = \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix} =: BA.$$

Now we go through all 6 choices for S: if S is the identity matrix, obviously $SAS^{-1} = A$ is not

upper triangular; if $S = A$, then $SAS^{-1} = AAA^{-1} = A$ is not upper triangular; if $S = B$, then $SBS^{-1} = BBB^{-1} = B$ is not upper triangular. Now for the last three possibilities (note that because all of these have order 2, they are their own inverse):

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} A \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} B \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{-1} = \left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} A \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right) \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

which are all not upper triangular. Thus, we have in fact found $A, B \in \mathrm{GL}_2(\mathbb{F}_2)$ with order 2 and that DO NOT commute s.t. for all $S \in \mathrm{GL}_2(\mathbb{F}_2)$, at least one of SAS^{-1}, SBS^{-1} are not upper triangular, and so this is a counterexample to the claim from (c) in the case that A, B do not commute.

504 Homework 2

Daniel Rui - 10/20/20

Problem 1

We want to show that $\binom{p^a m}{p^a}$ is not divisible by p when $\gcd(m,p)=1$ and a is a positive integer. We do this by showing the number of p's in the numerator and denominator is equal:

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

by proving the following lemma: $p^b \mid p^a - k \iff p^b \mid p^a m - k$ where $b \in \mathbb{N}$ and $k \in \{0, \ldots, p^a - 1\}$. This would show the result because it would show that each little fraction $\frac{p^a m - k}{p^a - k}$ in the large fraction has the same number of p's in the numerator and denominator, implying that the whole large fraction (the product of the little fractions) has that exact property.

($\implies$) Because $p^a - k > 0$, the divisibility condition implies that $p^b \leq p^a - k \leq p^a$, i.e. $b \leq a \implies p^{a-b} \in \mathbb{N}$. This makes things very easy for us, because the divisibility condition gives that $p^b x = p^a - k \iff k = p^b(p^{a-b} - x)$ for some $x \in \mathbb{Z}$, and so $p^a m - k = p^a m - p^b(p^{a-b} - x) = p^b(p^{a-b} m - p^{a-b} + x)$, where $(p^{a-b} m - p^{a-b} + x)$ is an integer because p^{a-b}, m, and x are all integers. In other words, we've shown that $p^a m - k$ is an integer multiple of p^b, and so $p^b \mid p^a m - k$.

($\impliedby$) If we are instead starting with $p^b \mid p^a m - k \iff p^b y = p^a m - k$ for some $y \in \mathbb{Z}$, then it is not immediately obvious that b must be $\leq a$. If $b \leq a$ is in fact the case, then the claim follows similar to the above ($\implies$) case, where we can write $p^a - k = p^b(p^{a-b} - p^{a-b} m + y)$ for integers p^{a-b}, m, and y. Now we consider what happens if $b > a$: we could divide by p^a in the first equality to get that $p^{b-a} y = m - \frac{k}{p^a}$. Well we know that $p^{b-a} y$ is an integer multiple of p (because $b > a$), while $m \in \mathbb{Z}$ is not divisible by p, and where $\frac{k}{p^a} \in [0, 1)$; thus if $\frac{k}{p^a} \neq 0$ the equality can not hold because the right side is not an integer, but if $\frac{k}{p^a} = 0$ the equality can not hold either because the LHS is a multiple of p whereas the RHS is not. That is to say, the case $b > a$ is impossible, and so the claim is proven.

Problem 2

Given a subgroup H in G, we want to show that the normalizer $N_G(H) = \{g \in G : gH = Hg\}$ is the (a?) maximal subgroup of G in which H is normal. Firstly, it is a subgroup of G:

- associativity is inherited from G
- closure is given because if $g_1, g_2 \in N_G(H)$, we have that $(g_1 g_2)H = g_1(g_2 H) = g_1(Hg_2) = (g_1 H)g_2 = H(g_1 g_2) \implies (g_1 g_2) \in N_G(H)$
- the identity e_G is obviously an element because $e_G H = H = H e_G$
- and finally the inverses are elements because if $g \in N_G(H)$, then $g^{-1} H g = g^{-1}(Hg) = g^{-1}(gH) = (g^{-1} g)H = H \iff g^{-1} H = H g^{-1}$

