Algebraic Theory I: Homework II

Thomas Fleming

Sun 26 Sep 2021 22:11

Problem (1)**.** Let G_1, G_2 be finite groups with $\gcd(|G_1|, |G_2|) = 1$. Show that $\operatorname{Aut}(G_1 \times G_2) \simeq \operatorname{Aut}(G_1) \times \operatorname{Aut}(G_2)$.

Solution. We induce a bijective correspondence. Let $\alpha \in \operatorname{Aut}(G_1 \times G_2)$, $x \in G_1$ and $y \in G_2$. Then, let $\alpha(x, 1) = (a, b)$ and $\alpha(1, y) = (c, d)$. We see,

$$\begin{aligned}
\alpha\left((x,1)^{|G_1|}\right) &= \alpha\left(x^{|G_1|}, 1\right) \\
\left((a,b)^{|G_1|}\right) &= \alpha(1,1) \\
\left(a^{|G_1|}, b^{|G_1|}\right) &= (1,1) \\
&= \left(1, b^{|G_1|}\right)
\end{aligned}$$

.

Hence, as α is a bijection, we must have $b^{|G_1|} = 1$ and as $|G_1|, |G_2|$ are coprime this implies $b = 1$. Similairly, we see $c = 1$. Hence,

$$\begin{aligned}
\alpha((x,1)\cdot(1,y)) &= \alpha((x,1))(\alpha((1,y))) \\
\alpha(x,y) &= (a,1)\cdot(1,d) \\
&= (a,d)
\end{aligned}$$

.

Then, we note that as $G_1 \simeq G_1 \times \{1\}$ and $G_2 \simeq \{1\} \times G_2$, we have

$\alpha(x,1) \in \operatorname{Aut}(G_1 \times \{1\}) \simeq \operatorname{Aut}(G_1)$ and $\alpha(1,y) \in \operatorname{Aut}(\{1\} \times G_2) \simeq \operatorname{Aut}(G_2)$

Hence, let us define $\alpha_1 : G_1 \to G_1$ and $\alpha_2 : G_2 \to G_2$ to simply be the projection of α into their respective coordinates. We see by the preceding argument that $\alpha_1 \in \operatorname{Aut}(G_1)$ and $\alpha_2 \in \operatorname{Aut}(G_2)$.
Hence, let $\Phi : \operatorname{Aut}(G_1 \times G_2) \to \operatorname{Aut}(G_1) \times \operatorname{Aut}(G_2)$, $\alpha \mapsto (\alpha_1, \alpha_2)$. Let $\alpha, \beta \in \operatorname{Aut}(G_1 \times G_2)$ and suppose $\Phi(\alpha) = \Phi(\beta)$. Then, we have $\Phi(\alpha) = (\alpha_1, \alpha_2) = (\beta_1, \beta_2) = \Phi(\beta)$, hence $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_2$, so we have

$\alpha(x,y) = \alpha(x,1)\cdot\alpha(1,y) = (\alpha_1(x), \alpha_2(y)) = (\beta_1(x), \beta_2(y)) = \beta(x,1)\,\beta(1,y) = \beta(x,y)$

for all $x \in G_1$, $y \in G_2$, so $\alpha = \beta$ and Φ is an injection. Now, let $(\alpha_1, \alpha_2) \in \operatorname{Aut}(G_1) \times \operatorname{Aut}(G_2)$ and we define $\alpha : G_1 \times G_2 \to G_1 \times G_2$, $(x,y) \mapsto (\alpha_1(x), \alpha_2(y))$.

