Proof Portfolio - Abstract Algebra

Sagnik Nandi

Proof 1 (Problem Set 1 Question 3)

For a, b in some group G. If $ab \neq ba$, then $aba \neq e$.

Proof: Consider that for some group G, ~~there exist~~ $a, b \in G$, such that $aba = e$, but $ab \neq ba$. Then, if $aba = e$, $(aba)b = e \cdot b = b$, and also that if $aba = e$, then $(aba)(ba) = e(ba) = ba$. But via rearangment, we have that $(ab)(aba) = ab$, as if $(aba) = e$ we will have that: $(aba)(ab) = (ab)(aba) = (ab) \cdot e = ab$, but from above we have that $ab = ababa = ba$ but $ab \neq ba$ by constrution so we have a contradiction.

Proof 2 (Problem Set 2 Question 2)

Let $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$ for this to be a subgroup we let the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$.

Then, this statement from inspection holds at $k=1$.

Then for $k+1$, we get $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

from induction assumption we get $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$$= \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$$

So by induction $\forall n \in \mathbb{Z}^+$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

For $n=0$, we get $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, which is the identity matrix.

Let $n>0$, then, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-n} = \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \right)^{-1} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1}$

By definition of matrix inverse, $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$

So for all $n \in \mathbb{Z}$ $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

Then to show that H is cyclic,

Let the all the matrices in the family $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$

thus, $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \subseteq H.$

Then for $A \in H$, $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, $a \in \mathbb{Z}$
then by the previous equations we get that

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^a \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \quad \text{so,} \quad H \subseteq \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$$

So, $H = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$

Proof 3 (Problem Set 2 Question 4)

If K is a subgroup of G, then $\phi(K)$ is a Subgroup of $\overline{G}$.

Proof: Via application of the subgroup test we have that for any group A, B is a subgroup if $\forall x,y \in B$, $xy^{-1} \in B$.

We note that Image (ϕ) is nonempty as $\exists e \in G$, such that $\phi(e) = e$.

So, consider $a, b \in$ Domain$[\phi] = G$, as ϕ is a bijection. then $\phi(a), \phi(b) \in$ Image$[\phi] = \overline{G}$. Then for $\phi(a)\phi(b)^{-1}$ we have that $\phi(b)^{-1} = \phi(b^{-1})$, so $\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1})$, so $\phi(a)\phi(b)^{-1} = \phi(ab^{-1})$. As $a, b \in K$, ab^{-1} is also in K. So, $\phi(ab^{-1}) \in \phi(K)$, so $\phi(a)\phi(b)^{-1} \in \phi(K)$, so $\phi(K)$ is a subgroup of $\overline{G}$.

Proof 4 (Problem Set 3 Question 4)

For an abelian group G with subgroup A, i.e. $A \leq G$, then we can show that G/A is also abelian.

Proof: For $x, y \in G$, let $X = xA$ and $Y = yA$.
Then by definition of coset-product we can compute to see that:

$$
\begin{aligned}
XY &= (xA)(yA) \\
&= (xy)(A) \\
&= (yx)(A) \quad \text{as } G \text{ is abelian} \\
&= (yA)(xA) \\
&= YX
\end{aligned}
$$

So, G/N is also abelian.

Note: As G is abelian, all subgroups A will be normal as theorem states that subgroup of all abelian groups is normal

Proof 5 (Problem Set 4 Question 1)

Let ϕ be a surjective homomorphismm. We let ϕ map from $G/N \longrightarrow G/M$ by the function $\phi(aN) = aM$.

ϕ is a homomorphusim as ϕ is well defined, surjective, and operation preserving.

<u>ϕ is well defined.</u>

From $aN = bN$ it follows that $ab^{-1}(N) \in N$, and as $N \leq M$, $ab^{-1}M \in M$ so, $ab^{-1}M = M$ so,

$aM = bM$ and ϕ is well defined.

So : $\phi(aN) = aM = bM = \phi(bN)$

<u>ϕ is surjective</u>

ϕ from construction is surjective as you can map any coset $aM \in G/M$ s.t. $\phi(aN) = aM$.

