Abstract Algebra

Solution to selected problems

Animesh Renanse

December 31, 2020

Answer I.2.2: Let S be a *finite semigroup* and cancellation law holds for it's elements, that is,

$$\begin{aligned} x \cdot y = x \cdot z &\implies y = z \\ y \cdot x = z \cdot x &\implies y = z \end{aligned} \tag{1}$$

Since S is a semigroup, hence it is already associative. Consider $x^n = x \cdot x \cdot \ \dots \ \cdot x \in S$ for all $n \geq 0$. But since S is finite, thus $\exists m \neq n$ such that $x^n = x^m$. Now by cancellation law, we get (assuming WLOG that $n > m$)

$$x^{n-m} = 1.$$

Since $n - m > 0$, hence $x^{n-m} = 1 \in S$. Now, consider $y \in S$ such that $y \cdot x^n = 1$, hence,

$$\begin{aligned} y \cdot x^n &= 1 \\ y \cdot x^n &= x^{n-m} \\ y \cdot x^m &= 1 = y \cdot x^n \ \text{ (Cancellation Law)} \end{aligned} \tag{2}$$

Hence, y is the inverse element of x^n. Thus we finally have S as a group. ∎

Answer I.3.14: Let G be a group with the two left cosets of $H \leq G$ and $K \leq G$. We need to show that intersection of these left cosets is either empty or an another left coset of $H \cap K$. Let $x, y \in G$. Consider the left coset of H as $x \cdot H$ and left coset of K as $y \cdot K$. Moreover, consider now the intersection of $x \cdot H$ and $y \cdot K$, $x \cdot H \cap y \cdot K$. Let $z \in x \cdot H \cap y \cdot K$. Therefore $z \in x \cdot H$ and $z \in y \cdot K$. This implies that $z = x \cdot h$ for some $h \in H$, similarly, $z = y \cdot k$ for some $k \in K$. Hence $x \cdot h = y \cdot k \implies h^{-1} \cdot x^{-1} \cdot y \cdot k = (h^{-1} \cdot k) \cdot (x^{-1} \cdot y) = 1 = (y^{-1} \cdot x) \cdot (k^{-1} \cdot h)$. Since $x, y \in G \implies x^{-1} \cdot y$ and $y^{-1} \cdot x$ is in G, therefore either $z = \Phi$ or if $H \cap K \neq \Phi$ then since $H \cap K$ is again a subgroup which implies $h \cdot k^{-1} \in H \cap K$ where $h, k \in H \cap K$, we get that z is in left coset of $H \cap K$. ∎

Answer I.5.1: *Given* : $\varphi : A \to B$, $\psi : A \to C$ are homomorphisms on groups.
Let ψ be surjective and Ker $\psi \subseteq$ Ker φ. With this, we need to show the following (for some unique homomorphism $\sigma : C \to B$):

$$1 : \begin{tikzcd} A \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & C \arrow[d, dashed, "\sigma"] \\ & B \end{tikzcd}$$

We know that $K = \text{Ker } \psi \trianglelefteq A$ (Proposition 19) and $K \subseteq \text{Ker } \varphi$. Now by Factorization (Theorem 1) we have that φ can be factored via the canonical map uniquely as $\varphi = \rho \circ \pi$ as :

$$2 : \begin{tikzcd} A \arrow[r, "\pi"] \arrow[d, "\psi"] \arrow[dr, "\varphi"] & A/\text{Ker } \psi \arrow[d, dashed, "\rho"] \\ C & B \end{tikzcd}$$

Now using Homomorphism theorem (Theorem 2), we see that $A/\text{Ker } \psi \cong \text{Im } \psi = C$ as ψ is surjective where this isomorphism is unique. We hence complete the diagram as follows:

$$3 : \begin{tikzcd} A \arrow[r, "\pi"] \arrow[d, "\psi"'] & A/\text{Ker } \psi \arrow[d, dashed, "\rho"] \arrow[dl, dashed, "\tau"'] \\ C \arrow[r, dashed, "\tau^{-1} \circ \rho"'] & B \end{tikzcd}$$

That is, since τ is a unique isomorphism by Theorem 2 and ρ is a unique homomorphism by Theorem 1, we get that $\sigma = \tau^{-1} \circ \rho$ would again be a unique homomorphism (Proposition 21).

