# Assorted Algebra Exercises

Exercise 1
Let $K \triangleleft H$ and $H \triangleleft G$. Show that if $K$ is a characteristic subgroup of $H$ (that is, $\phi(K) = K$ for every automorphism $\phi$ of $H$), then $K \triangleleft G$.

Exercise 2
Let $R$ be any ring with additive identity $0$ and unity $1$. Let $G$ be the group of matrices $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in R \right\}$ under matrix multiplication.

a. Show that $G$ is a group and hence construct a nonabelian group $H$ of order $27$. That is, explicitly define a group $H$ and prove it is nonabelian and has order $27$.

b. Let $H$ be the group constructed in part (a). Prove that $Z(H) \cong \mathbb{Z}/3\mathbb{Z}$. Then list all the elements of $Z(H)$.

Exercise 3
Prove that $\mathbb{Z} \times G$ is cyclic if and only if $G$ is the trivial group.

Exercise 4
Let $C_{13}$ be the cyclic group of order $13$. How many subgroups does $C_{13} \times C_{13}$ have?

Exercise 5
Prove $F = \mathbb{F}_3[X]/\langle X^4 + 1 \rangle$ is a field. Then find the multiplicative order of $X^2 + 1$ in $F$.

Exercise 6
Let $q$ be a prime power (so $\mathbb{F}_q$ is a field) and $n \in \mathbb{N}$.

a. By considering the linear independence of columns (or rows) of matrices in $\mathrm{GL}(n, \mathbb{F}_q)$, show that $\left|\mathrm{GL}(n, \mathbb{F}_q)\right| = (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$.

b. Using the fundamental theorem of group homomorphisms, find the order of $\mathrm{SL}(n, \mathbb{F}_q)$.

Exercise 7
Let $m, n$ be integers greater than $1$. Prove that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$. *Hint: Recall* $\gcd(m, n)\,\mathrm{lcm}(m, n) = mn$ *for positive integers* $m, n$.

Exercise 8
Let $D_n$ be the dihedral group of order $2n$ and let $C_n$ be the cyclic group of order $n$. You may assume that $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4$, and $Q_8$ are the only groups of order $8$ up to isomorphism. Determine how many copies of each of these groups are inside $C_4 \times D_3$ and hence find all order $8$ subgroups of $C_4 \times D_3$. Are they normal? Hints are provided below. *Challenge: Do not use the Sylow theorems.*

Hint 1:
Consider the orders of elements and/or subgroups in $C_4 \times D_3$. In particular, it may help to find all order $4$ and order $2$ elements in $C_4 \times D_3$.

Hint 2:
Note that $Q_8, D_4$, and $C_8$ all contain $C_4$.

Exercise 9
Recall that the group $\mathbb{Z}/n\mathbb{Z}$ is generated by $k \in \mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(k, n) = 1$. Use this result to prove the following statement, which is related to Bezout's lemma.

Let $m, n$ be positive integers such that $\gcd(m, n) = 1$. Then there exist integers $a, b \in \mathbb{Z}$ (not necessarily positive) such that $am + bn = 1$.

Exercise 1

Let $g \in G, k \in K$. Consider the inner automorphism $\phi: G \to G, \phi(t) = g^{-1}tg$. Then $\phi|_H$, which we denote $\varphi$, is an automorphism of $H$ and thus $\varphi(K) = K$. Note $\varphi^{-1}$ is also an automorphism of $H$ so $\varphi^{-1}(K) = K$ as well. Then $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = g(g^{-1}kg)g^{-1} = k$. Applying $\varphi^{-1}$ to both sides, $gkg^{-1} = \varphi^{-1}(k) \in K$. Hence $K \triangleleft G$.