<u>ϕ is operation preserving</u>

$$\phi(aN\,bN) = \phi(abN) = (ab)M = aM\,bM = \phi(aN)\,\phi(bN)$$

<u>Ker ϕ</u>

Letting $\phi(aN) = M$ for some a. By defintion this means $a \in M$. So $\ker(\phi) = \{aN \in G/N,\ a \in M\} = \{aN \in M/N,\ a \in M\}$

So, $\ker(\phi) = \frac{M}{N}$

If the kernel of our homomorphism is M/N it will follow that:

(by first isomorphism theorem)

$$G/M = \phi(G/N) \cong (G/N)\ker(\phi) = (G/N)(G/M)$$

Proof 6 (Problem Set 4 Question 4)

If G is a non-abelian group of order 6, then $G \cong S_3$.

Proof: Consider an element a, of order 3 in G and element b of order 2 in G. As 3 and 2 are primes that divide 6, via application of Cauchy's Theorem we have that a and b must exist in G. So we can construct an arbitrary construction of $G = \{e, a, a^2, ba, ba^2\}$.

Note: We know that as G is non-abelian that $ab \neq ba$, so there for $ab = ba^2$, so we can compute $(ab)b = (ba^2)b = a$ and also that if $a = ba^2b$, then $a^2 = bab$. We can now use this to helpfully determine our map.

We can now consider cosets of H, where $H = \{e, b\}$. We can note that $b \cdot H = H$ as $b \cdot H = \{b \cdot h \mid h \in H\} = \{b \cdot e, b \cdot b\} = \{b, e\} = H$. We can also see that $a \cdot H = \{a \cdot h \mid h \in H\} = \{a \cdot e, a \cdot b\} = \{a, ab\} = \{ba^2b, ba^2\}$ which is $a^2b \cdot H$.
We can also see that $a^2H = \{a^2 \cdot h \mid h \in H\} = \{a^2 \cdot e, a^2 \cdot b\} = \{a^2 \cdot a^2b\} = \{bab, ba\}$. which is $ab \cdot H$. Let $H = H_0$, $aH = H_1$, and $a^2H = H_2$.

Finally we can construct a group action with $X = \{H, aH, a^2H\}$. Then $G \times X \longrightarrow X$ is a group action as $e \cdot H_n = eH_n = H_n$ for all $H_n \in X$. Also, for $\forall g_1, g_2 \in G$, $g_1g_2 H_n = g_1(g_2 H_n)$.

We then define an isomorphism ϕ, such that $\phi: G \to S_3$, where for all $g \in G$, $\phi(g)$ is the permutation $\sigma_g \in S_3$, such that if for some $i \in \text{Domain}(\sigma_g)$, $\sigma_g(i) = j$ if and only if the left coset of the action gH_{n_1} is absorbed by H_{n_2}. Where $n_1 \neq n_2$. So if $\sigma_g(i) = j$ then, $iH_{n_1} = H_{n_2}$.

Here we can explicitly define the map ϕ as $\phi(e) = (1)$, $\phi(a) = (1\,2\,3)$ $\phi(a^2) = (1\,3\,2)$, $\phi(b) = (2\,3)$, $\phi(ba) = (1\,3)$ $\phi(ba^2) = (1\,2)$.

Proof 7 (Problem Set 5 Question 4)

The annihilator, $Ann(A) = \{\forall a \in A \subseteq R, r \in R \mid ra = 0\}$ is an ideal. For subring A of R.

Proof: Consider that if $Ann(A)$ is an ideal, then for $\forall a \in Ann(A)$, $\forall r \in R$, $ra, ar \in Ann(A)$. So we can use the ideal test to show that $Ann(A)$ is an ideal of R. The ideal test states that if $\forall a, b \in Ann(A)$, $r \in R$ $a - b \in Ann(A)$ and $ra \in Ann(A)$ then $Ann(A)$ is an ideal.

Consider $\forall a \in A$, $a \cdot 0 = 0 \in Ann(A)$. So $Ann(A)$ is non-empty.

