Math 594, HW2 - Solutions

Gilad Pagi, Feng Zhu

February 8, 2015

1

a). It suffices to check that $NA$ is closed under the group operation, and contains identities and inverses:

- $NA$ is closed under the group operation since $N$ is normal: $nan'a' = n(an'a^{-1})a = nn'aa' \in NA$.
- $e \in A \cap N$ since both are subgroups, so $e = ee \in NA$.
- Given $na \in NA$, $(a^{-1}n^{-1})a^{-1} \in NA$ since $N$ is normal, and $na(a^{-1}n^{-1})a^{-1} = e$.

b). Define a map $N \rtimes A \to NA$ by $(n, a) \mapsto na$. This is a group map, since $(n, a)(m, b) = (n \gamma_a(m), ab) \mapsto namb$.

Moreover this map is surjective by construction.

The map is an isomorphism iff it is injective, iff $na \neq e$ for $(n, a) \neq (e, e)$, which happens iff $N \cap A = \{e\}$ (otherwise we can find $N \ni n \neq e$ with $n^{-1} \in A$, and then $(n, n^{-1}) \mapsto e$.)

c). $N \cong N \times_\phi A$ as $n \mapsto (n, e)$; $A \cong N \times_\phi A$ as $a \mapsto (e, a)$; (the isomorphic image of) $N$ is normal in $N \times_\phi A$ since

$$(m, b)(n, e)(m, b)^{-1} = (m, b)(n, e)(b^{-1} \cdot m^{-1}, b^{-1}) = (mb \cdot n, b)(b^{-1} \cdot m^{-1}, b^{-1})$$
$$= (mb \cdot nm^{-1}, e) \in N$$

and $N \cap A = \{e\}$ by construction.

d). Taking the last computation from the previous part and setting $m = e$ (so that $(m, b) = (e, b) \in A$, we obtain

$$(e, b)(n, e)(e, b)^{-1} = (b \cdot n, e)$$

i.e. conjugation of $N$ by an element $a \in A$ is equivalent to the action of $a$ on $N$, as desired.

*And the indirect help of Umang Varma, Lara Du*
e). The key here is to prove that $G = MN$: $N, M$ normal in $G$ so $MN = NM \lhd G$. Since $MN \supset M, N$ it must be then $G = MN$ or $MN = M$ or $MN = N$ otherwise, using the forth iso theorem, the image of $MN$ under the quotient $G \to G/M$ will give a non trivial subgroup. Same for $N$, But $N \neq M$ so it must be $G = NM$. Now the rest follows:

- Observe the canonical map $MN = G \to G/M \times G/N$. The kernel is $M \cap N$ so $G/(M \cap N) \cong G/M \times G/N$.
- $G/M = NM/M \cong N/(N \cap M)$ by using the second iso theorem. And symmetrically for $M$.

2

a). Let $\psi$ be the group map $K \to \text{Aut}(H)$ described, and let $r$ and $x$ denote generators of $H$ and $K$ resp.; then, applying the result of 1(d) to write the action of $K$ on $H$ as conjugation by elements of $K$, $H \rtimes \psi K = \langle r, x \mid xr^{-1}x^{-1} = r^{-1} \rangle \cong D_n$, where the isomorphism is given by sending $r$ to a rotation through $\frac{2\pi}{n}$, and $x$ to any reflection.

b). Let $E$ be the transformation inverting one coordinate (i.e. after fixing a basis, represented by a diagonal matrix with 1 on the diagonal in $n - 1$ places and $-1$ at one place. Notice: $\text{Det}(E) = -1, E \notin SO_n(\mathbb{R}), E^2 = I$. Define an action $\{I, E\} \to \text{Aut}SO_n(\mathbb{R})$ by $E(A) = EAE^{-1} = EAE$. Since $SO_n$ is of index 2, it is normal, then we get the semi-direct product group and it must be $G \cong SO_n(\mathbb{R}) \times \langle E \rangle$ and in fact $G = SO_n(\mathbb{R}) \langle E \rangle$. Specifically, define $SO_n(\mathbb{R}) \times \langle E \rangle \to O_n(\mathbb{R})$ by $(A, B) \mapsto AB$, and observe that in fact this is an isomorphism. This is not a direct product because $\langle E \rangle$ is not normal in $O_n(\mathbb{R})$: $EA$ is the $A$ matrix with the first row multiplied by -1, whereas $AE$ is the $A$ matrix where the first column is multiplied by -1.

