Math 71: Algebra Fall 2022

PSET 6 — 2022-11-11

Prof. Voight Student: Amittai Siavava

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

- (a) Abstract Algebra by David S. Dummit & Richard M. Foote.
- (b) Algebra by Jacob K. Goldhaber & Gertrude Ehrlich

Problems

1. (DF 4.5.4)

For each of $G = D_{12}$ and $G = S_3 \times S_3$, do the following:

- (a) Exhibit all Sylow *p*-subgroups.
 - (a) D_{12}

 D_{12} has order $12 = 2^2 \cdot 3$.

(i) p = 2:

 $n_2 \mid 3 \land n_2 \equiv 1 \pmod{2} \implies n_2 \in \{1,3\}$ and each Sylow 2-subgroup has order 12/3 = 4. Since no singular element in D_{12} has order 4, let's consider the subgroups generated by pairs of elements of order 2. we can find them as groups generated by pairs of order-2 elements. One such pair is $\{r^3, s\}$, generating the subgroup $\{\varepsilon, r^3, s, sr^3\}$.

The other subgroups can be discovered by conjugation, to give the full set:

$$\langle r^3, s \rangle = \{\varepsilon, r^3, s, sr^3\}$$
$$\langle r^3, sr \rangle = \{\varepsilon, r^3, sr, sr^4\}$$
$$\langle r^3, sr^2 \rangle = \{\varepsilon, r^3, sr^2, sr^5\}$$

Thus, $n_2 = 3$ and D_{12} has 3 unique Sylow 2-subgroups, each having order 4. All the Sylow 2-subgroups are isomorphic to V_4 .

By Sylow's theorem, we see that $3 \mid 3 \land 3 \equiv 1 \pmod{2}$.

(ii) p = 3:

$$n_3 \mid 2^2 \text{ and } n_3 \equiv 1 \pmod{3} \implies n_3 \in \{1, 4\}.$$

Since $r^2 \in D_{12}$ has order 3, We can generate a Sylow 3-subgroup using r^2 as the generator. Thus, we have the subgroup

$$\langle r^2 \rangle = \{ \varepsilon, r^2, r^4 \}$$

Under conjugation, we notice that r^2 is centralized by r. We also notice that r^2 and r^4 are conjugate under all elements $sr^k, r \in \mathbb{Z}$. Take conjugation by sr^2 as an example:

$$sr^{2} \cdot r^{2} \cdot sr^{2} = sr^{4} \cdot sr^{2}$$

$$= s \cdot sr^{-4} \cdot r^{2}$$

$$= r^{-2}$$

$$= r^{4}$$

Therefore, the group generated by r^2 is normal in D_{12} . Since **all** Sylow 3-subgroups are conjugates, and all conjugates of elements in $\langle r^2 \rangle$ are in $\langle r^2 \rangle$, it must be that $\langle r^2 \rangle$ is the only Sylow 3-subgroup of D_{12} .

Thus, $n_3=1$ and D_{12} has 1 unique Sylow 3-subgroup, each having order 3.

By Sylow's theorem, we see that $1 \mid 4 \land 1 \equiv 1 \pmod{3}$.

- (b) $S_3 \times S_3$ $S_3 \times S_3 \text{ has order } 36 = 2^2 \cdot 3^2.$
 - (i) p=2: $n_2\mid 3^2 \ \land \ n_2\equiv 1 \pmod 2 \implies n_2\in \{1,9\} \ \text{and each Sylow 2-subgroup has order}$ 36/9=4.

Since $4 \nmid 6$, no order 4 element exists in S_3 . Since the order of direct products is equivalent to the lcm of the orders of the direct group, there therefore cannot exist an element of order 4 in $S_3 \times S_3$ (that would have been a potential generator for a Sylow 2-subgroup). Next, we can consider the groups generated by pairs of elements of order 2. In $S_3 \times S_3$, such elements will be pairs constituted of the identity element and a transposition.