Then for arbitrary $x, y \in Ann(A)$, $r \in R$, and $a \in A$, $ax = ay = 0$ as $a \in A$, so $ax, ay \in Ann(A)$ thus, $ax = ay = 0$. There for $ax - ay = 0$, so $ax - ay = a(x-y)$, but as $a \in A$, $a(x-y) = 0$. $ax - ay = a(x-y) = 0 \in Ann(A)$

Similarly, for $r \in R$, we have that $(rx)(a) = (r)(xa) = r \cdot (0) = 0 \in Ann(A)$

So then for $x, y \in Ann(A)$, $a \in A$, $r \in R$, $x - y$ and $rx \in Ann(A)$

So, by using the ideal test $Ann(A)$ is an ideal.

Proof 8 (Problem Set 6 Question 5)

If R is a ring and I and J are 2 proper ideals of R, such that they partition R as $R = I + J$, then: $R/(I \cap J) \cong R/I \oplus R/J$.

Proof: Consider $f : R \longrightarrow R/I \oplus R/J$. Let f be be defined as 2 partial maps q and p such that $f = (f_i, f_j) : R \longrightarrow R/I \oplus R/J$. Consider f_i as the map from $R \rightarrow R/I$ and f_j as the map from $R \rightarrow R/J$. f_i sends $r \in R$ to its equivalence class $r + I$ and similar to f_i, f_j sends elents to $r + J$.
We assert that f is a surjection and that the kernel of f, $\ker(f) = I + J$.

Suppose that there exist $r_1 r_2 \in R$, $i, i_2 \in I$, $j, j_2 \in J$ such that $r = i + j$ and $r_2 = i_2 + j_2$. Then, we consider that $f_i(i+j) = f_i(r) = f_i(j)$ due to the fact that $i \in I$ and the map $f_i(i) = i + I = I$. So, $f_i(r) = f_i(i+j) = f_i(j) + I$

Similarly considering the map f_j, we have that $f_j(i_2 + j_2) = f_j(r_2) = f_j(i_2)$ this is due to the similar fact that $f_j(j_2) = j_2 + J = J$ as $j_2 \in J$. So, $f_j(i_2 + j_2) = f_j(r_2) = f_j(i_2) + J$

We use this to show that f is surjective as for $r = j$ and $r_2 = i_2$, we achieve any desired pair of the form $(x + I, y + J)$ for $x, y \in R$ via f.

The kernel of f, $\ker(f)$ is exactly all elemets in the domain of f, such that $f\{\ker f\} = (0 + I, 0 + J)$, as $0 + I$ is the identity of R/I and $0 + J$ is the associative identity of R/J. So, thus each of the partial maps f_i, f_j is respectively equal to its identity. So, $f_i(r) = 0 + I$ and $f_j(r) = 0 + J$. Which is exactly when $r \in I$ and $r \in J$, so $r \in I \cap J$.

Finally to show that f is a ring homomorphism we prove that it follows ring homomorphism properties.

Consider z_1, z_2 in R, such that for a_1, a_2 in I and b_1 and b_2 in J. $z_1 = a_1 + b_1$ and $z_2 = a_2 + b_2$.

Then
$$
\begin{aligned}
f(z_1)+f(z_2) &= f_i(b_1) + f_j(a_1) + f_i(b_2) + f_j(a_2) \\
&= f_i(b_1 + b_2) + f_j(a_1 + a_2) \\
&= f(z_1 + z_2)
\end{aligned}
$$

And also
$$
\begin{aligned}
f(z_1)f(z_2) &= [f_i(b_1) + f_j(a_1)] \cdot [f_i(b_2) + f_j(a_2)] \\
&= f_i(b_1)f_i(b_2) + f_i(b_1)f_j(a_2) + f_j(a_1)f_i(b_2) + f_j(a_1)f_j(a_2) \\
&= f_i(b_1 b_2) + f_i(b_1)f_j(a_2) + f_j(a_1)f_i(b_2) + f_j(a_1 a_2)
\end{aligned}
$$

