MAS511 Spring 2020 Homework #02

June 4, 2022

Any ring homomorphism in this homework is assumed to preserve $+, \cdot$ and 1.

Problem 1

Let G be a finite group and p be a prime number dividing $|G|$. Assuming Cauchy's theorem for the case of abelian G, deduce Cauchy's theorem for general G by using the class equation for G. (Hint: Use induction on $|G|$.)

Theorem 1 (Cauchy's)**.** *Let G be a finite group. G has an element of order p for every prime number p which divides $|G|$.*

Solution

Lemma 1. *Let G be a group and $S \subseteq G$. Then, the centralizer $C_G(S)$ is a subgroup of G. In particular, $Z(G) = C_G(G) \leq G$.*

Proof. To show that $C_G(S) \leq G$, it's enough to show that (1) $C_G(S) \subseteq S$; (2) $C_G(S) \neq \emptyset$; (3) $\forall a, b \in C_G(S) : a^{-1}b \in C_G(S)$.

First, $C_G(S) \subseteq G$, because by the definition $C_G(S) = \{g \in G \mid \forall s \in S : gs = sg\}$.

Next, because 1_G satisfies $g1_G = g = 1_G g$ for every $g \in G$, $s1_G = 1_G s$ holds for every $s \in S$. Therefore, $1_G \in C_G(S)$ and $C_G(S) \neq \emptyset$.

Suppose that $a, b \in C_G(S)$. It means, for every $s \in S$, $as = sa$ and $bs = sb$ hold. Then,

$$\begin{aligned} a^{-1}bs = a^{-1}sb &= a^{-1}saa^{-1}b \\ &= a^{-1}asa^{-1}b = sa^{-1}b \end{aligned}$$

Thus, for every $s \in S$, $(a^{-1}b)s = s(a^{-1}b)$ also hold. It implies that $a^{-1}b \in C_G(S)$.

Therefore, $C_G(S) \leq G$. □

Let G be a finite group, and suppose that Cauchy's Theorem hold for abelian groups.

Let's use induction on $|G|$ to prove:

Hypothesis: For every finite group G, Cauchy's Theorem holds for G.

(Base case 1) Suppose that G is trivial. Then, there are no prime $p \in \mathbb{N}$ such that $p \mid |G| = 1$. Therefore, Cauchy's Theorem is vacuously true for a trivial group.

(Base case 2) Suppose that $|G| = p$ for some prime number $p \in \mathbb{N}$. Then, $|G|$ is a prime number $\Rightarrow$ G is a cyclic group $\Rightarrow$ G is an abelian group. Since we assumed Cauchy's Theorem for abelian groups, Cauchy's Theorem holds for G, which is one of abelian groups.

(Inductive step) Let $n \in \mathbb{N}$ be a non-prime number and G be a group of order n. Let's assume that Cauchy's Theorem holds for every group of order less than n as an induction hypothesis, and show that Cauchy's Theorem holds for G using the hypothesis.

Let p be an arbitrary prime number such that $p \mid n$. Then, there is $\alpha, m \in \mathbb{N}$ such that $p^\alpha m = n$ and $p \nmid m$. Let's show that G contains an element of order p for this arbitrary p.

First of all, suppose that $|G| = |Z(G)|$. Since $Z(G) \leq G$, $G = Z(G) = \{g \in G \mid \forall h \in G : gh = hg\}$. It means, for every $g \in G$, g commutes every $h \in G$. Thus, G is abelian. In this case, G has an element of order p by Cauchy Theorem for abelian groups.