As for the assertions regarding normality and maximality, H is normal in $N_G(H)$ because by definition, all $g \in N_G(H)$ are s.t. $gH = Hg$; and there is no subgroup strictly containing $N_G(H)$ that H is still normal in because if there was, then there would be some g in that subgroup but not in $N_G(H)$ satisfying the condition for normality ($gH = Hg$), which would mean that g was in $N_G(H)$ all along, contradiction.

Problem 3

We want to prove that if H is a subgroup of G of index 2, then H is normal in G. The index is just the number of left (or right) cosets, where we know that cosets partition the group and are the same size ($= |H|$). Let g_1H and g_2H be the representatives of the set of left cosets $\{gH : g \in G\}$ (which we know has 2 elements), i.e. for all $g \in G$, gH is either $= g_1H$ or $= g_2H$; similarly denote Hg_1' and Hg_2' to be the representatives of the set of right cosets.

Well for all $h \in H$, we know that $hH = H = Hh$, so H must be one of the left (or right) cosets, and so without loss of generality let $g_1H = H = Hg_1'$. By the fact that g_1H, g_2H (similarly Hg_1', Hg_2') is a partition of G, it must then be that $g_2H = H^{\complement} = Hg_2'$ ($H^{\complement}$ is H complement, i.e. all the elements in G not in H). Furthermore, it is EXACTLY the elements $g \in H$ that have $gH = H = Hg$, because $gH = H \implies g \in H$ (and similarly $Hg = H \implies g \in H$), and we already established $g \in H \implies gH = H$. That is to say, if $g \in H$, then $gH = g_1H = H = Hg_1' = Hg$, and if $g \notin H$, then

$$gH \neq H \implies gH \neq g_1H \implies gH = g_2H \quad \text{and} \quad Hg \neq H \implies Hg \neq Hg_1' \implies Hg = Hg_2',$$

so $gH = g_2H = H^{\complement} = Hg_2' = Hg$. We see that in both cases ($g \in H$ and $g \notin H$), $gH = Hg$, which means that H is normal in G.

Problem 4

Let G be a finite group and let H be a normal subgroup of G with $\gcd(|H|, [G : H]) = 1$. We want to show that H is the only subgroup of G of order $|H|$. Suppose not; then there is a subgroup $H' \neq H$ s.t. $|H'| = |H|$. The second isomorphism theorem tells us that the quotient groups $(H'H)/H$ and $H/(H' \cap H)$ are isomorphic, and so in particular, $[H'H : H] = [H : H' \cap H] = \frac{|H|}{|H' \cap H|}$ (recall that all subgroups must contain the identity and therefore have size ≥ 1). Furthermore, because $H \leq H'H \leq G$, we have that $[G : H] = [G : H'H][H'H : H]$. Putting these two equalities together, we have that

$$|H|[G : H'H] = [G : H]|H' \cap H|$$

(where again each term in the formula is an integer ≥ 1). But because $H' \neq H$, and yet has $|H'| = |H|$, it must be that $|H' \cap H|$ is strictly less than $|H|$. This means that H can not divide $|H' \cap H|$, which means that some factor of $|H|$ (other than 1 of course) must also be a factor of $[G : H]$, which contradicts the assumption that $\gcd(|H|, [G : H]) = 1$.

Problem 5

Consider the standard action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$, that is the action of an $n \times n$ real invertible matrix on a vector in $\mathbb{R}^n$. The orbits are just the zero vector $\mathbf{0}$ and $\mathbb{R}^n \setminus \mathbf{0}$ — the orbit of the zero vector is the zero vector because any matrix maps $\mathbf{0}$ to $\mathbf{0}$; and the orbit of any non-zero vector is $\mathbb{R}^n \setminus \mathbf{0}$, a fact that we will prove by showing that given any non-zero $v, w \in \mathbb{R}^n \setminus \mathbf{0}$, there is some matrix $\in \mathrm{GL}_n(\mathbb{R})$ that takes v to w (obviously there is no invertible matrix that can take a non-zero vector to the zero vector because then the transformation would not be injective given that $\mathbf{0}$ always maps to $\mathbf{0}$).