Conversely, we have the Diagram 1 with us, and the fact that ψ is surjective with $\varphi = \sigma \circ \psi$, we hence need to show that Ker $\psi \subseteq$ Ker φ. First note that Ker $\psi = \psi^{-1}(1_C)$ and Ker $\varphi = \varphi^{-1}(1_B)$. Let $a_\psi \in$ Ker ψ and $a_\varphi \in$ Ker φ. Since $\varphi = \sigma \circ \psi$, hence $\varphi^{-1} = \psi^{-1} \circ \sigma^{-1}$. Therefore, Ker $\varphi = \psi^{-1} \circ \sigma^{-1}(1_B)$. Since σ is a homomorphism, hence $1_C \subseteq$ Ker $\sigma = \sigma^{-1}(1_B)$. Hence, Ker $\psi = \psi^{-1}(1_C) \subseteq \psi^{-1} \circ \sigma^{-1}(1_B) = \varphi^{-1}(1_B) =$ Ker φ. ■

Answer I.5.2: *Given* : $1_{2\mathbb{Z}} : 2\mathbb{Z} \to 2\mathbb{Z}$ is a homomorphism and $\iota : 2\mathbb{Z} \to \mathbb{Z}$ is also a homomorphism. Groups $2\mathbb{Z}, \mathbb{Z}$ are under addition.
Assume that $1_{2\mathbb{Z}}$ can be factored via the inclusion map ι. That means that there is a homomorphism $\varphi : \mathbb{Z} : \mathbb{Z} \to 2\mathbb{Z}$ such that $1_{2\mathbb{Z}} = \varphi \circ \iota$, represented as:

$$\begin{tikzcd}
2\mathbb{Z} \arrow[r, "1_{2\mathbb{Z}}"] \arrow[d, "\iota"'] & 2\mathbb{Z} \\
\mathbb{Z} \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

By Homomorphism (Theorem 2), we have that $2\mathbb{Z}/\text{Ker } 1_{2\mathbb{Z}} \cong \text{Im } 1_{2\mathbb{Z}} = 2\mathbb{Z}$. But since Ker $1_{2\mathbb{Z}} = \{0\}$, hence it implies that $A/\text{Ker } 1_{2\mathbb{Z}} = 2\mathbb{Z}/\{0\} = \{0\}$. Which leads to the contradiction that $\{0\} \cong 2\mathbb{Z}$. ■

Answer I.5.3: *Given* : $\varphi : A \to C$ and $\psi : B \to C$ are homomorphisms. Also ψ is injective.
Let $\varphi = \psi \circ \chi$, that is, φ is factored via ψ and χ where $\chi : A \to B$ is a unique homomorphism. This means that we have the following situation:

$$1: \quad \begin{tikzcd}
A \arrow[r, dashed, "\chi"] \arrow[d, "\varphi"'] & B \arrow[dl, "\psi"] \\
C &
\end{tikzcd}$$

Using Homomorphism (Theorem 2) on φ and ψ, we get that $\varphi = \iota_1 \circ \theta_1 \circ \pi_1$ and $\psi = \iota_2 \circ \theta_2 \circ \pi_2$ as follows:

$$2: \quad \begin{tikzcd}
A/\text{Ker } \varphi \arrow[d, dashed, "\theta_1"'] & A \arrow[l, "\pi_1"'] \arrow[r, dashed, "\chi"] \arrow[d, "\varphi"'] & B \arrow[dl, "\psi"] \arrow[dr, "\pi_2"] & \\
\text{Im } \varphi \arrow[r, "\iota_1"'] & C & & B/\text{Ker } \psi \arrow[dl, dashed, "\theta_2"] \\
& & \text{Im } \psi \arrow[ul, "\iota_2"] &
\end{tikzcd}$$