We see α_1, α_2 are bijective, hence α is bijective. Furthermore,

$$\begin{aligned}
\alpha\left((a,b)(c,d)\right) &= \alpha\left(ac, bd\right) \\
&= \left(\alpha_1\left(ac\right), \alpha_2\left(bd\right)\right) \\
&= \left(\alpha_1\left(a\right)\alpha_1\left(c\right), \alpha_2\left(b\right)\alpha_2\left(d\right)\right) \\
&= \left(\alpha_1\left(a\right), \alpha_2\left(b\right)\right)\left(\alpha_1\left(c\right), \alpha_2\left(d\right)\right) \\
&= \alpha\left(a,b\right)\alpha\left(c,d\right)
\end{aligned}
.$$

Hence, α is a homomorphism, so $\alpha \in \mathrm{Aut}\left(G_1 \times G_2\right)$. Hence, Φ is a bijection. Lastly, we show Φ is a homomorphism,

$$\begin{aligned}
\Phi\left(\alpha\beta\right) &= \left(\alpha_1\beta_1, \alpha_2\beta_2\right) \\
&= \left(\alpha_1, \alpha_2\right)\left(\beta_1, \beta_2\right) \\
&= \Phi\left(\alpha\right)\Phi\left(\beta\right).
\end{aligned}$$

So, Φ is an isomorphism, so $\mathrm{Aut}\left(G_1 \times G_2\right) \simeq \mathrm{Aut}\left(G_1\right) \times \mathrm{Aut}\left(G_2\right)$.

Problem (2)**.** Let $n \geq 1$ be an integer. For $x \in \mathbb{Z}$, denote $\overline{x} = x + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ and let $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\overline{x} : x \in \mathbb{Z}, \gcd(x, n) = 1\}$.

1. Show that $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is an abelian multiplicative group.
2. Show that $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Solution.

1. First, we show multiplication is well defined. Let $a, b \in \mathbb{Z}$, hence $an, bn \in n\mathbb{Z}$ and we see for $x, y \in \mathbb{Z}$, $x + an \in \overline{x}$ and $y + bn \in \overline{y}$. Then, we have

$$\begin{aligned}(x + an) \cdot (y + bn) &= xy + (ay + bx)\, n + abn^2 \\ &= xy + n\,(ay + bx + abn) \\ &\in xy + n\mathbb{Z}\end{aligned}$$
.

   And, as x, y are coprime to n, we see $\gcd(xy, n) = 1$ hence we have $\overline{xy} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. Now, note that $\overline{1} = 1 + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ as 1 is coprime to all numbers and $\overline{1}\overline{x} = \overline{1x} = \overline{x1} = \overline{x}\overline{1} = \overline{x}$, so $\overline{1}$ is the identity. Now, recall that there is a linear combination $ax + bn = \gcd(x, n) = 1$, hence we have that $ax = xa = 1 - bn \in 1 + n\mathbb{Z} = \overline{1}$, hence $\overline{a} = \overline{x}^{-1}$, we note that as $a \mid 1 - bn$, we have $\gcd(a, n) = 1$, so $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, hence inverses exist and are well defined. Next, we show associativity.

$$\begin{aligned}(\overline{x} \cdot \overline{y})\, \overline{z} &= \overline{xy} \cdot \overline{z} \\ &= \overline{xyz} \\ &= \overline{x} \cdot \overline{yz} \\ &= \overline{x}\,(\overline{y} \cdot \overline{z})\,.\end{aligned}$$

   Lastly, let us determine commutativity,

$$\begin{aligned}\overline{x} \cdot \overline{y} &= \overline{xy} \\ &= xy + n\mathbb{Z} \\ &= yx + n\mathbb{Z} \\ &= \overline{yx} \\ &= \overline{y} \cdot \overline{x}\end{aligned}$$
.

   Hence, $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is an abelian group under multiplication.

2. Let $x \in \mathbb{Z}/n\mathbb{Z}$ be a generator and $\varphi \in \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ be an automorphism. We wish to induce a correspondance between each φ and each $0 \leq m < n$ such that $\gcd(m, n) = 1$, m being a congruence class in $(\mathbb{Z}/nZ)^{\times}$. First, note that all automorphisms of $\mathbb{Z}/n\mathbb{Z}$ amount to fixing a generator and mapping it to each other generator. Hence a generator $x \mapsto y = x^a$, $y \in \mathbb{Z}/n\mathbb{Z}$ being another generator. We see $\gcd(a, n) = 1$, else y would not be a generator, hence we have each φ corresponds to an $a \nmid n$, denote these automorphisms by φ_a, $1 \leq a < n$, $\gcd(a, n) = 1$. Then, define a bijective correspondance $\kappa : \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$, $\varphi_a \mapsto \overline{a}$. First, we

show this is a homomorphism,

$$\begin{aligned}\kappa\left(\varphi_a\right)\kappa\left(\varphi_b\right) &= \overline{a}\cdot\overline{b}\\ &= \overline{ab}\\ &= \kappa\left(\varphi_{ab}\right)\\ &= \kappa\left(x^{ab}\right)\\ &= \kappa\left(x^a x^b\right)\\ &= \kappa\left(\varphi_a\varphi_b\right)\end{aligned}$$

.

