Math 594. Solutions 2

Book problems §4.1:

9. Suppose that G acts transitively on the finite set A and let H be a normal subgroup of G with $\mathcal{O}_1 \ldots \mathcal{O}_r$ the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1 \ldots \mathcal{O}_r$ transitively. Deduce that all orbits of H on A have the same cardinality.

Solution: For each i there is some $a_i \in A$ such that $\mathcal{O}_i = Ha_i$. Now since $H \lhd G$, we have $g\mathcal{O}_i = gHa_i = Hga_i = H(ga_i)$. Now $ga_i \in Ha_j$ for some j since the sets Ha_j for $j = 1, \ldots, r$ partition A, from which it follows that $Hga_i = Ha_j$, i.e. $g\mathcal{O}_i = \mathcal{O}_j$ for some j. Since G acts transitively on A, for each i, j there is a $g \in G$ such that $ga_i = a_j$ and hence $g\mathcal{O}_i = \mathcal{O}_j$ so that G acts transitively on $\{\mathcal{O}_1 \ldots \mathcal{O}_r\}$. Since $gha_i = gh'a_i$ if and only if $ha_i = h'a_i$, all orbits of H on A have the same cardinality.

(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and that $r = |G : HG_a|$.

Solution: Suppose that for $h_1, h_2 \in H$ we have $h_1 a = h_2 a$. Then clearly $h_2^{-1}h_1 \in H_a$, or equivalently, $h_1 H_a = h_2 H_a$. The converse is clear, so that the distinct points of A in the orbit $\mathcal{O}_1 = Ha$ are in bijective correspondence with the cosets of H_a in H. It follows that $[H : H_a] = [H : H \cap G_a] = |\mathcal{O}_1|$. Similarly, since G acts transitively on A, we have $[G : G_a] = |A|$, and since A is partitioned into the distinct H orbits (which all have the same size by part (a)), we also have $|A| = r|\mathcal{O}_1| = r[H : H_a]$. Now since $H \lhd G$, we have $G_a < N_G(H) = G$. It then follows from the Second Isomorphism Theorem that $G_a H/H \simeq G_a/(G_a \cap H)$ so that in particular, $[G_a H : H] = [G_a : H_a]$. By Problem 2 ($i$), we have, using our calculations above,

$$\begin{aligned}
[G : G_a H][G_a H : H_a] &= [G : H_a] = [G : G_a][G_a : H_a] \\
&= |A|[G_a : H_a] = r[H : H_a][G_a H : H] \\
&= r[G_a H : H_a],
\end{aligned}$$

so that $[G : G_a H] = r$ as required.

10. Let H, K be subgroups of G and define $HxK = \{hxk : h \in H,\ k \in K\}$.

(a) Prove that HxK is a union of the right cosets $x_1 K, \ldots x_n K$, where $\{x_1 K, \ldots x_n K\}$ is the H orbit of the coset xK.

Solution: We must show that every $hxk \in HxK$ lies in some $x_i K$, where $\{x_1 K, \ldots, x_n K\}$ is the orbit of xK under the left action of H. Indeed, hxK is in the orbit of xK under the left action of H by definition, so that $hxK = x_i K$ for some i. It follows that $hxk \in x_i K$. Thus, $HxK \subset \cup_{i=1}^n x_i K$. On the other hand, we clearly have the reverse containment as every $x_i K$ is of the form $h_i xK$ for some $h_i \in H$ and is therefore contained in HxK.

(b) Prove that HxK is a union of left cosets of H.

Solution: Similarly, we let $\{Hy_1, \ldots, Hy_m\}$ be the orbit of Hx under the right action of K. Then $hxk \in Hxk \in Hy_j$ for some j since it is in the K orbit of Hx.

(c) For any $x, y \in G$, show that HxK and HyK are either disjoint or coincide, and conclude that the set of HK double cosets partitions G.

Solution: If $x \in HyK$ then we have $x = hyk$ for some $h \in H$ and $k \in K$, or what is the same thing, $y = h^{-1}xk^{-1}$. It follows that $y \in HxK$. The converse is just as clear (by interchanging x, y) so that $x \in HyK$ if and only if $HxK = HyK$. Now suppose that $y \in HxK$ and $z \in HyK$. Then we can write (as before) $z = h_1 y k_1 = h_1 h_2 x k_2 k_1 := hxk$ for some h_1, h_2, k_1, k_2, so that $z \in HxK$. (What we have shown is that $x \sim y$ if and only if $x \in HyK$ is an equivalence relation). Thus, if $z \in HxK \cap HyK$ then $HxK = HzK = HyK$ so that two double cosets are either disjoint or equal. Moreover, since $g \in G$ is in the coset HgK, the set of HK double cosets partitions G.

(d) Prove that $|HxK| = |K||H : H \cap xKx^{-1}|$.