First we prove that for any non-zero vector $v \in \mathbb{R}^n$, there is always a matrix $\in \mathrm{GL}_n(\mathbb{R})$ that takes $e_1 := \langle 1, 0, \ldots, 0 \rangle$ (the basis vector along the first coordinate in $\mathbb{R}^n$) to v: simply let the first column of the matrix be v, and take the rest to be linearly independent of v and each other (which recall is $\iff$ the matrix is invertible). An explicit example is as follows: because we know v is non-zero, there must be some non-zero entry at say the ith entry of the vector; now take the other $n-1$ columns to be $e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n$ (it is fairly obvious that this will guarantee linear independence). Ok back to v and w: we just showed that there's some $M_1, M_2 \in \mathrm{GL}_n(\mathbb{R})$ s.t. $M_1 e_1 = v$ and $M_2 e_1 = w$. Then we get that $e_1 = M_1^{-1} v \implies M_2(M_1^{-1} v) = (M_2 M_1^{-1})v = w$, where $M_2 M_1^{-1} \in \mathrm{GL}_n(\mathbb{R})$ because $M_1, M_2 \in \mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{R})$ is a group.

Now for the stabilizers — let us first find the stabilizers of e_1. If a matrix sends e_1 to e_1, then its first column must be exactly e_1 (the 0's in positions 2 through n in e_1 make the 2nd to nth columns of the matrix irrelevant, and so the output is exactly 1 times the first column of the matrix, and so the output being e_1 forces the 1st column to be e_1). The other $n-1$ columns can be anything as long as the columns remain linearly independent (or equivalently the determinant $\neq 0$, or any of the many other equivalent conditions) to ensure the matrix is invertible. Call this set of matrices $\mathscr{S}_{e_1}$ (the stabilizer of e_1).

As for the stabilizer of any other vector $v \in \mathbb{R}^n$: if it's $\mathbf{0}$, then all matrices in $\mathrm{GL}_n(\mathbb{R})$ fix $\mathbf{0}$; and if it's non-zero, then the stabilizer is a conjugate of S_{e_1}. We will show this by showing that given any non-zero $v, w \in \mathbb{R}^n$, the stabilizer of w (denoted $\mathscr{S}_w$) is a equal to some conjugate of $\mathscr{S}_v$. We know from above (paragraph 2) that there is some $M \in \mathrm{GL}_n(\mathbb{R})$ s.t. $Mv = w$. Now suppose we have some arbitrary $T \in \mathrm{GL}_n(\mathbb{R})$ s.t. $Tw = w$ (i.e. T is in the stabilizer of w). Then we have that $TMv = Mv \implies (M^{-1}TM)v = v$, or in other words, that there is some $S \in \mathscr{S}_v$ s.t.

$$(M^{-1}TM) = S \implies T = MSM^{-1} \implies T \in M\mathscr{S}_v M^{-1},$$

which by the fact that T is arbitrary would mean that $\mathscr{S}_w \subseteq M\mathscr{S}_v M^{-1}$. Swapping the places of v and w (so now the "M" in question is actually M^{-1} which takes w to v), we get that $\mathscr{S}_v \subseteq M^{-1}\mathscr{S}_w(M^{-1})^{-1} = M^{-1}\mathscr{S}_w M$. The two inequalities yield the desired result. Thus all stabilizers of non-zero vectors $\in \mathbb{R}^n$ are just conjugates of $\mathscr{S}_{e_1}$, which we have already described in detail.