Exercise 2

Taking $a = b = c = 0$ we see the identity matrix is in $G$ and is clearly the identity of $G$. To prove closure, note $\begin{bmatrix}1 & a_1 & b_1\\0 & 1 & c_1\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & a_2 & b_2\\0 & 1 & c_2\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a_2+a_1 & b_2+a_1c_2+b_1\\0 & 1 & c_2+c_1\\0 & 0 & 1\end{bmatrix} \in G$. To prove inverse exists, we can take $\begin{bmatrix}1 & a_2+a_1 & b_2+a_1c_2+b_1\\0 & 1 & c_2+c_1\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$ in the above matrix equation and solve for $a_2, b_2, c_2$ to see that $\begin{bmatrix}1 & -a_1 & a_1c_1-b_1\\0 & 1 & -c_1\\0 & 0 & 1\end{bmatrix} \in G$ is the inverse of $\begin{bmatrix}1 & a_1 & b_1\\0 & 1 & c_1\\0 & 0 & 1\end{bmatrix}$. Matrix multiplication is associative. Hence $G$ is a group.

Now define $H = \left\{\begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} : a, b, c \in \mathbb{F}_3\right\}$, which we now know is a group. Since each $a, b, c$ could be $0, 1,$ or $2$, we have $|H| = 3 \times 3 \times 3 = 27$.

Now, since $[H : Z(H)]$ divides $|H| = 27$ (by Lagrange's theorem) and $[H : Z(H)]$ is not prime (from class equation), it must be that either $[H : Z(H)] = 9 \Leftrightarrow |Z(H)| = 3$ or $[H : Z(H)] = 27 \Leftrightarrow |Z(H)| = 1$. But $|H| = 3^3$ implies 3 divides $|Z(H)|$ (also from class equation) so in fact we must have $[H : Z(H)] = 9 \Leftrightarrow |Z(H)| = 3$. It follows that $H$ is nonabelian and $Z(H) \cong \mathbb{Z}/3\mathbb{Z}$. Alternatively, one could show $H$ is nonabelian by noting $\begin{bmatrix}1 & a_1 & b_1\\0 & 1 & c_1\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & a_2 & b_2\\0 & 1 & c_2\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a_2 & b_2\\0 & 1 & c_2\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & a_1 & b_1\\0 & 1 & c_1\\0 & 0 & 1\end{bmatrix} \Rightarrow \begin{bmatrix}1 & a_2+a_1 & b_2+a_1c_2+b_1\\0 & 1 & c_2+c_1\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a_1+a_2 & b_1+a_2c_1+b_2\\0 & 1 & c_1+c_2\\0 & 0 & 1\end{bmatrix} \Rightarrow a_1c_2 = a_2c_1$, so if we pick numbers like $a_1 = c_2 = a_2 = 1$ and $a_2 = 2$, the corresponding matrices will not commute, hence $Z(H) \neq H$ so $H$ is nonabelian.

Then, either by observation or by playing with the equation $a_1c_2 = a_2c_1$ from before, we see that $\begin{bmatrix}1 & 0 & b\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \in Z(H)$ for all $b \in \mathbb{F}_3$, and there are precisely three matrices of this form in $H$. Since we already showed $|Z(H)| = 3$, we must have

$$Z(H) = \left\{\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 1\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 2\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}\right\}$$

Exercise 3

If $G$ is trivial then clearly $\mathbb{Z} \times G$ is cyclic (since $\mathbb{Z}$ is cyclic). To prove the other implication, let $\mathbb{Z} \times G$ be cyclic and suppose towards a contradiction $G$ is nontrivial. Then any generator of $\mathbb{Z} \times G$ must be of the form $(m, g)$ where $\langle g \rangle = G$ and $\langle m \rangle = \mathbb{Z}$, and to see why, suppose $(m, g)$ generates $\mathbb{Z} \times G$ but either $\langle g \rangle \neq G$ or $\langle m \rangle \neq \mathbb{Z}$. If $\langle g \rangle \neq G$, then there exists some $k \in G$ that is not a power of $g$, so then $(0, k)$ certainly could not be generated by $(m, g)$, contradicting $(m, g)$ being a generator. If $\langle m \rangle \neq \mathbb{Z}$, the same contradiction arises.