Solution: We claim that there is a natural bijection between the set of cosets of K contained in HxK and the set of cosets of $H \cap xKx^{-1}$ in H given by $hxK \mapsto h(H \cap xKx^{-1})$. Let us first show that this is well defined. Suppose that $h_1xK = h_2xK$. Then $h_1 = h_2xkx^{-1}$ for some $k \in K$. But since $h_1, h_2 \in H$, we see that $xkx^{-1} \in H \cap xKx^{-1}$ so that $h_1(H \cap xKx^{-1}) = h_2(H \cap xKx^{-1})$ and our map is well defined. Now suppose that $h_1(H \cap xKx^{-1}) = h_2(H \cap xKx^{-1})$. Then there exists $k \in K$ such that $h_1 = h_2xkx^{-1}$ so that $h_1x = h_2xk$ whence $h_1xK = h_2xK$ so that our map is injective. Surjectivity follows from the fact for any $h \in H$, the coset $h(H \cap xKx^{-1})$ is the image of $hxK \in HxK$. It follows that the number of cosets of K in HxK is equal to the number of cosets of $H \cap xKx^{-1}$ in H, that is $[HxK : K] = [H : H \cap xKx^{-1}]$. Now using the formula $[HxK : K] = |HxK|/|K|$ we establish

$$|HxK| = |K| \cdot |H : H \cap xKx^{-1}|.$$

(e) Prove that $|HxK| = |H||K : K \cap x^{-1}Hx|$.

Solution: The proof is identical to the above, with the map $Hxk \mapsto (K \cap x^{-1}Hx)k$ inducing the required bijection.

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 $\mathrm{GL}_2(\mathbf{C})$ of order exactly 8 (here, $i \in \mathbf{C}$ is a fixed square root of -1).

Solution: We define

$$\mathbf{k} = \mathbf{ij} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

By straightforward matrix multiplication, we find $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and

$$\begin{aligned} \mathbf{ij} &= \mathbf{k} & \qquad \mathbf{ji} &= -\mathbf{k} \\ \mathbf{jk} &= \mathbf{i} & \qquad \mathbf{kj} &= -\mathbf{i} \\ \mathbf{ki} &= \mathbf{j} & \qquad \mathbf{ik} &= -\mathbf{j} \end{aligned}$$

Thus, the group generated by $\mathbf{i}, \mathbf{j}$ consists precisely of the elements $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ under the above rules of multiplication, and is hence of order 8 and isomorphic to Q.

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

Solution: Observe that if any subgroup $H < Q$ contains two of $\mathbf{i}, \mathbf{j}, \mathbf{k}$ then it contains the third and is hence all of Q. It follows that the distinct subgroups of Q are:

$$\begin{aligned} H_0 &= \{\pm 1\} \\ H_1 &= \{\pm 1, \pm\mathbf{i}\} \\ H_2 &= \{\pm 1, \pm\mathbf{j}\} \\ H_3 &= \{\pm 1, \pm\mathbf{k}\}. \end{aligned}$$

Moreover, since ± 1 are scalar matrices, they commute with $\mathbf{i}, \mathbf{j}, \mathbf{k}$. From our multiplication rules above, we have

$$\mathbf{jij^{-1}} = -\mathbf{jij} = \mathbf{kj} = -\mathbf{i},$$

and similarly

$$\mathbf{kik^{-1}} = -\mathbf{kik} = -\mathbf{jk} = -\mathbf{i}.$$

It follows that $H_1 \lhd Q$ and similarly $H_2 \lhd Q$, $H_3 \lhd Q$. As we remarked above, $H_0 = \mathrm{Z}(Q)$ and so $H_0 \lhd Q$ also.

2. Let G be a group and $H' < H$ subgroups.

(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).

Solution: Suppose that the distinct cosets of H in G are given by $\{\alpha H\}$ with $\alpha \in A \subset G$ and that the distinct cosets of H' in H are given by $\{\beta H'\}$ for $\beta \in B \subset H$. We claim that the set $\{\alpha\beta H'\}$ for $\alpha \in A$ and $\beta \in B$ is a complete set of distinct coset representatives for H' in G. First, observe that if $\alpha_1\beta_1 H' = \alpha_2\beta_2 H'$ then there exists some $h' \in H'$ such that $\alpha_1\beta_1 = \alpha_2\beta_2 h'$. Now $H' < H$ and $\beta_i \in H$ so that, for suitable $h \in H$, we have $\alpha_1 = \alpha_2 h$. It follows that $\alpha_1 H \subseteq \alpha_2 H$. Similarly, $\alpha_2 = \alpha_1 h^{-1}$ whence $\alpha_2 H \subseteq \alpha_1 H$ and we therefore have $\alpha_1 H = \alpha_2 H$. But this is a contradiction (unless $\alpha_1 = \alpha_2$) as we assumed the αH to be distinct cosets of H in G. A similar contradiction follows if $\alpha_1 = \alpha_2$ but $\beta_1 \neq \beta_2$ (using the fact that the $\beta H'$ are distinct cosets of H' in H. It follows that the $\alpha\beta H'$ are distinct cosets of H' in G. We claim that they partition G. For let $g \in G$. Then $g \in \alpha h$ for some $\alpha \in A$ and some $h \in H$ (since $\{\alpha H\}$ is a complete set of cosets of H in G. But we can write $h = \beta h'$ for some $\beta \in B$ and $h' \in H'$ (since $\{\beta H'\}$ is a complete set of cosets for H' in H). Thus, $g \in \alpha\beta H'$ so the $\alpha\beta H'$ partition G. Now if $[G : H']$ is infinite, there must be infinitely many cosets $\alpha\beta H'$ from which it follows that one of A, B is infinite. So suppose that $[G : H']$ is finite. Then from our bijection above, we must have that $|A|, |B|$ are finite and

$$[G : H'] = |A||B| = [G : H][H : H'].$$

(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 $(X/H)/(G/H) \simeq X/G$.