Next, we show bijection. As each $\gcd(a,n)=1$ yields an autmorphism, we see κ is surjective and as each automorphism is completely determined by a, we see a given φ_a corresponds to only one $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^\times$ we have κ is injective. Thus, κ is an isomorphism, so we have $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)\simeq(\mathbb{Z}/n\mathbb{Z})^\times$

Problem (3)**.** Let $H = \langle x \rangle \simeq C_2$ and $N = \langle y \rangle \simeq C_{15}$ be cyclic groups generated by $x \in H$ and $y \in N$ respectively.

1. Show that $\mathrm{Aut}\,(C_{15}) \simeq C_2 \times C_4$.
2. Let $\alpha : H \to \mathrm{Aut}\,(N)$ be a homomorphism and let $\alpha\,(x)\,(y) = y^r$ with $r \in \{0, 1, \ldots, 14\}$. What possible values can r take?
3. For each possible value of α from item 2 determine which of the following four groups is isomoprhic to $N \rtimes_\alpha H$: $C_{30}, D_{15}, C_3 \times D_5, C_5 \times S_3$.

Solution.

1. Note that as $15 = 3 \cdot 5$, we have $C_{15} \simeq C_3 \times C_5$, so by problem 1, $\mathrm{Aut}\,(C_{15}) = \mathrm{Aut}\,(C_3) \times \mathrm{Aut}\,(C_5) = C_2 \times C_4$.
2. Recall from problem 2 that all automorphisms of a cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ amount to mapping generators to generators $y \mapsto z = y^a$, and we see as z is a generator that $a \nmid n$. Hence, the only possible r values are those coprime to 15: $r \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.
3. If $r = 1$, we see $\alpha_1\,(x) = y^1 = y$ is simply the identity automorphism, hence $C_2 \rtimes_\alpha C_{15} = C_2 \times C_{15} = C_{30}$.
   If $r = 14$, we see elements of the form (y^a, x) have $(y^a, x)^2 = \left(y^{15a}, 1\right) = (1, 1)$ and elements of the form $(y^a, 1)$ have $(y^a, 1)^{15} = \left(y^{15a}, 1\right) = (1, 1)$. Lastly, we have

$$\begin{aligned}
(y^a, x)\left(y^b, 1\right)(y^a, x)^{-1} &= (y^a, x)\left(y^b, 1\right)(y^a, x) \\
&= (y^a, x)\left(y^{b+a}, x\right) \\
&= \left(y^{a+14(b+a)}, 1\right) \\
&= \left(y^{15b} y^{14a}, 1\right) \\
&= \left(y^{14a}, 1\right) \\
&= (y^a, 1)^{-1}
\end{aligned}$$

.

   Hence, when $r = 14$, $N \rtimes_\alpha H \simeq D_{15}$

   Next, the case $r = 2$. Note that $C_5 \times S_3$ is the only nonabelian group with an element of order 10 out of the possibilities and as $\mathrm{ord}\,(y, x) = 10$ and $\left(y^2, x\right)\left(y^3, 1\right) = \left(y^8, x\right) \neq \left(y^5, x\right) = \left(y^3, 1\right), \left(y^2, x\right)$ we have $r = 2$ produces a nonabelian group, hence for $r = 2$ we have $N \rtimes_\alpha H \simeq C_5 \times S_3$.

   Similarly, for the case $r = 8$ we have $\mathrm{ord}\,(y, x) = 10$ and $(y, x)\,(y, 1) = \left(y^9, x\right) \neq \left(y^2, x\right) = (y, 1)\,(y, x)$ so $r = 8$ produces a nonabelian group, hence $N \rtimes_\alpha H \simeq C_5 \times S_3$.