Let's assume that $|Z(G)| \neq |G|$. With the fact that $Z(G) \leq G$, $|Z(G)| < |G|$ and $Z(G) \lneq G$ hold. Then, for some $x \in G \backslash Z(G)$, there is $y \in G$ such that $xy \neq yx$. Then, $\{g \in G \mid gxg^{-1}\}$ contains at least two elements $x = 1x1^{-1}$ and yxy^{-1}. Therefore, G has at least one conjugation orbit of length greater than 1. Let $O_1, O_2, \cdots, O_L$ are distinct conjugation orbits. And let $x_1, x_2, \cdots, x_L$ such that $x_i \in O_i$ for each $i \in \{1, 2, \cdots, L\}$. Then, the class equation holds:

$$|G| = |Z(G)| + \sum_{i=1}^{L} [G : C_G(x_i)]$$

Suppose that $p \mid |Z(G)|$. Then, because $Z(G)$ is a group, $p \mid |Z(G)|$, and $|Z(G)| < |G| = n$, $Z(G)$ has an element y of order p by the induction hypothesis. And since $Z(G) \lneq G$, $y \in Z(G) \subsetneq G$. It indicates that G has an element y, which has order p.

Suppose that $p \nmid |Z(G)|$. In other words, $|Z(G)| \not\equiv 0 \pmod{p}$. Then, because $|G| \equiv 0 \pmod{p}$, $|G| - |Z(G)| \not\equiv 0 \pmod{p}$. Then, let's take a modulo by p on the class equation:

$$\begin{aligned}
|Z(G)| + \sum_{i=1}^{L} [G : C_G(x_i)] &= |G| \\
\sum_{i=1}^{L} [G : C_G(x_i)] &= |G| - |Z(G)| \\
\sum_{i=1}^{L} [G : C_G(x_i)] &\equiv |G| - |Z(G)| \not\equiv 0 \pmod{p}
\end{aligned}$$

Thus, $\sum_{i=1}^{L} [G : C_G(x_i)] \not\equiv 0 \pmod{p}$.

In this case, $[G : C_G(x_i)] \not\equiv 0 \pmod{p}$ for at least one $i \in \{1, 2, \cdots, L\}$. Becuase, if not, $\forall i \in \{1, 2, \cdots, L\} : [G : C_G(x_i)] \equiv 0 \pmod{p}$ holds, and

$$\begin{aligned}
\sum_{i=1}^{L} [G : C_G(x_i)] &\equiv [G : C_G(x_1)] + \sum_{i=2}^{L} [G : C_G(x_i)] \equiv 0 + \sum_{i=2}^{L} [G : C_G(x_i)] \\
&\equiv [G : C_G(x_2)] + \sum_{i=3}^{L} [G : C_G(x_i)] \equiv 0 + \sum_{i=3}^{L} [G : C_G(x_i)] \\
&\equiv \cdots \equiv 0 + [G : C_G(x_L)] \equiv 0 + 0 \equiv 0 \pmod{p}
\end{aligned}$$

But it's a contradiction because $\sum_{i=1}^{L} [G : C_G(x_i)] \not\equiv 0 \pmod{p}$.

Let $k \in \{1, 2, \cdots, L\}$ such that $[G : C_G(x_k)] \not\equiv 0 \pmod{p}$. Then, $[G : C_G(x_k)] = \frac{|G|}{|C_G(x_k)|}$ does not contain p as a factor. However, because $|G| = p^\alpha m$, $|C_G(x_k)| = p^\alpha l$ where $l \leq m$ and $p \nmid l$. Thus, $p \mid |C_G(x_k)|$.

Also, $|C_G(x_k)| < |G|$. It's because, as we chose x_k to be a representative of some conjugation orbit of length greater than 1,

$$\begin{aligned}
[G : C_G(x_k)] &> 1 \\
\frac{|G|}{|C_G(x_k)|} &> 1 \\
|G| &> |C_G(x_k)|
\end{aligned}$$

Therefore, $p \mid |C_G(x_k)|$ and $|C_G(x_k)| < |G| = n$. It means, $C_G(x_k)$ contains an element y of order p by the induction hypothesis. And, by Lemma 1, $C_G(x_k) \leq G$. Thus, $y \in C_G(x_k) \subsetneq G$. Therefore, G has y, which is an element of order p.