Solution: Let $xH \in X/H$ and $g_1H, g_2H \in G/H$. Observe that $(xHg_1H)(g_2H) = (xg_1H)(g_2H) = (xg_1g_2)H = xHg_1g_2H$, where we have used the fact that $gH = Hg$ for all $g \in G$ since $H \lhd G$. Moreover, we have $xHH = xH$ so that we do indeed have a group action. (In fact, G acts on X/H and the proof is the same as above. However, since H acts trivially on X/H, this action descends to an action of G/H on X/H).

Now let us define a map $(X/H)/(G/H) \to X/G$ by $(xH)(G/H) \mapsto xG$. We must check that this is well defined. Suppose that $(xH)(G/H) = (yH)(G/H)$. Then there exists some gH in G/H such that $xH = yHgH = ygH$, i.e., for some $h \in H$ we have $x = ygh$, or in other words, $x \in yG$. It follows that $xG = yG$ so our map is well defined. Now suppose that $xG = yG$. Then there exists $g \in G$ with $x = yg$ so that $xH = ygH = yHg$ whence $(xH)(G/H) = (yH)(G/H)$ so our map is injective. Surjectivity is obvious, so that we have a bijection of sets $(X/H)/(G/H) \simeq X/G$.

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 ($\simeq F^\times$).

Solution: Recall that G acts transitively on the set of lines in V. We claim that any $h \in H = Z(G)$ must fix every line in G. For suppose not, and let l_1, l_2 be distinct lines with $h(l_1) = l_2$. then there exists a $g \in G$ such that $g(l_1) = l_1$ but $g(l_2) \neq l_2$. Then we have $gh(l_1) = g(l_2)$ while $hg(l_1) = h(l_1) = l_2$. Since g does not fix l_2, we see that g, h do not commute. But recall that on HW 1, Problem 4 (ii) we showed that if $h \in G$ fixes every line in V it must be scalar multiplication on V. Conversely, it is clear that every scalar multiplication on V is in $Z(G)$.

(ii) Let $V = \oplus V_i$ be a decomposition into a direct sum of (nonzero) subspaces $V_1, V_2, \ldots, V_r$. 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!

Solution: Let us call a nonzero vector space W equipped with linear H action *irreducible* if it has no H stable subspaces other than itself and $\{0\}$ (we shall say that an H stable subspace W' of W is *trivial* if $W' = \{0\}$). We claim that the irreducible subspaces of V are precisely the V_i. First, since H is the group of invertible linear transformations of V preserving V_i, for each i we have a natural map $H \to \mathrm{GL}(V_i)$ given by restriction to V_i. Using the same arguments as HW 1, Problem 3 (ii), it is not difficult to see that this map is surjective for each i. It follows that V_i is irreducible (since, for example, we can find a $g' \in \mathrm{GL}(V_i)$ taking any nonzero vector to any other nonzero vector), and it's not hard to convince one's self that in fact $H \simeq \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \ldots \times \mathrm{GL}(V_r)$. Conversely, suppose that $W \subset V$ is an irreducible subspace of V, and let $\phi_i : W \to V_i$ be projection onto V_i. Since W is by assumption H stable, the image of W under ϕ_i is an H stable subspace of V_i, and thus must be all of V_i or $\{0\}$ for each i, i.e. ϕ_i is either 0 or surjective. Similarly, the kernel of ϕ_i is an H stable subspace of W, and since W is irreducible, its kernel is either trivial or all of W, so that each each ϕ_i is either 0 or an isomorphism. Certainly, some ϕ_i is nonzero: since $V = \oplus V_i$, if $w \in W$ projects to 0 in every V_i, it must be zero, and we chose $W \neq \{0\}$. Thus, let i_0 be such that ϕ_{i_0} is nonzero; then it must be an isomorphism $\phi_{i_0} : W \to V_{i_0}$. We now claim that $\phi_i = 0$ for all $i \neq i_0$. Pick any nontrivial $g_0 \in \mathrm{GL}(V_{i_0})$ (this is possible even if $\dim(V_{i_0}) = 1$ since $|F| > 2$) and let $h \in H \simeq \mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \ldots \times \mathrm{GL}(V_r)$ be such that $h|_{V_i} = 1$ for $i \neq i_0$ and $h|_{V_{i_0}} = g_0$. Now since $\phi_{i_0} : W \to V_{i_0}$ is an isomorphism carrying the H action on W over to $\mathrm{GL}(V_{i_0})$ action on V_{i_0}, we see that H acts nontrivially on W. Again, we know that ϕ_i carries the H action on W to the $\mathrm{GL}(V_i)$ action on V_i, and by our construction of h (trivial component in each $\mathrm{GL}(V_i)$ for $i \neq i_0$), the action of $\mathrm{GL}(V_i)$ on V_i induced by the action of h on W is trivial for all $i \neq i_0$. Thus, if some ϕ_i for $i \neq i_0$ were an isomorphism, h would act trivially on W, which is a contradiction. It follows that $\phi_i = 0$ for all $i \neq i_0$. Finally, since V_{i_0} is the intersection of the kernels of ϕ_i for $i \neq i_0$, we see that $W \subseteq V_i$. Irreducibility of V_i then forces $W = V_i$ (this is actual *equality* and not just an isomorphism).