c). Both $O_2, \mathbb{R}^2 \leq E$, intersection is trivial so it is a semi-product if one of the subgroups is normal. If $T$ is translation by $t$, and $A \in O_2$ then $ATA^{-1}$ is a translation by $At$ as seen in the computation below, thus $\mathbb{R}^2 \triangleleft E$ and we are done. The action $O_2 \to \text{Aut}(\mathbb{R}^2)$ must be conjugation in $E$, where the actual automorphism is quite natural: let $t$ be translation so $x \mapsto x + At$ is the same as $x \mapsto A^{-1}x \mapsto A^{-1}x + t \mapsto A(A^{-1}x + t) = x + At$

3

a). Given a split, we denote $A'$ as the image of $A$ in $G$ and denote $B'$ as the image of $B$ in $G$ under $\phi$. WTS $G = A'B', A' \vartriangleleft G, A' \cap B' = e$. First, consider $g \in G, g \notin A'$. chasing the diagram $g \mapsto b \neq e \in B \mapsto g' \in B' \mapsto b \in B$. So under $\pi$, the images of $g, g'$ are the same, and the $ker = A'$ so $g \in g'^{-1}A' \subset B'A'$. Indeed $A' \triangleleft G$. Finally, chasing a member of the kernel with preimage in $B$ must be $e$.

Alternatively, consider $G = N \rtimes H$. So the following is exact: $1 \to N \to G \xrightarrow{\pi} H \to 1$ using the projections, and $N$ normal. Consider $\phi : a \mapsto (e, a)$ so $\pi \phi = id_H$. 

2
b). All the subgroups of $Q$ are normal so every semi-product would be direct product, but $Q$ is not abelian. $1 \rightarrow (-1) \rightarrow Q \xrightarrow{x \mapsto x^2} Klein \rightarrow 1$.

4

a). Let $H(k)$ denote the Heisenberg subgroup. Note $H(k) \subset GL_3(k)$ as a subset.

Now the identity is in $H(k)$, since we may take $a = b = c = 0$, and that $H(k)$ is closed under composition and under taking inverses: the composition of two elements is given by

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & b + b' + ac' \\ 0 & 1 & c + c' \\ 0 & 0 & 1 \end{pmatrix}$$

and inverses may be obtained by taking $a' = -a$, $c' = -c$ and $b' = ac - b$ in the above. Hence $H(k)$ is a subgroup of $GL_3(k)$, as claimed.

b). We certainly have $H \subset H(k)$ as a subset, and $H$ contains the identity; moreover, from the above computation, $H$ is closed under composition ($a = a' = 0 \implies a + a' = 0$) and inverses ($a = 0 \implies -a = 0$), so it is a subgroup of $H(k)$.

We may verify that it is isomorphic to $k^2$ by the isomorphism

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto b, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto c.$$  

$H$ is a normal subgroup of $H(k)$, since it is the kernel of the group map $H(k) \rightarrow k$ given by $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto a$.

c). $\{id\} \subset K \subset H(k)$ in the category of sets; from the above computation, $K$ is closed under composition ($b = b' = c = c' = 0 \implies b + b' + ac' = c + c' = 0$) and inverses ($b = c' = 0 \implies -c = ac - b = 0$), so it is a subgroup of $H(k)$.

We may verify that it is isomorphic to $k$ by the isomorphism $\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto a$.

$K$ is a not a normal subgroup of $H(k)$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & -a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin K$$

for $a \neq 0$. 