504 Homework 1

Daniel Rui - 10/13/20

Problem 1

By definition, every group G has a (two-sided) identity e, and an (two-sided) inverse g^{-1} for every $g \in G$. These must be unique, because if we are given an element e' that is also a(two-sided) identity, we get that $e = e \cdot e' = e'$ (where the first equality follows because e' is an identity, and where the second equality follows because e is an identity); similarly if we are given an element $(g^{-1})'$ that is also a (two-sided) inverse of g, we get that $g^{-1} = g^{-1} \cdot e = g^{-1} \cdot (g \cdot (g^{-1})') = (g^{-1} \cdot g) \cdot (g^{-1})' = e \cdot (g^{-1})' = (g^{-1})'$.

Problem 2

Given some set X with some fixed element e, equipped with two binary operations $*$ and $\circ$ such that e is the identity for both operations and $(a \circ b) * (c \circ d) = (a * c) \circ (b * d)$, we want to show that the operations are the same, and moreover are associative and commutative:

- ($\circ = *$): letting a, d be arbitrary elements of X, and setting b, c to e, the identity yields $a * d = (a \circ e) * (e \circ d) = (a * e) \circ (e * d) = a \circ d$.
- (assoc): letting a, b, d be arbitrary elements of X, and setting $c = e$, the identity yields $(a \circ b) * d = a \circ (b * d)$, which is associativity of both operations because they are the same.
- (comm): letting b, c be arbitrary elements of X, and setting a, d to e, the identity yields $b * c = c \circ b$, which is commutativity of both operations because they are the same.

Problem 3

We want to show that all finitely generated (non-trivial) subgroups of $\mathbb{Q}$ are cyclic and isomorphic to $\mathbb{Z}$. Suppose we are given some subgroup H of $\mathbb{Q}$ generated by $\{r_1, \ldots, r_n\} := \{\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}\}$; i.e. all elements of H can be written as some linear combination of the r_i. Let q be the smallest natural number s.t. all the $r_i q$ are integers; such a q must exist because a non-empty set of natural numbers has a least element (non-empty because $q_1 \cdots q_n$ is in it). By the same principle, we can let p to be the smallest element in the set $S := \{a_1 r_1 q + \ldots + a_n r_n q \in \mathbb{N} : a_i \in \mathbb{Z}\}$. Then I claim that $H = \langle \frac{p}{q} \rangle$.

- ($H \subseteq \langle \frac{p}{q} \rangle$): we want to show that any linear combination of the r_i can be written as some multiple of $\frac{p}{q}$. First, we show that $S = p\mathbb{N}$. Obviously, $S \supseteq p\mathbb{N}$ because we can just double all the a_i corresponding to p to get $2p$, and so on. For the other direction, let's say that it's some natural number not in $p\mathbb{N}$, and hence not $\equiv 0 \mod p$. Then, we could just subtract p (i.e. subtract the a_i corresponding to p) over and over until we end up with a number in $\{1, \ldots, p-1\}$ (i.e. we perform the division algorithm until we get to the remainder). But we said that p was the minimum number of S, and so it is impossible that one of the numbers $\{1, \ldots, p-1\}$ was in S; contradiction. Alright, with that in place, we see that any linear combination $a_1 r_1 + \ldots + a_n r_n$, multiplied by q, is in $p\mathbb{N}$, i.e. equal to some cp for $c \in \mathbb{Z}$. That is, we've proved that $a_1 r_1 + \ldots + a_1 r_n = c\frac{p}{q}$.

- $(H \supseteq \langle \frac{p}{q} \rangle)$: we just need to prove that $\frac{p}{q} \in H$; i.e. $\frac{p}{q} = a_1 r_1 + \ldots + a_n r_n$ (because all multiples $c\frac{p}{q} = ca_1 r_1 + \ldots ca_n r_n$). This is obvious because p is an element of $S = \{a_1 r_1 q + \ldots + a_n r_n q \in \mathbb{N} : a_i \in \mathbb{Z}\}$.