Now we describe $N_G(H)$. Suppose that $g \in N_G(H)$, so that $gH = Hg$. (Observe that we really are computing the normalizer $N_G(H) = \{g \in G : gHg^{-1} = H\}$, and not the "fake" normalizer $N'_G(H) = \{g \in G : gHg^{-1} \subset H\}$). Then for any i we have $gH(V_i) = g(V_i) = Hg(V_i)$, so that H preserves $g(V_i)$. Certainly, since g is invertible, $\dim(V_i) = \dim(gV_i)$. Observe that gV_i is irreducible: if $W \subset gV_i$ is a nontrivial, proper H stable subspace then $Hg^{-1}W = g^{-1}HW = g^{-1}W$ so that $g^{-1}W$ is a nontrivial, proper H stable subspace of V_i, which is impossible by the above. Thus, by our characterization of the V_i, we see that $g(V_i) = V_j$ for some j with $\dim(V_i) = \dim(V_j)$ (since g is invertible). In short, any element of $N_G(H)$ permutes V_j's of the same dimension. Conversely, the above argument shows that any $g \in G$ which permutes V_j's of the same dimension is in $N_G(H)$. It follows that $N_G(H)$ is generated by H together with those elements of G that permute V_i's of the same dimension.

Now let $g \in Z_G(H)$. Since we obviously have $Z_G(H) < N_G(H)$ we already know that g permutes V_i's of the same dimension. We claim that in fact g must take V_i to itself for each i. For suppose not, and let $gV_i = V_j \neq V_i$ for some i, j. From our description above of H as a direct product, and since $|F| > 2$, there exists $h \in H$ such that $h|_{V_i}$ is scalar multiplication by $\lambda_i \in F^\times$ and $h|_{V_j}$ is scalar multiplication by $\lambda_j \neq \lambda_i$. For $v_i \in V_i$ we then have $gh(v_i) = \lambda_i g(v_i)$ while $hg(v_i) = \lambda_j g(v_i)$ since $g(v_i) \in V_j$. This is a contradiction. It follows that $g(V_i) = V_i$ so that we get a reduction map $Z_G(V_i) \to \mathrm{GL}(V_i)$. Again, since $H \to \mathrm{GL}(V_i)$ is surjective, we must have $g|_{V_i} \in Z(\mathrm{GL}(V_i))$ so that by part (i), g must be scalar multiplication on each V_i. Conversely, it is clear that any $g \in G$ which is scalar multiplication on each V_i (possibly different scalars for each i) is in $Z_G(H)$.

Let n_k for $k = 1, \ldots, s$ be the distinct values of $\dim V_j$ for $j = 1 \ldots r$ and let $e_k = |\{j : \dim(V_j) = n_k\}|$. We have just seen that for each k, the group $N_G(H)$ acts on the set of all V_i of dimension n_k. Moreover, from our description of H, we see that this action can be described by any permutation of the e_k spaces V_i of dimension n_k, together with an element of $\mathrm{GL}_{n_i}(F)^{e_i}$ (or equivalently, e_i elements of $\mathrm{GL}_{n_i}(F)$). That is, any $g \in N_G(H)$, when restricted to the set of V_i of dimension n_k, can be written in the form $f_k = (\sigma, (g_1, g_2, \ldots, g_{e_k}))$, where $\sigma \in \mathfrak{S}_k$ and $g_i \in \mathrm{GL}_{n_i}(F)$, and we have

$$f_k(V_{k,1} \oplus V_{k,2} \oplus \cdots \oplus V_{k,e_k}) = g_1 V_{k,\sigma(1)} \oplus g_2 V_{k,\sigma(2)} \oplus \cdots \oplus g_{e_k} V_{k,\sigma(e_k)},$$

where $V_{k,l}$ for $l = 1, \ldots, e_k$ are all the V_i of dimension n_k. Observe that we have

$$\begin{aligned}(\sigma, (g_1, \ldots, g_{e_k}))&(\tau, (h_1, \ldots, h_{e_k}))(V_{k,1} \oplus V_{k,2} \oplus \cdots \oplus V_{k,e_k}) \\ &= (\sigma, (g_1, \ldots, g_{e_k}))(h_1 V_{k,\tau(1)} \oplus h_2 V_{k,\tau(2)} \oplus \cdots \oplus h_{e_k} V_{k,\tau(e_k)}) \\ &= g_1 h_{\sigma(1)} V_{k,\sigma\tau(1)} \oplus g_2 h_{\sigma(2)} V_{k,\sigma\tau(2)} \oplus \cdots \oplus g_{e_k} h_{\sigma(e_k)} V_{k,\sigma\tau(e_k)} \\ &= (\sigma\tau, (g_1 h_{\sigma(1)}, \ldots, g_{e_k} h_{\sigma(e_k)}))(V_{k,1} \oplus V_{k,2} \oplus \cdots \oplus V_{k,e_k}),\end{aligned}$$

so that multiplication is defined by

$$(\sigma, (g_1, \ldots, g_{e_k}))(\tau, (h_1, \ldots, h_{e_k})) = (\sigma\tau, (g_1 h_{\sigma(1)}, \ldots, g_{e_k} h_{\sigma(e_k)})).$$