So any generator of $\mathbb{Z} \times G$ must be $(\pm 1, g)$ where $\langle g \rangle = G$ (since $\pm 1$ are the only generators of $\mathbb{Z}$). If the generator is $(1, g)$, then consider $(2, g) \in \mathbb{Z} \times G$. So there exists $n \in \mathbb{Z}$ such that $(1, g)^n = (2, g)$, so $n(1) = 2$ and $g^n = g$. But $n(1) = 2$ implies $n = 2$, so $g^2 = g$, which implies $g = e$. But since $G = \langle g \rangle$, this implies $G$ is trivial, a contradiction. If the generator is $(-1, g)$, then consider $(-2, g) \in \mathbb{Z} \times G$ and the same contradiction will arise.

Incidentally, a slightly stronger result says that if $G$ and $H$ are groups and $G$ is infinite, then $G \times H$ is cyclic if and only if $G$ is cyclic (so $G \cong \mathbb{Z}$) and $H$ is trivial.

Exercise 4

Since $|C_{13} \times C_{13}| = 169$, by Lagrange's theorem every nonidentity element must have order $13$ and thus generates some copy of $C_{13}$ (if an element had order $169$ then the whole group would be $C_{169}$, which is obviously not $C_{13} \times C_{13}$). There are $168$ nonidentity elements and every copy of $C_{13}$ has $12$ nonidentity elements, so in all there must be $168/12 = 14$ copies of $C_{13}$ inside $C_{13} \times C_{13}$. Counting the trivial group and the whole group itself, there are $16$ subgroups total. In general, $C_p \times C_p$ has $p + 3$ subgroups for $p$ prime.

Exercise 5

To show $F$ is a field, it suffices to show $f(X) = X^4 + 1$ is irreducible over $\mathbb{F}_3$. Since $f(0) = 1, f(1) = 2, f(2) = 2$, there are no roots of $f$ in $\mathbb{F}_3$, so if there is a nontrivial factoring of $f$ it must be of two quadratic factors. Any such factoring must be $X^4 + 1 = (X^2 + aX + 1)(X^2 + bX + 1) = X^4 + (a + b)X^3 + (ab + 2)X^2 + (a + b)X + 1$ and equating coefficients leads to $a + b = 0$ and $ab + 2 = 0$. Solving simultaneously yields $b^2 = 2$ (or $a^2 = 2$) but it is easily verified that $2$ has no square roots in $\mathbb{F}_3$, so there is no quadratic factoring of $f$. Hence $f$ is irreducible over $\mathbb{F}_3$, so $F$ is the quotient of a ring by a maximal ideal, so $F$ is a field.

We have $(X^2 + 1)^2 = X^4 + 2X^2 + 1 = 2X^2$ (since $X^4 + 2X^2 + 1 = f(X) + 2X^2$). But we also have $(2X^2)^2 = X^4 = 2$ (since $X^4 = f(X) + 2$). Then $(X^2 + 1)^8 = ((X^2 + 1)^2)^4 = (2X^2)^4 = ((2X^2)^2)^2 = 2^2 = 1$. Then the order of $X^2 + 1$ must divide $8$. But we just found that $(X^2 + 1)^2 = 2X^2 \neq 1$ and $(X^2 + 1)^4 = 2 \neq 1$, so $n = 8$ is indeed the smallest integer such that $(X^2 + 1)^n = 1$. Hence $X^2 + 1$ has order $8$.