Note: it turned out that q didn't have to be the minimum; in fact the proof still works as long as $r_i q$ is an integer for all the r_i. Ok, now that we've proved that all finitely generated subgroups of $\mathbb{Q}$ are generated by one element (i.e. they are cyclic), it is immediate that they are isomorphic to $\mathbb{Z}$ (we did discuss this in class, but just take the isomorphism $\mathbb{Z} \to H$ defined by $c \mapsto c\frac{p}{q}$, which satisfies $c + c' \mapsto (c + c')\frac{p}{q} = c\frac{p}{q} + c'\frac{p}{q}$, and which has inverse $H \to \mathbb{Z}$ defined by $c\frac{p}{q} \mapsto c$).

Problem 4

Let $C := \mathbb{R} \times \mathbb{R}^3$, and define a product on C by

$$(a, u)(b, v) = (ab - u \cdot v, av + bu + u \times v)$$

and a norm on C by $N((a, u)) = a^2 + |u|^2$.

(a) The product above is associative:

$$\begin{aligned}
\Big((a,u)(b,v)\Big)(c,w) &= (ab - u\cdot v, av + bu + u\times v)(c,w) \\
&= \Big((ab - u\cdot v)c - (av + bu + u\times v)\cdot w, \\
&\qquad (ab - u\cdot v)w + c(av + bu + u\times v) + (av + bu + u\times v)\times w\Big) \\
&= \Big(abc - c(u\cdot v) - a(v\cdot w) - b(u\cdot w) - (u\times v)\cdot w, \\
&\qquad (ab)w - (u\cdot v)w + (ac)v + (bc)u + c(u\times v) + a(v\times w) + b(u\times w) + (u\times v)\times w\Big)
\end{aligned}$$

and

$$\begin{aligned}
(a,u)\Big((b,v)(c,w)\Big) &= (a,u)(bc - v\cdot w, bw + cv + v\times w) \\
&= \Big(a(bc - v\cdot w) - u\cdot(bw + cv + v\times w), \\
&\qquad a(bw + cv + v\times w) + (bc - v\cdot w)u + u\times(bw + cv + v\times w)\Big) \\
&= \Big(abc - a(v\cdot w) - b(u\cdot w) - c(u\cdot v) - u\cdot(v\times w), \\
&\qquad (ab)w + (ac)v + a(v\times w) + (bc)u - (v\cdot w)u + b(u\times w) + c(u\times v) + u\times(v\times w)\Big)
\end{aligned}$$

are the same because $(u \times v) \cdot w = u \cdot (v \times w)$ (the scalar triple product), and because

$$u \times (v \times w) - (v \cdot w)u = (u \cdot w)v - (u \cdot v)w - (v \cdot w)u \quad \text{and}$$

$$(u \times v) \times w - (u \cdot v)w = -w \times (u \times v) - (u \cdot v)w = -((w \cdot v)u - (w \cdot u)v) - (u \cdot v)w$$

are the same by commutativity of dot product (the equalities/simplifications are by the vector triple product identity, and anticommutativity of cross product).

However the product is not in general commutative, because the cross product is anticommutative; for example, letting i, j, k be the standard basis vectors for $\mathbb{R}^3$, we see that

$$(1,i)(1,j) = (1-0, j+i+i\times j) = (1, i+j+k) \neq (1, i+j-k) = (1-0, i+j+j\times i) = (1,j)(1,i)$$

(b) We want to show that the norm N is multiplicative. $N((a,u)(b,v)) = (ab-u\cdot v)^2+|av+bu+u\times v|^2$, but $u \times v$ is perpendicular to both u and v, and so by the Pythagorean theorem this is equal to

$$\begin{aligned}
N((a,u)(b,v)) &= (ab)^2 - 2ab(u\cdot v) + (u\cdot v)^2 + |av+bu|^2 + |u\times v|^2 \\
&= (ab)^2 - 2ab(u\cdot v) + (|u||v|\cos\theta)^2 + (av+bu)\cdot(av+bu) + (|u||v|\sin\theta)^2 \\
&= (ab)^2 - 2ab(u\cdot v) + (|u||v|)^2 + a^2|v|^2 + 2ab(u\cdot v) + b^2|u|^2 \\
&= (ab)^2 + (|u||v|)^2 + a^2|v|^2 + b^2|u|^2 \\
&= (a^2+|u|^2)(b^2+|v|^2) = N((a,u))N((b,v))
\end{aligned}$$