Then we consider
$$
\begin{aligned}
f(z_1 z_2) &= f(b_1 b_2 + b_1 a_2 + a_1 b_2 + a_1 a_2) \\
&= f(b_1 b_2) + f(b_1 a_2) + f(a_1 b_2) + f(a_1 a_2)
\end{aligned}
$$

as $b_1 b_2 \in J$, $f(b_1 b_2) = f_i(b_1 b_2)$

as $b_1 \in J$ and $a_2 \in I$, $f(b_1 a_2) = f_i(b_1) f_j(a_2)$

as $b_2 \in J$ and $a_1 \in I$, $f(b_2 a_1) = f_i(b_2) f_j(a_1)$

as a_1 and $a_2 \in I$, $f(a_1 a_2) = f_j(a_1 a_2)$

So, $f(z_1 z_2) = f_i(b_1 b_2) + f_i(b_1) f_j(b_2) + f_i(b_2) f_j(a_1) + f_j(a_1 a_2) = f(z_1) f(z_2)$

So, f is a ring morphism.

As we have shown $f(f_i, f_j): R \longrightarrow R/I \oplus R/J$ is a surjective homomorphism, with kernel : $\ker f = I \cap J$. Then via the first theorem of isomorphisms we have that $R/I \cap J = R/I \oplus R/J$.

Proof 9 (Problem Set 1 Question 3)

An integral domain R satisfys the ascending chain condition if and only if every ideal of R is finitly generated.

Proof: To prove this statement we must prove that the Statement is true bi-directionally. So, we consider that if R satisfies the ascending chain condition, then every ideal of R is finitely generated.

Lemma: Assume R Satisfies ACC, then for some ideal I of R, I must be finitely generated. To show this we construt a recursive formula to generate finite ideals. We select some element x within our ideal I. If a_1 is the elemnt that generates the ideal I, then $I = \langle a_1 \rangle$. If $I \neq \langle a_1 \rangle$ then there must exist some other a_2 in the ideal. So we consider $a_2 \in I / \langle a_1 \rangle$. Then $\langle a_1, a_2 \rangle$ may be an ideal of A. If $I = \langle a_1, a_2 \rangle$ then a_1 and a_2 generat the ideal, if $I \neq \langle a_1, a_2 \rangle$ then there must exist $a_3 \in I / \langle a_1, a_2 \rangle$.

If we continue this recursive process we will see that $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle$, but $\langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle$, and $\langle a_1, a_2, a_3 \rangle \subsetneq \langle a_1, a_2, a_3, a_4 \rangle$. and so on...

So, $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \ldots$

But if R satisfies the ascending chain condition, then we cannot have an infinity ascending chain, so it must terminate at some a_n. Therefor the ideal $I = \langle a_1, a_2, a_3, \ldots a_n \rangle$, for $n \in \mathbb{N}$, is finitely generated as $n < \infty$.

We can also consider that if every ideal is finitely generated then R satisfies the ascending chain condition.

Lemma: Assume that all ideals I_n of R are finitely generated. Then if $I_1 \subsetneq I_2 \subsetneq I_3 \ldots$ is an infinite containment sequence of ideals of R Then $\bigcup_{n=1}^{\infty} I_n = I_1 \cup I_2 \cup I_3 \ldots = I$, as the union of 2 ideals is an ideal we have that I is an ideal, as theorem states that if $I_{n\in N}$ is a nested ordered family of ideals of some ring R, then $\bigcup_{n\in N} I_n$ is an ideal.

So it follows that as $I_1 \subsetneq I_2 \subsetneq I_3 \ldots$ follows the ascending chain rule, then $\bigcup_{n=1}^{\infty} I_n = I$ is also an ideal.

As I is an ideal of R, by assumption I must be terminating. So for some $n \in \mathbb{N}$, $I = \langle a_1, a_2, a_3 \ldots a_n \rangle$. Then that must mean that for all $a_n \in I$, there must also exist b_n such that $a_n \in \langle b_n \rangle$, which we will call I_{b_n}. Then if a_ℓ is the last generator of I and thus contained in a n-th ideal I_{b_n}. Consider this ideal I_ℓ which contains the terminating generator of I. Then it must follow that it contains all generators of the form a_x where $0 \leq x \leq \ell$. So, as I_ℓ contains all generators of I. I_ℓ must then equal $I, (I_\ell = I)$. So for all $i \geq \ell$, $I_i = I$.

As we have proved both directions of the finite ideal proof we have successfully shown the ascending chain condition.