Exercise 6

For a matrix $A$ to be in $\mathrm{GL}(n, \mathbb{F}_q)$, it must be invertible, so all its columns (or rows, since row rank equals column rank) must be linearly independent. Consider the first column of $A$. Each entry has $q$ options but we cannot have all entries being zero, so there are a total of $q^n - 1$ possibiltiies for the first column. The second column must be independent of the first column, which means it cannot be a scalar multiple. There are $q$ scalars in $\mathbb{F}_q$ (including $0$) so there are $q$ scalar multiples of the first column (including the zero vector) that we cannot have as the second column, so there are $q^n - q$ possibilities for the second column. The third column cannot be a combination of the previous two columns, but again there are $q$ multiples of each of the previous columns, so there are $q^2$ different linear combinations of the previous two columns, hence $q^n - q^2$ possibilities for the third column. In general, there are $q^k$ linear combinations of $q$ columns and thus $q^n - q^k$ possibilities for the $k^{th}$ column, so $\left|\mathrm{GL}(n, \mathbb{F}_q)\right| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$. Consider now the function $\det: \mathrm{GL}(n, \mathbb{F}_q) \to \mathbb{F}_q^*$. It is well-defined since matrices from $\mathrm{GL}(n, \mathbb{F}_q)$ are invertible and thus have nonzero determinant, it is a homomorphism since the $\det$ function is multiplicative, and it is onto since for any $k \in \mathbb{F}_q^*$, the $n \times n$ diagonal matrix $(a_{ij}) \in \mathrm{GL}(n, \mathbb{F}_q)$ with $a_{11} = k$ and $a_{ii} = 1$ for all $i \neq 1$ has determinant $k$. Then $A \in \ker(\det) \Leftrightarrow \det(A) = 1 \Leftrightarrow A \in \mathrm{SL}(n, \mathbb{F}_q)$. Then by fundamental theorem of group homomorphism, we have $\mathrm{GL}(n, \mathbb{F}_q)/S\mathrm{L}(n, \mathbb{F}_q) \cong \mathbb{F}_q^*$, so

$$\left|\mathrm{SL}(n, \mathbb{F}_q)\right| = \frac{\left|\mathrm{GL}(n, \mathbb{F}_q)\right|}{\left|\mathbb{F}_q^*\right|} = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{q - 1}$$

Exercise 7

Suppose $\gcd(m, n) = 1$. We claim $(1, 1)$ generates $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We have $(1, 1)^{mn} = \big((mn) \bmod m, (mn) \bmod n\big) = (0, 0)$ so $o\big((1, 1)\big)$ divides $mn$. Then to show $o\big((1, 1)\big) = mn$ it suffices to prove $(1, 1)^k \neq 0$ for any divisor $k$ of $mn$ where $k \neq mn$. So let $k$ be such a divisor. If $0 < k < m$ or $0 < k < n$, then $(1, 1)^k = (k, k \bmod n) \neq (0, 0)$ and $(1, 1)^k = (k \bmod m, k) \neq (0, 0)$ respectively, so we are done. If $k \geq m$ and $k \geq n$, suppose towards a contradiction that $(1, 1)^k = (0, 0)$. Then $(k \bmod m, k \bmod n) = (0, 0)$, so $k \bmod m = k \bmod n = 0$. Then $m|k$ and $n|k$. Since $k \geq m$ and $k \geq n$, we can conclude $\mathrm{lcm}(m, n) \leq k < mn$. But $\gcd(m, n) = 1$ implies $\mathrm{lcm}(m, n) = mn$, so we have a contradiction. Hence $o\big((1, 1)\big) = mn$, so $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic (and thus isomorphic to $\mathbb{Z}/(mn)\mathbb{Z}$ since they are cyclic groups of the same order).

Suppose $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by $(a, b)$, so $o\big((a, b)\big) = mn$. If $\gcd(m, n) > 1$, then $\mathrm{lcm}(m, n) = mn/\gcd(m, n) < mn$. But certainly $(a, b)^{\mathrm{lcm}(m,n)} = (0, 0)$ since $\mathrm{lcm}(m, n)$ is a multiple of both $m$ and $n$. But this contradicts $o\big((a, b)\big) = mn$. So it must be that $\gcd(m, n) = 1$.

Exercise 8

We will use $\mathbb{Z}/4\mathbb{Z}$ to represent $C_4$ and $D_3 = \langle f, g : f^3 = g^2 = e, gf = f^2 g \rangle$. It is apparent enough that $C_4 \times \langle f^k g \rangle$ is a subgroup isomorphic to $C_4 \times C_2$ for $k = 0, 1, 2$, and there are no other copies of $C_4 \times C_2$ since $D_3$ has no $C_4$ subgroups and $\langle f^k g \rangle$, $k = 0, 1, 2$ are its only $C_2$ subgroups. So there are precisely three copies of $C_4 \times C_2$ in $C_4 \times D_3$.