   Again, for the case $r = 11$ we have $\mathrm{ord}\,(y, x) = 10$ and $(y, x)\,(y, 1) = \left(y^{12, x}\right) \neq \left(y^2, x\right) = (y, 1)\,(y, x)$, hence $r = 11$ produces a nonabelian group, so we have $N \rtimes_\alpha H = C_5 \times S_3$.

Now, for the case $r = 4$ note that $C_3 \times D_5$ is the only nonabelian group with an element of order 6 out of the possibilities and as $\operatorname{ord}(y, x) = 6$ and $\left(y^2, x\right)\left(y^3, 1\right) = \left(y^{14}, x\right) \neq \left(y^5, 1\right) = \left(y^3, 1\right)\left(y^2, x\right)$ we see $r = 4$ produces a nonabelian group, hence for $r = 4$ we have $N \rtimes_\alpha H \simeq C_3 \times D_5$.

Similarly, we have for $r = 7$, $\operatorname{ord}\left(y^5, x\right) = 6$ and $(y, x)(y, 1) = \left(y^8, x\right) \neq \left(y^2, x\right) = (y, 1)(y, x)$. Hence, for $r = 7$ $N \rtimes_\alpha H \simeq C_3 \times D_5$.

Lastly, note that when $r = 13$, we have $\operatorname{ord}(y, x) = 30$ and as C_{30} is the only group under consideration of order 30, we have $N \rtimes_\alpha H \simeq C_{30}$.

Problem (4)**.** Show there is no simple group of order 5103.

Solution. Let G be a simple group with $|G| = 5103 = 3^6 \cdot 7$. Then, note the congruence conditions of sylows theorem paired with G being simple implies the number of sylow 3-groups, $n_3 = 7$. Hence, there exists a homomorphism $\alpha : G \to S_7$ with the kernel being a normal subgroup. As G is simple, we know $\ker(\alpha) = \{1\}$. So, we have G being isomorphic to a subgroup of S_k, hence $|G| \mid |S_k|$, implying $5103 \mid 5040 = 7!$. $\lightning$. Hence, $n_3 = 1$ and we see G is not simple.

Problem (5)**.** Show there is no simple group of order 4851.

Solution. Let G be a simple group of order $4851 = 3^2 \cdot 7^2 \cdot 11$ and let n_3, n_{11} be the number of sylow 3-groups and sylow 11-groups in G respectively. Then, we find by sylows theorem $n_3 = 7$ or 49 and $n_{11} = 3^2 \cdot 7^2 = 441$. Hence, let us first assume $n_3 = 7$ and let Q be a sylow 3-group. We find $|N_G(Q)| = 3^2 \cdot 7 \cdot 11$. Let P be an 11-group of $N_G(Q)$ and m_{11} to be the number of sylow 11-groups in $N_G(Q)$. We see $m_{11} \mid 3^2 \cdot 7$ and $m_{11} \equiv 1 (\mod 11)$, so $m_{11} = 1$. Hence, $P \trianglelefteq N_G(Q)$ and as P is an 11-group of G, we find $\langle N_G(Q), P\rangle \leq N_G(P)$. So, $3^2 \cdot 7 \cdot 11 \mid |N_G(P)|$. Similarly, if $n_3 = 49$, let Q be a sylow 3-group of G then we find $|N_G(Q)| = 3^2 \cdot 11$. Let P be a sylow 11-group of $N_G(Q)$, and we see by the congruence conditions that once again, the number of sylow 11-groups in $N_G(P)$, $m_{11} = 1$, hence $P \trianglelefteq N_G(Q)$. And, as P is a sylow 11-group of G, we find $\langle N_G(Q), P\rangle \leq N_G(P)$ implies $3^2 \cdot 11 \mid |N_G(P)|$. Then, As $3 \mid |N_G(P)|$ in either case and P is a sylow 11-group in G, with $3^2 \mid |G|$ we find $3^2 \nmid |G : N_G(P)| = n_{11}$. $\lightning$. Hence, $n_{11} = 1$, so G is simple.