The Sylow 2-subgroups are:

$$\langle [\varepsilon, (1\,2)], [(1\,2), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (1\,2)], [(1\,2), \varepsilon], [(1\,2), (1\,2)] \} \tag{0.1}$$

$$\langle [\varepsilon, (12)], [(13), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (12)], [(13), \varepsilon], [(13), (12)] \}$$

$$(0.2)$$

$$\langle [\varepsilon, (1\,2)], [(2\,3), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (1\,2)], [(2\,3), \varepsilon], [(2\,3), (1\,2)] \} \tag{0.3}$$

$$\langle [\varepsilon, (1\,3)], [(1\,2), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (1\,3)], [(1\,2), \varepsilon], [(1\,2), (1\,3)] \}$$

$$\tag{0.4}$$

$$\langle [\varepsilon, (13)], [(13), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (13)], [(13), \varepsilon], [(13), (13)] \}$$

$$(0.5)$$

$$\langle [\varepsilon, (13)], [(23), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (13)], [(23), \varepsilon], [(23), (13)] \}$$

$$(0.6)$$

$$\langle [\varepsilon, (23)], [(12), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (23)], [(12), \varepsilon], [(12), (23)] \}$$

$$(0.7)$$

$$\langle [\varepsilon, (23)], [(13), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (23)], [(13), \varepsilon], [(13), (23)] \}$$

$$(0.8)$$

$$\langle [\varepsilon, (23)], [(23), \varepsilon] \rangle = \{ [\varepsilon, \varepsilon], [\varepsilon, (23)], [(23), \varepsilon], [(23), (23)] \}$$

$$(0.9)$$

We can confirm that these subgroups are conjugate to each other, but the entire set is closed under conjugation. Therefore, there are 9 Sylow 2-subgroups in $S_3 \times S_3$.

By Sylow's theorem, we see that $9 \mid 9 \land 9 \equiv 0 \pmod{2}$.

(ii) p=3: $n_3\mid 2^2$ and $n_3\equiv 1\pmod 3\implies n_3\in\{1,4\}$. In this case, each subgroup will have 9 elements. We can generate a Sylow 3-subgroup using an order-3 element as a generator. The only such groups are $(1\ 2\ 3)$ and $(1\ 3\ 2)$. The Sylow 3-subgroup is the group $G=\langle (1\ 2\ 3), (1\ 2\ 3)\rangle$.

$$\left\{ \begin{array}{l} [\varepsilon,\varepsilon], [\varepsilon,(1\,2\,3)], [\varepsilon,(1\,3\,2)], \\ [(1\,2\,3),\varepsilon], [(1\,2\,3),(1\,2\,3)], [(1\,2\,3),(1\,3\,2)], \\ \\ [(1\,3\,2),\varepsilon], [(1\,3\,2),(1\,2\,3)], [(1\,3\,2),(1\,3\,2)] \end{array} \right\}$$

In this case, each generator in the direct product generates a group of order 3, isomorphic to Z_3 . The Sylow 3-subgroup is isomorphic to $Z_3 \times Z_3$ and $C_3 \times C_3$.

By Sylow's theorem, we see that $4 \mid 4 \land 4 \equiv 1 \pmod{3}$.

(b) Verify the conclusion of Sylow's theorem in each case (i.e., $n_p(G) \equiv 1 \pmod{p}$ and $n_p(G) \mid m$).

Demonstrated above.

(c) In each case where a Sylow p-subgroup $P \subseteq G$ is normal, describe the group G/P up to isomorphism (i.e., what more recognizable group is it isomorphic to?).

Demonstrated above.

- 2. (DF 4.5.10)
 - (a) Let F be a field and let $n \geq 1$. Show that

$$\operatorname{SL}_n(F) := \{ A \in \operatorname{GL}_n(F) : \det(A) = 1 \}$$

is a normal subgroup of $GL_n(F)$, called the special linear group. [Hint: kernel of determinant.]

(a) $SL_n(F) \subseteq GL_n(F)$:

By definition, det(A) = 1 for all $A \in SL_n(F)$.

Also, by definition, $det(M) \neq 0$ for all $M \in GL_n(F)$.

Since $1 \neq 0$, it follows that $SL_n(F) \subseteq GL_n(F)$.

(b) $SL_n(F)$ contains the identity of $GL_n(F)$:

Under matrix multiplication, the identity matrix in $GL_n(F)$ is the matrix

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

where 0 is the additive identity, and 1 is the multiplicative identity.