**EITHER:**

To show there are no copies of $C_2 \times C_2 \times C_2$, note that all seven nonidentity elements of $C_2 \times C_2 \times C_2$ have order 2. We find that $(2, e), (2, f^k g), (0, f^k g)$, $k = 0, 1, 2$ are the only order 2 elements in $C_4 \times D_3$ and there are seven of them, so any $C_2 \times C_2 \times C_2$ must consist of these seven elements and $(0, e)$. But the collection of those seven elements is not closed since composing any two distinct reflections $f^k g$ leads to a rotation, for instance, we have $(0, g) * (0, fg) = (0, f^2)$. Hence there are no copies of $C_2 \times C_2 \times C_2$ in $C_4 \times D_3$. Of course, there are other methods.

To show there are no copies of $Q_8, D_4$, or $C_8$, note that $Q_8, D_4$, and $C_8$ all contain $C_4$. But any $C_4$ inside $C_4 \times D_3$ must be $C_4 \times H$ for some $H \leq D_3$ since $D_3$ has no elements of order 4. If $C_4 \times H$ were to equal $Q_8, D_4$, or $C_8$, then $H$ would have to be order 2 for $C_4 \times H$ to have order 8, so $H = C_2$, but $C_4 \times C_2$ is not equal to $Q_8, D_4$, or $C_8$. So there are no copies of $Q_8, D_4$, or $C_8$ in $C_4 \times D_3$. Of course, $C_8$ can also be handled by arguing there are no elements of order 8 in $C_4 \times D_3$ (since $C_4$ and $D_3$ themselves have no elements of order 8), and $Q_8$ in particular can be handled with relative ease by considering its elements of order 4.

**OR:**

Since $|C_4 \times D_3| = 24$, the order 8 subgroups $C_4 \times \langle f^k g \rangle$, $k = 0, 1, 2$ are all Sylow 2-subgroups. Since Sylow $p$-subgroups are conjugate (and thus isomorphic under some inner automorphism), there can be no order 8 subgroups that are not isomorphic to $C_4 \times C_2$.

**THEN:**

Consequently, the only order 8 subgroups of $C_4 \times D_3$ are $C_4 \times \langle f^k g \rangle$ for $k = 0, 1, 2$, all isomorphic to $C_4 \times C_2$. None of them are normal as $(0, f^{k+1} g)(C_4 \times \langle f^k g \rangle)(0, f^{k+1} g)^{-1} = (0, f^{k+1} g)(C_4 \times \langle f^k g \rangle)(0, g f^{-k-1})$ which contains $(0, f^{k+1} g f^k g g f^{-k-1}) = (0, f^{k+2} g)$, but $(0, f^{k+2} g) \notin C_4 \times \langle f^k g \rangle$.

Exercise 9

Let $\gcd(m, n) = 1$. If $m = n$, then the condition $\gcd(m, n) = 1$ forces $m = n = 1$, upon which $1m + 0n = 1$ and we are done. So suppose $m \neq n$, and without loss of generality suppose $n > m$ (so $m \in \mathbb{Z}/n\mathbb{Z}$). By Euclidean division we can write $m = qn + r$ for $q \in \mathbb{Z}$ and $0 \leq r < n$. Now consider $r + 1 \in \{1, 2, .., n\}$. If $r + 1 = n$, then $m = qn + n - 1$, so $-m + (q + 1)n = 1$ and we are done. If $r + 1 \in \{1, 2, \ldots, n - 1\}$ then $r + 1 \in \mathbb{Z}/n\mathbb{Z}$, but $\gcd(m, n) = 1$ and $m \in \mathbb{Z}/n\mathbb{Z}$ together imply $m$ generates $\mathbb{Z}/n\mathbb{Z}$, so there exists $a \in \mathbb{Z}$ such that $am = r + 1$. Then $m = qn + am - 1$, so $(a - 1)m + qn = 1$ and we are done. Incidentally the converse statement is true and the proof is as follows: let $d$ be a divisor of $m$ and $n$. Then $d|m$ and $d|n$, so $d$ divides $am + bn = 1$, so $d = 1$. Then $\gcd(m, n) = 1$.