In conclusion, if Cauchy's Theorem holds for every groups of order less than some non-prime number n, Cauchy's Theorem also holds for every group of order n.

Thus, by induction, for every group G such that $|G| \in \mathbb{N}$, Cauchy's Theorem holds for G. $\square$

Problem 2

Let p and q be a prime numbers with $p < q$. Prove that any group G of order pq^n for some integer $n \geq 1$ is solvable.

Solution

Theorem 2 (Sylow Theorem)**.** *Let G be a group of order $p^\alpha m$, where p is a prime not dividing m and $\alpha \in \mathbb{N}$.*

(1) $\mathrm{Syl}_p(G) \neq \emptyset$.

(2) Let $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ be a p-subgroup. There exists $g \in G$ such that $Q \leq gPg^{-1}$.

(3) $|\mathrm{Syl}_p(G)| = n_p \equiv 1 \pmod{p}$ *and* $n_p \mid m$.

Lemma 2. *Let G be a finite group acts on a set X. Let $x \in X$, $G \cdot x = \{g \cdot x \mid g \in G\}$ be the orbit of x, and $G_x = \{g \in G \mid g \cdot x = x\}$ be the stabilizer of x. Then,*

1. $G_x \leq G$.
2. $|G \cdot x| = [G : G_x]$
3. $|G \cdot x|$ *and* $|G_x|$ *divides* $|G|$

Proof. 1. By definition, $G_x \subseteq G$. And $1_G \in G_x$ because an identity of G fixes every element of X. Lastly, if $a, b \in G_x$, they satisfies $a \cdot x = x$ and $b \cdot x = x$, and,

$$a^{-1}b \cdot x = a^{-1} \cdot x = a^{-1} \cdot a \cdot x = x$$

Thus, $a^{-1}b \in G_x$. These results indicate that $G_x \leq G$.

2. Let L be a set of cosets of G_x in G. Let's define $\varphi : G \cdot x \to L$ such as $\varphi : y \mapsto gG_x$ where $g \in G$ satisfies $g \cdot x = y$. Then,

- φ is well-defined. If $y \in G \cdot x$, it means there is $g \in G$ such that $g \cdot x = y$ holds. Also, if $g, h \in G$ satisfies $g \cdot x = h \cdot x = y$, then $h^{-1}g \cdot x = x$. Since $h^{-1}g$ fixes x, $h^{-1}g \in G_x$. Thus $h^{-1}gG_x = G_x$ and $gG_x = hG_x$.
- φ is injective. Let $y, z \in G \cdot x$ satisfies $\varphi(y) = \varphi(z)$. It means, $g_1 \cdot x = y$, $g_2 \cdot x = z$, and $g_1G_x = g_2G_x$. Since $g_1G_x = g_2G_x$ implies $g_2^{-1}g_1 \in G_x$ (i.e. $g_2^{-1}g_1$ fixes x),

$$y = g_1 \cdot x = g_2 \cdot g_2^{-1}g_1 \cdot x = g_2 \cdot x = z$$

- φ is surjective. Let $gG_x \in L$. If we take $y = g \cdot x$, $y \in G \cdot x$ and $\varphi(y) = gG_x$.

Thus, φ is a well-defined bijective map. Because G is a finite group, $|L| = [G : G_x]$ is also finite. And because there is a bijective map between L and $G \cdot x$, $|G \cdot x| = |L| = [G : G_x]$ holds.

3. Since $|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}$, $|G \cdot x| \cdot |G_x| = |G|$. Thus, $|G \cdot x|$ and $|G_x|$ divides $|G|$. □

Lemma 3 (Sylow Theorem $(1)'$)**.** *Let G be a group of order $p^\alpha m$, where p is a prime not dividing m and $\alpha \in \mathbb{N}$. Then, there exists $H_1, H_2, \cdots, H_\alpha$ such that*

$$\{1\} = H_0 \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_\alpha$$

where $[H_i : H_{i-1}] = p$ for all $i \in \{1, 2, \cdots, \alpha\}$ and $H_\alpha \in \mathrm{Syl}_p(G)$.