Since the determinant of a diagonal matrix is the product of its diagonal entries, in this case $\det(I_n) =$

$$1 \cdot 1 \cdot \cdot \cdot 1 = 1$$
.

Therefore, $I_n \in \mathrm{SL}_n(F)$.

(c) $SL_n(F)$ is closed under multiplication:

The determinant of a product of matrices is the product of the determinants.

Taking $A, B \in SL_n(F)$, we have det(A) = 1 and det(B) = 1.

Therefore, $det(AB) = det(A) det(B) = 1 \cdot 1 = 1$ and $AB \in SL_n(F)$.

(d) $SL_n(F)$ is closed under inversion:

The determinant of the inverse of a matrix is the inverse of the determinant.

Taking $A \in \mathrm{SL}_n(F)$, Consider A^{-1} as the inverse of A.

By matrix properties, $\det(A^{-1}) = \frac{1}{\det(A)}$.

Since det(A) = 1, $det(A^{-1}) = 1$ and $A^{-1} \in SL_n(F)$.

(e) $SL_n(F)$ is normal in $GL_n(F)$.

For $SL_n(F)$ to be normal in $GL_n(F)$, its conjugates must be in $SL_n(F)$.

Let
$$S \in \mathrm{SL}_n(F)$$
, $\det(S) = 1$ and $G \in \mathrm{GL}_n(F)$, $\det(G) = g \neq 0$.

Consider the conjugate GSG^{-1} .

By matrix properties, $\det(GSG^{-1}) = \det(G) \cdot \det(S) \cdot \det(G^{-1}) = g \cdot 1 \cdot \frac{1}{g} = 1$. Therefore, $GSG^{-1} \in \mathrm{SL}_n(F)$, and $\mathrm{SL}_n(F)$ is normal in $GL_n(F)$.

(b) Let $F = \mathbb{Z}/p\mathbb{Z}$ for p prime. Let's write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ to remind ourselves that it is a field. Show that $\#\mathrm{GL}_2(\mathbb{F}_p) = (p^2 - 1)(p^2 - p)$. [Hint: a matrix $A \in \mathrm{M}_2(\mathbb{F}_p)$ is invertible if and only if its columns are linearly independent. So the first column must be nonzero, and then ...]

Consider the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \subset M_2(\mathbb{F}_p)$$

For the matrix to be invertible, its first column must be nonzero.

First, observe that $\#(\mathbb{F}_p) = p$ (since p is prime). If unrestricted, each position in A could be filled up by p different values. and the entire matrix could be filled by p^4 different *combinations* of values from \mathbb{F}_p . In our case, A must be invertible, so its first column must be nonzero. Let's consider the ordered pairs (a, c) to be the first column and (b, d) to be the second column.

Then, $(a, c) \neq (0, 0)$. This takes away one option for the first column, leaving $p^2 - 1$ options (p options for a and p options for c multiply to p^2 , take away (0, 0) to give $p^2 - 1$ remaining options).

Next, the second column (b,d) must not be a linear multiple of the first column (a,c). There are p multiples of any pair (a,c), so there are p options that are invalid for the pair (b,d). This leaves p^2-p options.

Therefore, the total number of distinct invertible matrices will be $(p^2 - 1)(p^2 - p)$.

(c) Compute $\#\operatorname{SL}_2(\mathbb{F}_p)$ as a polynomial in p, then the numerical value for p=2,3.

By the same reasoning above, we have $p^2 - 1$ options for the first column.

However, once the pair (a,c) has been fixed, we must now pick the pair (b,d) such that $ad \times bc = 1$. We can pick any of p options for d, but only a single option for b thereafter.

This gives a total of $p(p^2-1)$ possible combinations for (and, therefore, elements in) $\mathrm{SL}_n(\mathbb{F}_p)$.

(a) p = 2:

$$p(p^2 - 1) = 2 \cdot 3 = 6$$

(b) p = 3:

$$p(p^2 - 1) = 3 \cdot 8 = 24$$

(d) Show that the subgroup $P \leq \operatorname{SL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to Q_8 . [Hint: map i,j to the given generators; it's not too many matrix multiplications, because -1.]