Take any $c \in$ Im φ which is also in C. Assume that $c \notin$ Im ψ. Since θ_1 is an isomorphism (so a bijection), hence $\theta_1^{-1}(c) \in A/\text{Ker } \varphi$. Since π_1 is a canonical projection which is surjective homomorphism (Proposition 23), hence $\pi_1^{-1} \circ \theta_1^{-1} \circ \iota_1^{-1}(c) = \varphi^{-1}(c) = a_1 \in A$. Now $\chi(a_1) \subseteq B$. But since ψ is injective, hence for all $b \in B$, there exists unique element in C. Hence $\psi(\chi(a_1)) = \psi \circ \chi(a_1) = \varphi(a_1) = \varphi \circ \varphi^{-1}(c) = c \in$ Im ψ which is a contradiction.

Conversely, assume that Im $\varphi \subseteq$ Im ψ with ψ being injective. We need to show that Diagram 1 is true. Theorem 2 leads us to Diagram 2 above without the homomorphism $\chi : A \to B$. Since Im $\varphi \subseteq$ Im ψ, hence for any $c \in$ Im φ, $c \in$ Im ψ, which implies that there exists a inclusion homomorphism $\tau :$ Im $\varphi \to$ Im ψ because both Im φ, Im $\psi \subseteq C$. Since ψ is injective, it means that for each $b \in B$, we have a distinct $\psi(b) \in C$. Hence, Ker $\psi = \psi^{-1}(1_C) = 1_B$. Therefore $B/\text{Ker } \psi = B/1_B = B$. Therefore, π_2 becomes a identity mapping from B to B. We can now form the homomorphism χ as the following composition, $\chi = \theta_2^{-1} \circ \tau \circ \theta_1 \circ \pi_1 : A \to B$. Note that θ_1 and θ_2 are unique isomorphisms, courtesy of Theorem 2. Hence χ is also unique. ■

Answer I.5.4: Consider the homomorphism (as $\mathbb{R}$ is an additive group) $\psi : \mathbb{R} \to \mathbb{C}$ such that $\psi(\theta) = e^{i2\pi\theta}$. Clearly, $|\psi(\theta)| = 1$ so ψ maps to complex numbers of modulus 1. Note that Ker $\psi = \mathbb{Z}$. Hence by Homomorphism (Theorem 2) we get that $\mathbb{R}/\text{Ker } \psi = \mathbb{R}/\mathbb{Z} \cong \mathbb{C}_1$ where $\mathbb{C}_1$ is the multiplicative group of all complex numbers of modulus 1. ■

Answer II.3.10: We have $x \in G$ and it's centralizer $C_G(x)$ in G. From this, we need to prove that in the set of all subgroups H whose center contains x, $C_G(x)$ is the largest of them.
We begin by expanding the $Z(C_G(x)) = \{g' \in C_G(x) \mid g' \cdot y = y \cdot g' \; \forall \; y \in C_G(x)\}$. This clearly is the set of all those elements of centralizer $C_G(x)$ which commute with each other. First, it's trivial to see that $C_G(x)$ is a subgroup of G. Second, we take a larger subgroup $J \leq G$ such that $x \in Z(J)$ and $C_G(x) \subseteq J$. Now since $x \in Z(J)$, this implies that $x \cdot z = z \cdot x$ for all $z \in J$. But this implies that $Z(J) \subseteq C_G(x)$ and since $J \subseteq Z(J)$, hence $J \subseteq C_G(x)$. Hence $J = C_G(x)$. ■

Answer II.3.13: We have a group G, Group of automorphic functions from G to G, $\mathbf{Aut}\,(G)$ and the center $Z(G)$. Clearly, $Z(G)$ is a subgroup itself. Now by definition, any $\alpha : G \to G$ in $\mathbf{Aut}\,(G)$ is a bijective homomorphism. Hence, we can write $\alpha(Z(G)) = \{\alpha(y) \mid y \in Z(G)\}$. Now since α is homomorphic, hence for $y \in Z(G)$, $\alpha(y) = \alpha(x \cdot y \cdot x^{-1}) = \alpha(x) \cdot \alpha(y)(\alpha(x))^{-1}$ for all $x \in G$. Rearranging this leads to the equation that $\alpha(y) \cdot \alpha(x) = \alpha(x) \cdot \alpha(y)$ for all $x \in G$ and $y \in Z(G)$. This implies that $\alpha(y) \in Z(G)$ because $\alpha(x) \in G$ is and α is bijective. Therefore we have $\alpha(Z(G)) = Z(G)$, that is, center of a group is a characteristic subgroup. ■