3
d). Denote $G$ as the Heisenberg group. Notice that together they generate $G$:

\[
\begin{pmatrix}
1 & a & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 & b - ac \\
0 & 1 & c \\
0 & 0 & 1
\end{pmatrix}
= 
\begin{pmatrix}
1 & a & b \\
0 & 1 & c \\
0 & 0 & 1
\end{pmatrix}
\]

So $G = HK, H \triangleleft G, H \cap K = I$ so we have direct product. The action must be by conjugation $a \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ya \\ y \end{pmatrix}$.

e). $\mathbb{F}_2 \cong C_2, \mathbb{F}_2^2 = \text{Group of order 4}$, So $G$ is of order 8. $G$ is not abelian so either $D_4$ or $Q$.

Since $\mathbb{F}_2^2$ already contains 3 elements of order 2, this can’t be $Q$.

f). $\mathbb{H}(\mathbb{F}_p)$

5

a). $|D_q| = 2q$ and we have a 2-Sylow of the reflection $\langle t \rangle$, and the rotation $\langle r \rangle$ is a q-sylow.

b). We may characterize $\text{GL}_n(\mathbb{F}_p)$ as the group of $n \times n$ matrices of full rank over $\mathbb{F}_p$. We may count these as follows: there are $p^n - 1$ choices for the first column (it can be any nonzero column), $p^n - p$ choices for the second column (it can be anything which is not a multiple of the first column), $p^n - p^2$ choices for the third column (anything not in the span of the first two columns), etc., up to $p^n - p^{n-1}$ choices for the last column; hence

$$|\text{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

and in particular $p^{1+\cdots+(n-1)} = p^{\binom{n}{2}}$ divides $|\text{GL}_n(\mathbb{F}_p)|$ and so we will be done if we can show that the subgroup of upper triangular matrices with ones on the diagonal has cardinality $p^{\binom{n}{2}}$; but this is clear since there are $p$ choices for each of the $1 + \cdots + (n - 1) = \binom{n}{2}$ matrix entries above the diagonal (note that all upper triangular matrices with ones on the diagonal have determinant one and are already invertible, and we have no further restrictions.)

6

a). By Lagrange’s theorem, $p^t n \mid |G|$; in particular $p^t \mid |P|$. Let $|P| = p^{t+k}$ where $k \geq 0$.

Observe $|G| = |P| \cdot \sum_{Y \text{ orbit }} |Y|$, where we sum over the orbits when $H$ acts on $G/P$.

If every orbit has cardinality divisible by $p$, then $|G|$ is divisible by $|P| \cdot p = p^{t+k+1}$, which contradicts that $P$ is a $p$-Sylow group of $G$.

Hence there is some orbit $X$ when $H$ acts on $G/P$ of cardinality not divisible by $p$. 

b). Let $x \in X$. By the stabilizer-orbit theorem, $|\text{Stab}_H(x)| \cdot |X| = |H|$. Since $p^t$ divides $|H|$ but not $|X|$, we must have $p^t \mid |\text{Stab}_H(x)|$ (since the integers form a UFD.)

c). Let $x \in X$. If $h \in \text{Stab}_H(x)$, then $hx = x$; but now recall that $x$ is a coset of $G/P$ (if $P$ is not normal, replace “coset” with “left coset”), so we may also say, for any $y$ in this coset, $yh^{-1} \in P$. Since this holds for all $h \in \text{Stab}_H(x)$, we may deduce that $yHy^{-1} \subset P$, i.e. $H$ is conjugate (in $G$) to a subgroup of $P$.

Any subgroup of $P$ has order a power of $p$ (by Lagrange’s theorem) and so $\text{Stab}_H(x)$ has order a power of $p$.

d). Let $G$ be a finite group with a $p$-Sylow subgroup $P$, and let $H$ be a subgroup of $G$ of order $p^tn$ as above; suppose further that $p \nmid n$.

From the above, we have a subgroup $S \leq H$ (a stabilizer of a certain orbit $X$ of the action of $H$ on $G/P$) whose order divisible by $p^t$ [from (b)] and whose order is a power of $p$ [from (c)]. Since $|S|$ divides $|H| = p^tn$ from Lagrange’s theorem, we may conclude that $|S| = p^t$, i.e. $S$ is a $p$-Sylow subgroup of $H \leq G$.