Proof. Let's construct $H_1, \cdots, H_\alpha$ in two steps: (1) constructing H_1, (2) constructing H_{i+1} when H_i was constructed for $i \in \{1, 2, \cdots, \alpha - 1\}$.

(1) We can easily find H_1. By Cauchy Theorem, G contains an element x of order p. Let $H_1 = \langle x \rangle$. Then $\{1\} \lneq H_1 = \langle x \rangle$, and $[H_1 : \{1\}] = |H_1| = p$.

(2) Suppose that we already constructed $H_1, \cdots, H_i$ for some $i \in \{1, 2, \cdots, \alpha - 1\}$, such that $\{1\} = H_0 \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_i$, and $[H_k : H_{k-1}] = p$ for every $k \in \{1, 2, \cdots, i\}$. Note that

$$|H_i| = |H_0| \prod_{k=1}^{i} \frac{|H_k|}{|H_{k-1}|} = 1 \cdot \prod_{k=1}^{i} [H_k : H_{k-1}] = \prod_{k=1}^{i} p = p^i$$

Let $L = \{gH_i \mid g \in G\}$, the set of left cosets of H_i. Then, $|L| = [G : H_i]$. Also, we will consider that H_i acts on L by left multiplication.

Let $L_{H_i} = \{S \in L \mid \forall h \in H_i : hS = S\}$. Then, for any $a \in G$,

$$\begin{aligned}
aH_i \in L_{H_i} &\Leftrightarrow \forall h \in H_i : haH_i = aH_i \\
&\Leftrightarrow \forall h \in H_i : a^{-1}haH_i = H_i \\
&\Leftrightarrow \forall h \in H_i : a^{-1}ha \in H_i \\
&\Leftrightarrow a^{-1}H_ia \subseteq H_i \\
&\Leftrightarrow a^{-1}H_ia = H_i \ \ (\because H_i \text{ is a finite group, and } |H_i| = |a^{-1}H_ia| \text{ holds}) \\
&\Leftrightarrow a \in N_G(H_i) \\
&\Leftrightarrow aH_i \in N_G(H_i)/H_i
\end{aligned}$$

holds. This shows that $L_{H_i} = N_G(H_i)/H_i$, and $|L_{H_i}| = [N_G(H_i) : H_i]$.

Let $O_S = \{hS \mid h \in H_i\}$, the orbit of $S \in L$. Let $S_1, \cdots, S_n \in L$ are the representatives of distinct orbits; i.e. $O_{S_1}, \cdots, O_{S_n}$ are disjoint pairwisely and $\bigcup_{k=1}^{n} O_{S_k} = L$. Then,

$$|L| = \sum_{k=1}^{n} |O_{S_k}|$$

holds.

Suppose that $|O_{S_k}| = 1$ for some $k \in \{1, \cdots, n\}$. It means $hS_k = S_k$ for all $h \in H_i$. Then $S_k \in L_{H_i}$ by the definition of L_{H_i}. Conversely, if $S_k \in L_{H_i}$, then $\forall h \in H_i : hS_k = S_k$, $O_{S_k} = \{S_k\}$, and $|O_{S_k}| = 1$. Thus, for $I = \{k \in \{1, 2, \cdots, n\} \mid |O_{S_k}| = 1\}$, $L_{H_i} = \{S_i \mid i \in I\}$ and $|I| = |L_{H_i}|$.

Let $k \in \{1, 2, \cdots, n\} \backslash I$. Then, $|O_{S_k}| \neq 0$ because $S_k \in O_{S_k}$, and $|O_{S_k}| \neq 1$ because $k \notin I$. Thus, $|O_{S_k}| \geq 2$. But by Lemma 2, $|O_{S_k}| \mid |H_i| = p^i$. This two facts show that $p \mid |O_{S_k}|$ must hold for $k \in \{1, \cdots, n\} \backslash I$.

