Math 594. Homework 2 (due January 22)

Book problems: §4.1: 9 (ignore hint for (*b*); think geometrically), 10.

1. Let Q denote the quaternion group from §1.5.

(*i*) As the book notes, merely writing down relations doesn't guarantee that there exists a non-trivial group satisfying the relations (e.g., if we try to "define" a group by the condition that it be generated by an element g satisfying the relations $g^3 = g^5 = 1$, then it must be the trivial group). Get around this issue in the present case by checking that the matrices

$$\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbf{C})$ satisfy the desired relations and generate a subgroup of $\mathbf{GL}_2(\mathbf{C})$ of order exactly 8 (here, $i \in \mathbf{C}$ is a fixed square root of -1).

(*ii*) Work out all of the distinct subgroups of Q, and check they're all normal by inspection.

2. Let G be a group and H a subgroup.

(*i*) If H' is a subgroup of H, show that the various group indices are related by the equation $[G : H'] = [G : H][H : H']$, understood to implicitly include the assertion that if any two of the three are finite then so is the third (in which case this equation holds).

(*ii*) If G acts on the right on a set X and H is normal in G, show that the *group* G/H naturally *acts* on the right on the set X/H, and construct a natural bijection $(X/H)/(G/H) \simeq X/G$.

3. Let F be a field and V a vector space of dimension $n > 0$ over F.

(*i*) Show that the center of $G = \mathrm{GL}(V)$ is the subgroup of nonzero scalar multiplications ($\simeq F^{\times}$).

(*ii*) Let $V = \oplus V_i$ be a decomposition into a direct sum of (nonzero) subspaces. Let $H \subseteq G$ be the subgroup which respects this decomposition (i.e., those elements carrying each V_i back into itself); in terms of a basis adapted the V_i's, there are "block" matrices. Assume $|F| > 2$. By thinking about stable subspaces (don't use matrices!!!), describe $N_G(H)$ and $Z_G(H)$, as well as $N_G(H)/Z_G(H)$ (identify this latter quotient with a suitable symmetric group). Pay attention to V_i's of the same dimension!

(*iii*) For an element $g \in K = \mathfrak{S}_n$ generating a subgroup H, describe $N_K(H)$, $Z_K(H)$, and $N_G(K)/Z_G(K)$ in terms of the cycle decomposition of g (hint: look at orbits of g-action, the analogues of stable subspaces).

4. Let G be a finite abelian group, H a subgroup. Let $\chi : H \to \mathbf{C}^{\times}$ be a group homomorphism.

(*i*) Show that the image $\chi(H)$ consists of roots of unity.

(*ii*) If H' is a second subgroup of G and $\chi' : H' \to \mathbf{C}^{\times}$ is a group homomorphism, then assuming $\chi|_{H \cap H'} = \chi'|_{H \cap H'}$ shows that there exists a unique group homomorphism $\widetilde{\chi} : HH' \to \mathbf{C}^{\times}$ which restricts to χ on H and χ' on H' (must use that G is abelian!).

(*iii*) Show that the originally given χ extends to a group homomorphism $G \to \mathbf{C}^{\times}$.

5. This exercise determines the structure of $(\mathbf{Z}/p^r)^{\times}$ for any prime p and any $r \geq 1$.

(*i*) Assume $p > 2$. Show that a is an integer not divisible by p, then $(1 + ap^i)^p = 1 + a'p^{i+1}$ for some a' not divisible by p (you'd better use somewhere that $p \neq 2$). Deduce for any $i \geq 0$ that that $(1+p)^r \equiv 1 \bmod p^{i+1}$ if and only if $p^i | r$. Give a counterexample to this when $p = 2$.

(*ii*) Fix $p \geq 2$ and $i \geq 1$. Show that the natural reduction map $\mathbf{Z}/p^i \to \mathbf{Z}/p$ induces a homomrphism of unit groups $(\mathbf{Z}/p^i)^{\times} \to (\mathbf{Z}/p)^{\times}$. But in HW1 we saw (conditional on a result to be shown later, if not knowm already) that $(\mathbf{Z}/p)^{\times}$ is a cylic group, since $\mathbf{Z}/p$ is a *finite field*. Picking $u \in (\mathbf{Z}/p^i)^{\times}$ lifting a generator of $(\mathbf{Z}/p)^{\times}$, deduce there must exist an element of $(\mathbf{Z}/p^i)^{\times}$ of order $p - 1$. But in (*i*) you showed $1 + p \bmod p^i$ has order p^{i-1}. Deduce that there exists an element of order $p^{i-1}(p-1)$, and conclude that such an element is a generator (so $(\mathbf{Z}/p^i)^{\times}$ is *cyclic*).

(*iii*) The case $p = 2$ is a little different. By inspection, $(\mathbf{Z}/2)^{\times}$ is cyclic, so now fix $i \geq 2$ and consider $G = (\mathbf{Z}/2^i)^{\times}$. Let H be the subgroup of elements congruent to 1 mod 4 (i.e., the kernel of $(\mathbf{Z}/2^i)^{\times} \twoheadrightarrow (\mathbf{Z}/4)^{\times}$). Show that every element in G can be *uniquely* written in the form $\varepsilon \cdot h$ where $\varepsilon = \pm 1$ and $h \in H$. To show H is cyclic (of what order?), prove a suitable variant on (*i*) by studying $(1 + a \cdot 2^j)^2$ for $j \geq 2$ and odd a.