(c) We want to show that the non-zero elements of C form a group under multiplication. We have already shown that the product is associative. The set is closed under the operation because if (a,u) and (b,v) are non-zero elements of C, then their product is also a non-zero element of C, because an element is the zero element $= (0,(0,0,0))$ if and only if the norm N is 0 ($a^2 = 0 \iff a = 0$ and $|u| = 0 \iff u = (0,0,0)$), and from (b) the norm is multiplicative. The identity of the set is $(1,(0,0,0))$ because

$$(a,u)(1,(0,0,0)) = (a-0, 0+1u+0) = (1,(0,0,0))(a,u).$$

And finally, the inverse: if we multiply the element (a,u) by $(-a,u)$, we get the zero vector in the second coordinate:

$$(a,u)(-a,u) = (a(-a) - u\cdot u, au - au + u\times u) = (-(a^2+|u|^2),(0,0,0))$$

If we scale $(-a,u)$ to be $(a/N((a,u)), -u/N((a,u)))$, then in fact the first coordinate goes to 1 and the second coordinate stays $(0,0,0)$, and so the inverse of $(a,u) \in C^*$ is $(a/N((a,u)), -u/N((a,u)))$.

(d) Define Q to be the set of all elements in C^* with integer coefficients/values and have norm 1. $N((a,u)) = N((a,(u_1,u_2,u_3)) = a^2+u_1^2+u_2^2+u_3^2$ can only be 1 (when a, u_1, u_2, u_3 are integers) if one of the numbers is ± 1 and the others are all 0. There are 8 such elements in C^*; we want to show that they form a subgroup. Associativity is inherited from C^*. Closure comes from the fact that the product consists of the operations $+, -, \cdot, \times$ which spit out integers if the inputs are integers and the fact that the norm N is multiplicative, so the product of two elements in Q must remain in Q. The identity $(1,(0,0,0))$ is in Q. And lastly, the inverse is in Q because from the formula in the end of (c), the inverse of $(a,u) \in Q$ is $(a,-u)$ (so the values remain integers), and again from the fact that the norm is multiplicative $N((a,-u))$ must be 1 and hence it must be in Q.

Problem 6

Consider $G = D_8$, the group of symmetries of the square: $\{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$ (r is a rotation by 90 degrees, and s is a flip). Recall the properties that $r^4 = 1, s^2 = 1$, and $rs = sr^{-1}$ (or more generally $r^n s = sr^{-n}$). Let $K = \{1, s\}$ and $N = \{1, s, r^2, r^2s\}$. Then I claim that K is normal in N, N is normal in G, but K is not normal in G.

- K is normal in N, because if $n \in N$ is also in K, then obviously $nK = K = Kn$. That leaves the possibilities $n = r^2$ or r^2s. From the properties above, we know that $r^2s = sr^{-2} = sr^2$ and hence
$$r^2K = \{r^2, r^2s\} = \{r^2, sr^2\} = Kr^2$$
and lastly
$$(r^2s)K = r^2(sK) = r^2K = Kr^2 = (Ks)r^2 = K(sr^2) = K(r^2s)$$
where we used the fact that $s \in K$.

- N is normal in G, because if $g \in G$ is also in N, then obviously $gN = N = Ng$. That leaves the possibilities that $n \in \{r, r^3, rs, r^3s\}$. First,
$$rN = \{r, rs, r^3, r^3s\} = \{r, sr^{-1}, r^3, sr^{-3}\} = \{r, sr^3, r^3, sr\} = Nr.$$
Then,
$$r^3N = r(r^2N) = rN = Nr = (Nr^2)r = Nr^3$$
where we used the fact that $r^2 \in N$. The rs and r^3s follow similarly because s and r^2s are both in N.

- However, K is not normal in G because $rK = \{r, rs\}$ while $Kr = \{r, sr\}$ but $rs = sr^{-1} \neq sr$.