Answer II.3.14: For first part, consider $C \leq N \trianglelefteq G$ where C is a characteristic subgroup. Now note that action of G by inner automorphism on N. Considering the center of N as $Z(N) = \{g \in G \mid g \cdot N \cdot g^{-1} = N\}$, which is also normal. Since $C \leq N \trianglelefteq Z(N)$ and by Proposition 34, we have that $C \trianglelefteq G$.

Second part can be seen easily by noting that the following relation is transitive : $x \leq_C y$ if $\alpha(x) = x \; \forall \; \alpha \in \mathbf{Aut}\,(y)$, where $x \leq_C y$ means x is the characteristic subgroup of y. ■

Answer II.3.15: We have that $N \leq_C G$, $N \leq K \leq G$ with $K/N \leq_C G/N$. We need to prove that $K \leq_C G$. To show this, simply take any $\alpha \in \mathbf{Aut}\,(G)$. Note that $\mathbf{Aut}\,(G/N) \subseteq \mathbf{Aut}\,(G)$. Therefore for any pair of $k_1 \cdot N$, $k_2 \cdot N \in K/N$, we have $\alpha(k_1 \cdot N \cdot k_2 \cdot N) = \alpha(k_1 \cdot k_2 \cdot N) = \alpha(k_1 \cdot k_2) \cdot \alpha(N) = \alpha(k) \cdot N \in K/N$ where $\alpha(k) \in K$. Since α is bijective, therefore $\alpha(K) = K$ for all $\alpha \in \mathbf{Aut}\,(G)$. Hence $K \leq_C G$. ■

Answer III.1.3: Assume a $w \in R$ such that $w \cdot u = u \cdot w = 1_R$ on top of the given fact that $\exists u \in R$ such that $u \cdot v = v \cdot u = 1_R$ for some $v \in R$. Now we simply assume that $w - v \neq 0_R$. Note that if $u = 0_R$, then $R = \{0_R, 1_R\}$ under given conditions (one would get $0_R = 1_R$) and then only such pair would be $1_R \cdot 1_R = 1_R$. For the other non-trivial case, we have $u \neq 0_R$. Therefore by distributive property, we have $0_R = u \cdot 0_R \neq u \cdot (w - v) = u \cdot w - u \cdot v = 1_R - 1_R = 0_R$ which is a contradiction. Hence $w - v = 0 \implies w = v$ so that any *unit* v is unique for ring R with identity.
Showing that the set $U_R = \{u \in R \mid u \cdot v = v \cdot u = 1_R \text{ for some } v \in R\}$ is a group is trivial because associativity and identity are ensured by ring structure and by the fact that $1_R \in U_R$. Moreover, existence of inverse elements of U_R is inbuilt of it's definition. ■

Answer III.1.4: If u is unit of R with identity, then $\exists v \in R$ such that $v \cdot u = u \cdot v = 1_R$. So the second statement follows trivially for $y = x = v$.
Conversely, we have $x \cdot u = u \cdot y = 1_R$ for some $x, y \in R$. Assume that $\nexists z \in R$ such that $z \cdot u = u \cdot z = 1_R \implies z \cdot (u \cdot z) = u \cdot z^2 \implies z \cdot 1_R = z = u \cdot z^2$. Now note that $(x \cdot u) \cdot y = u \cdot y^2 = y \implies u \cdot y^2 = y$ which is a contradiction. Therefore $\exists z \in R$ such that $z \cdot u = u \cdot z = 1_R$, so u is unit of R. ■