There is a special construction for groups of this form, called a "semi-direct product," (denoted by a "$\ltimes$"). We have just seen that $N_G(H)$, when restricted to the direct sum of all V_i's of the same dimension n_k, acts as

$$\mathfrak{S}_{e_k} \ltimes \mathrm{GL}_{n_k}(F)^{e_k},$$

where $\mathfrak{S}_{e_k}$ acts on $\mathrm{GL}_{n_k}(F)^{e_k}$ by permuting the factors (as we saw in the multiplication rule above). Each direct sum "block" of V_i's of the same dimension is acted on independently by $N_G(H)$, so that we have

$$N_G(H) \simeq (\mathfrak{S}_{e_1} \ltimes \mathrm{GL}_{n_1}(F)^{e_1}) \times \cdots \times (\mathfrak{S}_{e_s} \ltimes \mathrm{GL}_{n_s}(F)^{e_s}).$$

If you are having trouble seeing all this, think of the case done in class, where each V_i is linear. In this case, we saw that the normalizer $N_G(H)$ consisted of all diagonal matrices (i.e. $\mathrm{GL}_1(F)^n \simeq (F^\times)^n$) together with any permutation $\sigma \in \mathfrak{S}_\mathfrak{n}$ of the V_i's, and hence that $N_G(H) \simeq \mathfrak{S}_n \ltimes \mathrm{GL}_1(F)^n$, and any $(\sigma, (\alpha_1, \ldots, \alpha_n)) \in \mathfrak{S}_n \ltimes \mathrm{GL}_1(F)^n$ acted by

$$(\sigma, (\alpha_1, \ldots, \alpha_n))(V_1 \oplus V_2 \oplus \cdots \oplus V_n) = \alpha_1 V_{\sigma(1)} \oplus \alpha_2 V_{\sigma(2)} \oplus \cdots \oplus \alpha_n V_{\sigma(n)}.$$

Finally, we have determined that $Z_G(H)$ consists of those $g \in G$ that act by scalar multiplication on each V_i. That is, we can write

$$Z_G(H) \simeq (F^\times)^r = (F^\times)^{e_1} \times (F^\times)^{e_2} \times \cdots \times (F^\times)^{e_k}.$$

We claim that for normal subgroups B_i of groups A_i, we have $B_1 \times \ldots \times B_r \lhd A_1 \times \ldots \times A_r$ and $(A_1 \times \ldots \times A_r)/(B_1 \times \ldots \times B_r) \simeq (A_1/B_1) \times (A_2/B_2) \times \ldots \times (A_r/B_r)$. The normality of $B_1 \times \ldots \times B_r$ in $A_1 \times \ldots \times A_r$ is easy to check, just using the definition of multiplication in the direct product. We claim that the natural map $A_1 \times \ldots \times A_r \to (A_1/B_1) \times \ldots \times (A_r/B_r)$ given by $(a_1, \ldots, a_r) \mapsto (a_1 B_1, \ldots a_r B_r)$ is surjective (obvious) and has kernel $B_1 \times \ldots \times B_r$. This is straightforward to verify, and the First Isomorphism Theorem gives the required result. It follows that

$$N_G(H)/Z_G(H) \simeq (\mathfrak{S}_{e_1} \ltimes \mathrm{PGL}_{n_1}(F)^{e_1}) \times \cdots \times (\mathfrak{S}_{e_s} \ltimes \mathrm{PGL}_{n_s}(F)^{e_s}),$$

where $\mathrm{PGL}_{n_k}(F) = \mathrm{GL}_{n_k}(F)/F^\times$ is the projective linear group.

(*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).

Solution: Write $g \in K$ as $g = \sigma_1 \sigma_2 \cdots \sigma_r$, where the σ_i are disjoint cycles, and let $H =< g >$. Let us compute $Z_K(H)$. Observe that $k \in Z_K(H)$ if and only if $kgk^{-1} = (k\sigma_1 k^{-1})(k\sigma_2 k^{-1}) \ldots (k\sigma_r k^{-1}) = g$, i.e. if and only if the sets $\{k\sigma_i k^{-1} : 1 \leq i \leq r\}$ and $\{\sigma_i : 1 \leq i \leq r\}$ are identical (observe that it is inconsequential how k acts on the fixed points of g). Moreover, since conjugate cycles must have the same length, we see that conjugation by k must permute cycles of the same length. As in part (*ii*), suppose that there are e_l cycles of common length n_l in the factorization of g for $l = 1, \ldots, s$. Define $\sup(\sigma_i) = \{j : \sigma_i(j) \neq j\}$ (the "support" of σ_i). Clearly, disjoint cycles have disjoint supports. We may endow $\sup(\sigma_i)$ with a natural partial order, where for $m, n \in \sup(\sigma_i)$ we say $m < n$ if $\sigma(m) = n$. We claim that any $k \in N_K(G)$ with $k\sigma_1 k^{-1} = \sigma_2$ for disjoint cycles σ_1, σ_2 must respect the orderings on $\sup(\sigma_1)$ and $\sup(\sigma_2)$. Clearly, $k : \sup(\sigma_1) \to \sup(\sigma_2)$. Now let $x \in \sup(\sigma_1)$ with $\sigma(x) = y$. Then by hypothesis, $\sigma_2(kx) = k\sigma_1 k^{-1}(kx) = ky$. Conversely, it is not difficult to see that any $k \in K$ which permutes (under conjugation) the σ_i of the same length and respects the orderings of $\sup(\sigma_i)$ is in $N_K(H)$. Now up to cyclic permutations of $\sup(\sigma_i), \sup(\sigma_j)$, there is exactly one order preserving way to map $\sup(\sigma_i)$ to $\sup(\sigma_j)$. Moreover, our discussion above shows that we can permute the e_l elements of the set $S_l := \{\sup(\sigma_j) : \sigma_j$ has length $n_l\}$ arbitrarily for each l, and that every $k \in N_K(H)$ acts as one such permutation together with arbitrary cyclic permutations of $\sup(\sigma_j)$ for each j. Since every cyclic permutation of $\sup(\sigma_j)$ is effected by some power of σ_j, we can identify the group of such permutations (which obviously commute with H since σ_j commutes with H for all j) with $\langle\sigma_j\rangle \simeq \mathbf{Z}/n_j$. Thus, fixing a particular order on $\sup(\sigma_j)$ (say that we write the least member of $\sup\sigma_j$ first, and then use the ordering specified above), any element $k \in N_K(H)$ when restricted to