So, we obtain:

$$\begin{aligned}
|L| = \sum_{k=1}^{n} |O_{S_k}| &= \sum_{k \in I} |O_{S_k}| + \sum_{k \in \{1, \cdots, n\} \backslash I} |O_{S_k}| \\
&= \sum_{k \in I} 1 + \sum_{k \in \{1, \cdots, n\} \backslash I} |O_{S_k}| \\
&= |I| + \sum_{k \in \{1, \cdots, n\} \backslash I} |O_{S_k}| \\
&= |L_{H_i}| + \sum_{k \in \{1, \cdots, n\} \backslash I} |O_{S_k}|
\end{aligned}$$

and

$$\begin{aligned}
[G : H_i] = |L| &\equiv |L_{H_i}| + \sum_{k \in \{1, \cdots, n\} \backslash I} |O_{S_k}| \\
&\equiv |L_{H_i}| = [N_G(H_i) : H_i] \pmod{p}
\end{aligned}$$

Also, $p \mid [G : H_i] = p^{\alpha-i}m$ holds since $|H_i| = p^i$ and $i < \alpha$. Thus $[N_G(H_i) : H_i] \equiv [G : H_i] \equiv 0 \pmod{p}$. But because $[N_G(H_i) : H_i] > 0$, $[N_G(H_i) : H_i] \geq p > 1$. This indicates that $H_i \lneq N_G(H_i)$.

Let $Q = N_G(H_i)/H_i$, and the canonical surjective homomorphism $\gamma : N_G(H_i) \to Q$ such that $\gamma : h \mapsto hH_i$. Because $p \mid |Q|$, by Cauchy Theorem, there exists $x \in Q$ of order p. Trivially, we know that $\{H_i\} \lneq \langle x \rangle$. Let's define $H_{i+1} = \gamma^{-1}(\langle x \rangle)$. Then, $H_i = \gamma^{-1}(\{H_i\}) \lneq \gamma^{-1}(\langle x \rangle) = H_{i+1}$ because of the fourth isomorphism theorem (lattice theorem). In addition,

$$[H_{i+1} : H_i] = |\langle q \rangle : \{H_i\}| = |\langle x \rangle| = p$$

Therefore, this H_{i+1} satisfies $H_i \lneq H_{i+1}$ and $[H_{i+1} : H_i] = p$.

By following (1) and repeating (2) for $\alpha - 1$ times, we obtain $H_1, H_2, \cdots, H_\alpha$ which satisfies

$$\{1\} = H_0 \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_\alpha$$

and $[H_i : H_{i-1}] = p$ for every $i \in \{1, 2, \cdots, \alpha\}$. Also, because

$$|H_\alpha| = |H_0| \prod_{i=1}^{\alpha} \frac{|H_i|}{|H_{i-1}|} = 1 \cdot \prod_{i=1}^{\alpha} [H_i : H_{i-1}] = \prod_{i=1}^{\alpha} p = p^\alpha$$

$H_\alpha \in \mathrm{Syl}_p(G)$ holds. □

Lemma 4 (Sylow Theorem (2)′)**.** *Let G be a group of order $p^\alpha m$, where p is a prime not dividing m. $\mathrm{Syl}_p(G) = \{H\}$ implies $H \trianglelefteq G$.*

Proof. Suppose that $\mathrm{Syl}_p(G) = \{H\}$. Then, for any $g \in G$, $gHg^{-1} \in \mathrm{Syl}_p(G)$.