Let P be the subgroup generated by the matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
 and $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$

Through matrix multiplication, we see that:

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

$$A \cdot B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = C$$

$$A \cdot C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -B$$

$$B \cdot A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$$

$$B \cdot B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

$$B \cdot C = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = A$$

$$C \cdot A = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -A$$

$$C \cdot C = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

First, notice that *P* has 8 elements generated by *A* and *B*:

$$P = \{\pm I, \pm A, \pm B, \pm C \colon C = AB\}$$

Suppose $A \sim i, B \sim j, C \sim k$, and $I \sim 1$. Then:

Amittai, S

$$i \cdot i = -1$$

Math 71: Algebra

$$i \cdot j = k$$

$$i \cdot k = -j$$

$$j \cdot i = -k$$

$$j \cdot j = -1$$

$$j \cdot k = i$$

$$k \cdot i = j$$

$$k \cdot j = -i$$

$$k \cdot k = -1$$

We see that ${\cal P}$ under matrix multiplication is isomorphic to ${\cal Q}_8$ under multiplication.

(e) Continuing part (d), show that P is a Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, and conclude that $\mathrm{SL}_2(\mathbb{F}_3) \not\simeq S_4$.

As we saw in part (c) above, $SL_2(\mathbb{F}_3)$ has 24 elements.

 $24 = 2^3 \cdot 3$, so $SL_2(\mathbb{F}_3)$ has a Sylow 2-subgroup.

Precisely, $n_2 \mid 3$ and $n_2 \equiv 1 \pmod{2}$, which implies that either $n_2 = 1$ or $n_2 = 3$. Furthermore, Sylow 2-subgroups must have size 24/3 = 8. Since P has order 8, it is a Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$. Since we demonstrated in part (e) above that P is isomorphic to Q_8 , it must follow that P is closed under conjugation! Therefore, P must be the only Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$.

In contrast, S_4 has 24 elements, and 16 of those elements have an order that divides 8. These are:

- 1 (order 1)
- (12) (order 2)
- (13) (order 2)
- (14) (order 2)
- (23) (order 2)
- (24) (order 2)
- (34) (order 2)
- (12)(34) (order 2)
- $(1\,3)(2\,4)$ (order 2)
- (14)(23) (order 2)
- (1234) (order 4)
- (1243) (order 4)
- (1324) (order 4)
- (1342) (order 4)
- (1 4 2 3) (order 4)
- (1432) (order 4)

These elements must occur in the Sylow 2-subgroups of S_4 , yet each Sylow 2-subgroup of S_4 must have size 8. Therefore, S_4 cannot have a single Sylow 2-subgroup — it must have 3, and $\mathrm{SL}_2(\mathbb{F}_3) \not\simeq S_4$ because $\mathrm{SL}_2(\mathbb{F}_3)$ has 1 Sylow 2-subgroup.

3. (DF 4.5.13)

(a) Prove that a group G of order #G=21 has a normal Sylow 7-subgroup.

$$21 = 3 \cdot 7.$$

(a) $n_7 \mid 3 \land n_7 \equiv 1 \pmod{7} \implies n_7 = 1$.

In this case, the Sylow 7-subgroup will have order 3. However, there is only one group of order 3 up to isomorphism, that is C_3 , which is abelian.

We know that the conjugates of a Sylow p-subgroup are also Sylow p-subgroups. In this case, there is only one Sylow 7-subgroup, C_3 , and its conjugates must therefore be equal to itself. This implies that the subgroup is normal in G.

(b) Prove that a group G of order #G = 56 has a normal Sylow p-subgroup for some prime p dividing its order. [Hint: count elements of order 7, arguing that distinct Sylow 7-subgroups only intersect in the identity.]

FIrst, Cauchy's theorem tells us that G must have an element of order 7, and an element of order 2. Given $a \in G$ of order 7, then the entire set generated by a, that is $\{a^i : 1 \le i \le 6\}$, will have order 7 (since 7 is prime). Thus, there are a total of 7 elements of order 7 in G which, together with the identity, form a subgroup of order 8.