$$\sup(\sigma_{j,1}) \cup \sup(\sigma_{j,2}) \cup \ldots \cup \sup(\sigma_{j,e_l}),$$

where $\sigma_{j,i}$ for $i = 1, \ldots, e_l$ are the e_l σ_j's of common cycle length n_l, can be identified with some

$$(\tau, (i_1, i_2, \ldots, i_{e_l})) \in \mathfrak{S}_{e_l} \times (\mathbf{Z}/n_l)^{e_l}$$

and

$$(\tau, (i_1, i_2, \ldots, i_{e_l}))(\sup(\sigma_{j,1}) \cup \ldots \cup \sup(\sigma_{j,e_l})) = \sigma_{j,\tau(1)}^{i_1} \sup(\sigma_{j,\tau(1)}) \cup \ldots \cup \sigma_{j,\tau(e_l)}^{i_{e_l}} \sup(\sigma_{j,\tau(e_l)}).$$

Much as in part (ii), we can determine the multiplication rule

$$(\tau', (i'_1, i'_2, \ldots, i'_{e_l}))(\tau, (i_1, i_2, \ldots, i_{e_l})) = (\tau'\tau, (i'_1 + i_{\tau'(1)}, i'_2 + i_{\tau'(2)}, \ldots, i'_l + i_{\tau'(e_l)})).$$

We therefore have the identification

$$N_K(H) \simeq (\mathfrak{S}_{e_1} \ltimes (\mathbf{Z}/n_1)^{e_1}) \times (\mathfrak{S}_{e_2} \ltimes (\mathbf{Z}/n_2)^{e_2}) \times \cdots \times (\mathfrak{S}_{e_l} \ltimes (\mathbf{Z}/n_l)^{e_l}) \times \mathfrak{S}_f,$$

where each $\mathfrak{S}_{e_j}$ acts on $(\mathbf{Z}/n_l)^{e_l}$ by permuting the factors, and f is the number of fixed points of g so that $\mathfrak{S}_f$ accounts for the (allowable) arbitrary permutations of the fixed points of G.

Determining the structure of $N_K(H)$ and $N_K(H)/Z_K(H)$ is quite a bit more difficult. Everyone who tried this part was given credit for trying. Sometimes in math we are faced with hard problems.

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.

Solution: Let $h \in H$. Then $h^{|H|} = 1$ and since $\chi : H \to \mathbf{C}^\times$ is a homomorphism, we have $\chi(h)^{|H|} = 1$ and therefore $\chi(h)$ is a root of unity or order dividing $|H|$.

(ii) If H' is a second subgroup of G and $\chi' : H' \to \mathbf{C}^\times$ is a group homomorphism, then assuming $\chi|_{H\cap H'} = \chi'|_{H\cap H'}$ show 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!).

Solution: Define $\widetilde{\chi} : HH' \to \mathbf{C}^\times$ by $\widetilde{\chi}(hh') = \chi(h)\chi'(h')$ for $h \in H$ and $h' \in H'$ (observe that every element of HH' may be written in this form). Now $\widetilde{\chi}$ is well defined. For suppose that $h_1h'_1 = h_2h'_2$ for $h_i \in H$ and $h'_i \in H'$. Then we have $h_1h_2^{-1} = h'_2{h'_1}^{-1}$ since G is abelian. Observe that $h_1, h_2 \in H$ and $h'_1, h'_2 \in H'$ so that $h_1h'_1 = h_2h'_2 \in H \cap H'$ so that, since χ, χ' agree on $H \cap H'$ we have that $\chi(h_1)\chi(h_2)^{-1} = \chi'(h'_2)\chi'(h'_1)^{-1}$. Thus, $\chi(h_1)\chi'(h'_1) = \chi(h_2)\chi'(h'_2)$. Moreover, $\widetilde{\chi}$ is a group homomorphism. For let $h_1h'_1, h_2h'_2 \in HH'$; then we have