Since $H$ may be any subgroup of $G$ in the above, we are done.

e). Any group $G$ of order $n$ acts on the vector space $\mathbb{F}_p^n$ as follows: choose a basis $\mathcal{B}$ of $\mathbb{F}_p^n$ and label them with the elements of the group, i.e. choose a bijection between $\mathcal{B}$ and $|G|$; then let $G$ act on the elements of $\mathcal{B}$ by left-multiplication (of the corresponding labels) and extend this action linearly to all of $\mathbb{F}_p^n$.

This produces a group map $G \to \text{GL}_n(\mathbb{F}_p)$. This map is injective—i.e. an embedding, as desired—since the left-multiplication action described above is faithful (indeed, free, i.e. the action of any non-identity element has no fixed points.)

f). (appears as second (e) on Homework)

From the previous part (e), every finite group $G$ embeds in $\text{GL}_n(\mathbb{F}_p)$ for $n = |G|$ and for every $p$. From #4(b), $\text{GL}_n(\mathbb{F}_p)$ has a $p$-Sylow subgroup. From part (d), $G$ also has a $p$-Sylow subgroup.

g). (appears as (f) on Homework)

Fix $G$ be a finite group and let $P_1$ and $P_2$ be two $p$-Sylow subgroups of $G$.

If we run the above argument [(a) through (d)] with $P = P_1$ and $H = P_2$, then we see, by considerations of cardinality, that the stabilizer in question must be all of $H = P_2$, which is in turn conjugate to a subgroup of $P_1$; again, by considerations of cardinality, we may then conclude that $P_2$ is conjugate to $P_1$.

7

a). We may represent $S_n$ by the set of $n \times n$ permutation matrices over $k$: if we let $(e_1, \ldots, e_n)$ denote a basis of $k^n$, $S_n$ acts naturally on $\{e_1, \ldots, e_n\}$ as a set of $n$ objects (by permuta-
tions), and this extends uniquely (linearly) to an action of $S_n$ on $k^n$, i.e. a group map $S_n \to \text{GL}_n(k)$.

We may verify that this group action is faithful, i.e. the group map $S_n \to \text{GL}_n(k)$ is injective, and hence $S_n$ may be viewed as a subgroup of $\text{GL}_n(k)$ (by taking its isomorphic image in $\text{GL}_n(k)$ under this map.)

If we fix $(e_1, \ldots, e_n)$ to be the standard basis for $k^n$, the transposition $(ij)$ corresponds to the elementary matrix obtained from the identity matrix by switch columns (or rows) $i$ and $j$. Notice that each transposition has a determinant of -1. So define $\text{Det} : S_n \to \{\pm 1\}$ and observe that this is a group map, and $A_n$ is its kernel. Thus, $A_n \leq S_n$.

b). We remark that alternating $n$-linear maps are skew $n$-linear.

By skew-multilinearity and by the characterisation in (a) of the matrices representing transpositions, we note that $\text{det}(\tau_{ij}) = -1$ for any transposition $\tau_{ij} := (ij)$.

Since $\text{det} : S_n \subset \text{GL}_n(k) \to k^*$ is a group map, the determinant of a product $\sigma$ of $n$ transpositions is given by the product of their determinants, i.e. $\text{det}(\sigma) = (-1)^n$. In particular, $\text{det}(\sigma) = 1$ if $\sigma$ can be written as a product of an even number $n$ of transpositions, and $\text{det}(\sigma) = -1$ if $\sigma$ can be written as a product of an odd number of transpositions.

If there is more than one way to write $\sigma$ as a product of transpositions, then we must conclude that the numbers of transpositions in each of these products has the same parity, since the above argument must hold and $\text{det}$ is a well-defined function.

c). $A_n$ is normal. Take $B = \langle (12) \rangle$. Their intersection is trivial. All we need to show is $S_n = A_n B$. Enough to show that we can create any cycle $(ab)$. For $a \neq 1, 2, b \neq 1, 2$ Use $(ab)(12) \cdot (12)$. For $(12)$ - done. For $(1a)$ or $(2a)$ use $(12)(2a) \cdot (12)$ or $(12)(1a) \cdot (12)$ respectively.