First, observe that $56 = 2^3 \cdot 7$. We know $n_7 \mid 8$ and $n_7 \equiv 1 \pmod{7}$, which implies that $n_7 = 1$. Thus, there is only one Sylow 7-subgroup in G, and it must have 56/7 = 8 elements. There are also only 7 elements of order 7 in G, which, together with the identity, form a subgroup of order 8. Therefore, the Sylow 7-subgroup is the subgroup generated by the elements of order 7 in G.

As demonstrated in part (a) above, a singular Sylow p-subgroup must be normal in G, since its conjugates must also be Sylow p-subgroups, which in this case means its conjugates must be the group itself.

4. (DF 5.1.1)

centers.

Let G_1, G_2 be groups. Show that the center of the direct product is the direct product of the centers, i.e.,

$$Z(G_1 \times G_2) = Z(G_1) \times Z(G_2) \le G_1 \times G_2.$$

Conclude that a direct product $G_1 \times G_2$ is abelian if and only if G_1 and G_2 are abelian.

Let $a=(a_1,a_2)$ and $b=(b_1,b_2)$ be two elements in $G_1\times G_2$. Furthermore, suppose $a,b\in Z(G_1\times G_2)$. This implies that

$$ab = ba \implies (a_1b_1, a_2b_2) = (b_1a_1, b_2a_2) \implies a_1b_1 = b_1a_1 \land a_2b_2 = b_2a_2$$

which implies that $a_1, b_1 \in Z(G_1)$ and $a_2, b_2 \in Z(G_2)$. Thus, we see that whenever $a = (a_1, a_2) \in (G_1 \times G_2)$ is in the center $Z(G_1 \times G_2)$, then it must hold that $a_1 \in Z(G_1)$ and $a_2 \in Z(G_2)$, and the center of the direct-product is, in fact, equivalent to the direct-product of the respective

If a direct product $G_1 \times G_2$ is abelian, then its center covers the entire group and therefore all elements in G_1 must be in $Z(G_1)$ and all elements in G_2 must be in $Z(G_2)$.

Therefore, G_1 and G_2 must be abelian if $G_1 \times G_2$ is abelian.

5. (DF 5.2.1) For each of parts (a) and (b), give the lists of invariant factors and elementary divisors for all abelian groups of the specified order n—matching them up—and then count the number of abelian groups of order n up to isomorphism.

(a)
$$n = 105$$

First, note that $105 = 3 \cdot 5 \cdot 7$.

Since all the primes are distinct, the only invariant factor is $n_1 = 105$, and the only abelian group of order 105 is Z_{105} . For proof, consider an invariant factor n_1 . We know that $3 \cdot 5 \cdot 7 = n$ must divide n_1 , and that n_1 must divide n. Therefore, $n_1 = n$.

There is, therefore, 1 abelian group of order 105 up to isomorphism.

(b) n = 540

Note that $540 = 2^2 \cdot 3^3 \cdot 5$.

For each every first factor n_1 , we must have that $2 \cdot 3 \cdot 5 \mid n_1$.

Then, for every factor n_1 , we seek a factor n_2 such that $n_2 \mid n_1 \wedge n_1 n_2 \mid n_1 \wedge n_2 \mid n_2 \wedge n_1 \mid n_2 \wedge n_2 \mid n_2 \wedge n_2 \mid n_2 \wedge n_2 \wedge n_2 \mid n_2 \wedge n_2$

	Invariant Factors	Abelian Groups
$2^2 \cdot 3^3 \cdot 5$		Z_{540}
$2\cdot 3^3\cdot 5$	2	$Z_{270} imes Z_2$
$2^2 \cdot 3^2 \cdot 5$	3	$Z_{180} imes Z_3$
$2 \cdot 3^2 \cdot 5$	$2 \cdot 3$	$Z_{90} imes Z_6$
$2^2 \cdot 3 \cdot 5$	3^2	$Z_{60} imes Z_9$
$2 \cdot 3 \cdot 5$	$2 \cdot 3^2$	$Z_{30} imes Z_{18}$

Therefore, there are 6 abelian groups of order 540 up to isomorphism.