$$\widetilde{\chi}(h_1h'_1h_2h'_2) = \widetilde{\chi}(h_1h_2h'_1h'_2) = \chi(h_1h_2)\chi'(h'_1h'_2) = \chi(h_1)\chi(h_2)\chi'(h'_1)\chi'(h'_2) = \widetilde{\chi}(h_1h'_1)\widetilde{\chi}(h_2h'_2),$$

where we have used that G is abelian, and moreover $\widetilde{\chi}(1) = \chi(1) = 1$. It is clear that $\widetilde{\chi}$ is the unique homomorphism restricting to χ on H and χ' on H', since if any other homomorphism $\tau : HH' \to \mathbf{C}^\times$ had this property, we would be forced to have $\tau(hh') = \tau(h)\tau(h') = \chi(h)\chi'(h')$ for any $h \in H$ and $h' \in H'$, and since every $h \in H$ is of this form, $\tau = \widetilde{\chi}$ on all of HH'.

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

Solution: If $H = G$ we are done. Otherwise, there exists $g \in G - H$. Let n_g be the order of $\phi(g)$, where ϕ is the natural reduction map $G \to G/H$ (G is abelian, so H is normal!), i.e. n_g is the least positive integer such that $g^{n_g} \in H$. Pick $z \in \mathbf{C}^\times$ satisfying $z^{n_g} = \chi(g^{n_g})$ and define $\chi(g) = z$. This is possible since $x \mapsto x^n$ is surjective as a map from $\mathbf{C}^\times$ to itself, since every $x \in \mathbf{C}^\times$ may be written in the form $x = r\exp(2\pi i\theta)$ for $r \in \mathbf{R}_{>0}$. It is clear that χ defined in this way gives a character χ' on $\langle g\rangle$, and that χ, χ' agree on $H \cap \langle g\rangle$. It follows from (ii) that there is a unique character $\widetilde{\chi} : H\langle g\rangle \to \mathbf{C}^\times$ restricting to χ on H and χ' on $\langle g\rangle$.

Observe that since $g \notin H$ we have $|H| < |H\langle g\rangle|$. We can thus continue in this manner to obtain a sequence of subgroups G_i of G and extensions of χ to G_i with $G_i < G_{i+1}$ and $|G_i| < |G_{i+1}|$. Since $|G|$ is finite and $|G_i|$ is an integer for each i, there exists some $N > 0$ such that $G_N = G$, so that χ extends (but in general not uniquely—observe that we could have chosen a different value of z above) to a character on G.

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 $p = 2$.

Solution: We use the binomial theorem and find

$$(1+ap^i)^p = \sum_{j=0}^{p} \binom{p}{j} a^j p^{ij}.$$

If $i > 0$ then $p|\binom{p}{j}$ for $0 < j < p$. Therefore, we may rewrite the above sum as

$$(1+ap^i)^p = 1 + p^{i+1}\left(a + \sum_{j=1}^{p-1} \binom{p}{j+1} a^{j+1} p^{ij-1}\right).$$

Observe that if $p > 2$ then $p|\binom{p}{j}$ for $2 \leq j \leq p-1$ and, since $i > 0$, $p|p^{i(p-1)-1}$ (which is false for $i = 1$ and $p = 2$). Thus, we have

$$(1+ap^i)^p = 1 + p^{i+1}(a+px)$$

for some integer x. Since a is not divisible by p we see that $a' = (a+px)$ is not divisible by p as required. Now let $r = p^u s$, where $p \nmid s$. We have

$$(1+p)^r = ((1+p)^s)^{p^u} = \left(1 + \sum_{j=1}^{s} \binom{s}{j} p^j\right)^{p^u} = (1+ap)^{p^u},$$

where $a = s + p(\binom{s}{2}p + \cdots + \binom{s}{s}p^s)$ so that for $s \geq 1$ we see that a is not divisible by p. We therefore deduce that $(1+p)^r = (1+ap)^{p^u}$ for $p \nmid a$. Now, inductively assume that $(1+ap)^{p^{i-1}} = 1 + a'p^i$ for a' not divisible by p. Then we have $(1+ap)^{p^i} = (1+a'p^i)^p = 1 + a''p^{i+1}$ for $p \nmid a''$. Since we have already established this for $i = 0$, we conclude that $(1+p)^r = 1 + ap^{u+1}$ for some a not divisible by p. It follows that $(1+p)^r \equiv 1 \bmod p^{i+1}$ if and only if $p^i | r$ for any $p > 2$. When $p = 2$, we have the counterexample $2^3 | (3^2 - 1)$, but $2^2 \nmid 2$.

(*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*).

Solution: Let $r : \mathbf{Z}/p^i \to \mathbf{Z}/p$ be the natural reduction map. Observe that $(a + p^i x)(b + p^i y) = ab + p(p^{i-1}(ay + bx) + p^{2i}xy) \equiv ab \bmod p$ for any integers $a, b, x, y,$, and clearly $r(1) = 1$, so that r is a homomorphism. Moreover, r induces a homomorphism of unit groups since if $x \in (\mathbf{Z}/p^i)^\times$ then there exists $y \in (\mathbf{Z}/p^i)^\times$ with $xy = 1$, so that $r(xy) = r(x)r(y) = r(1) = 1$ whence $r(x) \in (\mathbf{Z}/p)^\times$. We further claim that r is surjective. Let $x \in (\mathbf{Z}/p)^\times$ and pick $x' \in \mathbf{Z}$ any lift of x. Then we must have $(x', p) = 1$ since x is a unit so that $(x', p^i) = 1$. It follows that multiplication by x' on $\mathbf{Z}/p^i$ is injective, and hence surjective by a counting argument. In particular, 1 is in the image of this map so that $x' \bmod p^i \in (\mathbf{Z}/p^i)^\times$ and $r(x') = x$.