($\because$ Let $\phi_g : G \to G$ such that $\phi_g : x \mapsto gxg^{-1}$ for $g \in G$. ϕ_g is surjective because for any $h \in G$, $g^{-1}hg \in G$ and $\phi_g(g^{-1}hg) = gg^{-1}hgg^{-1} = h$. ϕ_g is injective because for any $h_1, h_2 \in G$, $\phi_g(h_1) = \phi_g(h_2)$ implies $gh_1g^{-1} = gh_2g^{-1}$ and $h_1 = h_2$ by multiplicating g^{-1} on left and g on right. Thus, ϕ_g is bijective and $|gHg^{-1}| = |\phi_g(H)| = |H| = p^\alpha$. Therefore, gHg^{-1} is also a subgroup of G of order p^α.)

But since $\mathrm{Syl}_p(G)$ is a singleton containing H, $H \in \mathrm{Syl}_p(G)$ implies $H = gHg^{-1}$ for arbitrary $g \in H$. Thus, H is a normal subgroup of G. □

Let's think about Sylow q-group of G.

First of all, by Sylow Theorem (3), for $n_q = |\mathrm{Syl}_q(G)|$, $n_q \equiv 1 \pmod{p}$ and $n_q \mid p$. It implies there is $k \in \mathbb{Z}^{\geq 0}$ such that $n_q = 1 + kq$ and $1 + kq \mid p$. But if $k \geq 1$, then $1 + kq \geq 1 + q > q > p$ and $n_q = 1 + kq \nmid p$. Therefore, k must be 0 and $n_q = 1$. Let $\mathrm{Syl}_q(G) = \{H\}$.

In this case, by Lemma 4, $H \trianglelefteq G$ and $|H| = q^n$.

And, by Lemma 3, there is a subnormal series

$$\{1\} = H_0 \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_n$$

where $[H_i : H_{i-1}] = q$ for all $i \in \{1, 2, \cdots, n\}$ and $H_n \in \mathrm{Syl}_q(G)$. However, since $\mathrm{Syl}_q(G)$ is a singleton of H, $H_n = H$. Thus, $\{1\} = H_0, H_1, \cdots, H_n = H, G$ form a subnormal series:

$$\{1\} = H_0 \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_n = H \lneq G$$

where $[H_i : H_{i-1}] = q$ for all $i \in \{1, 2, \cdots, n\}$ and $[G : H] = p$. Because p and q are prime numbers, H_i/H_{i-1} for $i \in \{1, 2, \cdots, n\}$ and G/H are cyclic groups, which are abelian. This shows that G is solvable. □

Problem 3

Let X be a set of cardinality at least 2. Prove that $\mathrm{Aut}(F(X))$, the group of all group automorphisms of the free group $F(X)$, is not a nilpotent group. (Hint: Compute $Z(F(X))$ by looking at the number of non-e-letters of a reduced word in it.)

Solution

Lemma 5. *Let G be a group and $g \in G$. Then, for any $g \in G$, a conjugation $f_g : G \to G$ defined as $f_g : x \mapsto gxg^{-1}$ is an automorphism of G.*

Proof. f_g is an endomorphism by the definition.

f_g is a homomorphism. Because, for any $x, y \in G$,

$$f_g(x)f_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = f_g(xy)$$

f_g is surjective. Because, for any $x \in G$, $g^{-1}xg \in G$ since G is closed under $\cdot$ and $f_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$.

f_g is injective. Because $\ker f_g = \{1_G\}$. (Let x be an arbitrary element of G. If $x \in \ker f_g$, $f_g(x) = gxg^{-1} = 1_G$ must hold. Then, $x = g^{-1}1_G g = g^{-1}g = 1_G$. Therefore, 1_G is the only element of $\ker f_g$.) □

Lemma 6. *Let G be a group. If $Z(G) = \{1_G\}$, $Z(\mathrm{Aut}(G)) = \{\mathrm{Id}_G\}$.*