Now let u be any lift of a generator of $(\mathbf{Z}/p)^\times$ to $(\mathbf{Z}/p^i)^\times$. Since $r(u)$ has order $p-1$, it follows that u cannot have order less than $p-1$ (otherwise, for some $k < p-1$ we have $r(u^k) = r(u)^k = 1$ whence u does not generate $(\mathbf{Z}/p)^\times$). On the other hand $r(u^{p-1}) = 1$ so that u^{p-1} is in the kernel of r, which is the subgroup of $(\mathbf{Z}/p^i)^\times$ consisting of those units that lift to an integer of the form $1 + px$ for some integer x.

But by part (i) we have seen that these units have order dividing p^{i-1}. Thus, there is a $j < i$ such that u has exact order $p^j(p-1)$ (for observe that $r(u^{p^j}) = r(u)^{p^j} = r(u)$, so that u^{p^j} cannot have order less that $p-1$). Thus, u^{p^j} has exact order $p-1$. Now in part (i) we showed that $1+p \bmod p^i$ has order p^{i-1}. Hence, since $(p, p-1) = 1$, by HW 1, Problem 7 (ii), we see that there exists an element of $(\mathbf{Z}/p^i)^\times$ of order $p^{i-1}(p-1)$. Now we have just seen that $r : (\mathbf{Z}/p^i)^\times \to (\mathbf{Z}/p)^\times$ is surjective with kernel N of size p^{i-1} (generated by the p^{i-1} distinct powers of $(1+p) \bmod p^i$). Therefore, $(\mathbf{Z}/p^i)^\times/N \simeq (\mathbf{Z}/p)^\times$ and hence $|(\mathbf{Z}/p^i)^\times| = |(\mathbf{Z}/p)^\times||N| = p^{i-1}(p-1)$. Since we have constructed an element of order $p^{i-1}(p-1)$, it follows that $(\mathbf{Z}/p^i)^\times$ is cyclic for every $i \geq 1$ and $p > 2$.

(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.

Solution: The group $(\mathbf{Z}/2)^\times$ is trivial and therefore cyclic. Now $x \in \mathbf{Z}/2^j$ is a unit if and only if any lift of x to $\mathbf{Z}$ is odd. Since the odd integers fall into two residue classes modulo 4 (with representatives $\pm$ 1), it follows that there are precisely two cosets of H in G with coset representatives ± 1 and hence that every element of G can be written uniquely as $\varepsilon \cdot h$ for $\varepsilon = \pm 1$ and $h \in H$. Next, we claim that $(1+4a)^r \equiv 1 \bmod 4 \cdot 2^i$ if and only if $2^i | r$. For we have $(1 + 4 \cdot 2^i a)^2 = 1 + 4 \cdot 2^{i+1} a + 2^{4+2i} a^2 = 1 + 4 \cdot 2^{i+1} a'$ where $a' = a + 2^{i+1} a^2$ is odd whenever a is (for all $i \geq 0$). Much as before, we employ the binomial theorem to obtain, for odd s,

$$(1+4a)^s = 1 + 4\left(as + 4\left(\binom{s}{2}4a^2 + \cdots + \binom{s}{s}4^{s-1}a^s\right)\right) = 1 + 4a'$$

where a' is odd (since as is odd and $s \geq 1$). Letting $r = 2^i s$ where s is odd, we have $(1+4a)^r = ((1+4a)^s)^{2^i} = (1+4a')^{2^i}$ where a' is odd. Now inductively assume that for a odd, we have $(1+4a)^{2^i} = 1 + 4 \cdot 2^i a'$ with a' odd. Then by our computations above, we have

$$(1+4a)^{2^{i+1}} = (1 + 4 \cdot 2^i a')^2 = 1 + 4 \cdot 2^{i+1} a''$$

with a'' odd. Since the case $i = 0$ is obvious, we see that $(1+4a)^r = 1 + 4 \cdot 2^i a'$ where 2^i is the exact power of 2 dividing r and a' is odd. It follows that $(1+4a)^r \equiv 1 \bmod 4 \cdot 2^i$ if and only if $2^i | r$. Thus, $5 \bmod 2^j$ has order 2^{j-2} in $(\mathbf{Z}/2^j)^\times$ for all $j \geq 2$. Moreover, $5 \in H$ since it is 1 modulo 4. It follows that the subgroup of G generated by $5 \bmod 2^j$ is contained in H (since the product of two integers that are 1 modulo 4 is again 1 modulo 4). But from our earlier characterization of units in $\mathbf{Z}/2^j$, we know that G has size 2^{j-1}, and since H has index 2 in G, it follows that $|H| = 2^{j-2}$ and hence that H is a cyclic subgroup of G generated by $5 \bmod 2^j$. It follows that every element of G may be written uniquely as $\pm 5^l \bmod 2^j$ with $0 \leq l < 2^{j-2}$.