Proof. Suppose that $Z(G) = \{1_G\}$, and let $\varphi \in Z(\mathrm{Aut}(G))$. Then, for every $\psi \in \mathrm{Aut}(G)$, $\psi \circ \varphi = \varphi \circ \psi$ must hold. Because a conjugation $f_g : G \to G$ such that $x \mapsto gxg^{-1}$ for $g \in G$ is an automorphism, $f_g \circ \varphi = \varphi \circ f_g$ must hold for every $g \in G$. Then, for every $h \in G$,

$$\begin{aligned} g\varphi(h)g^{-1} &= f_g(\varphi(h)) \\ &= \varphi(f_g(h)) = \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \end{aligned}$$

must holds. And if the above holds, the below equation also holds:

$$\varphi(g)^{-1}g\varphi(h) = \varphi(h)\varphi(g)^{-1}g$$

Because φ is an automorphism, $G = \varphi(G)$. Thus,

$$\forall h \in G : (\varphi(g)^{-1}g)\varphi(h) = \varphi(h)(\varphi(g)^{-1}g)$$

is equivalent to

$$\forall h \in G : (\varphi(g)^{-1}g)h = h(\varphi(g)^{-1}g)$$

Then, $\varphi(g)^{-1}g \in Z(G)$ since the definition of $Z(G)$ is $\{x \in G \mid \forall h \in G : xh = hx\}$. However, as $Z(G) = \{1_G\}$, $\varphi(g)^{-1}g = 1_G$ and $g = \varphi(g)$. In summary, if $\varphi \in Z(\mathrm{Aut}(G))$, then $g = \varphi(g)$ for all $g \in G$ at the least. However, if $\forall g \in G : g = \varphi(g)$, then $\varphi = \mathrm{Id}_G$ since G is the domain of φ. Therefore, $\varphi = \mathrm{Id}_G$ if $\varphi \in Z(\mathrm{Aut}(G))$. This indicates that $Z(\mathrm{Aut}(G)) \subseteq \{\mathrm{Id}_G\}$.

Also, $\mathrm{Id}_G \in Z(\mathrm{Aut}(G))$, because for every $\psi \in \mathrm{Aut}(G)$, $\psi \circ \mathrm{Id}_G = \psi = \mathrm{Id}_G \circ \psi$.

Therefore, $Z(\mathrm{Aut}(G)) = \{\mathrm{Id}_G\}$. □

Lemma 7. *Let G be a non-trivial group. If $Z(G) = \{1_G\}$, G is not nilpotent.*

Proof. Let $Z_0(G) = \{1_G\}$, $Z_1(G) = Z(G)$, $Z_i(G) \leq G$ such that $Z_i/Z_{i-1} \simeq Z(G/Z_{i-1})$ for integer $i \geq 2$. Then,

$$\{1_G\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots \trianglelefteq Z_n(G) \trianglelefteq \cdots$$

If G is nilpotent, then there exists $n \in \mathbb{N}$ such that $Z_n(G) = G$.

Suppose that $Z(G) = \{1_G\}$. Then, $Z_1(G) = Z(G) = \{1_G\}$.

For $i \in \mathbb{N}$, suppose that $Z_i(G) = \{1_G\}$. Then, $G/Z_i(G) = G/\{1_G\} \simeq G$, and $Z(G/Z_i(G)) \simeq Z(G) = \{1_G\}$. Thus, $Z_{i+1}(G)/Z_i(G) \simeq Z(G/Z_i(G)) \simeq \{1_G\}$. It implies that $Z_{i+1}(G)/Z_i(G)$ is a trivial group, and $Z_{i+1}(G) = Z_i(G)$. Therefore, $Z_{i+1}(G) = Z_i(G) = \{1_G\}$.

In this case, $\forall n \in \mathbb{N} : Z_n(G) = \{1_G\}$ by induction with $Z_1(G) = \{1_G\}$ (base case) and $\forall i \in \mathbb{N} : Z_i(G) = \{1_G\} \Rightarrow Z_{i+1}(G) = \{1_G\}$ (inductive step). Also, because G is non-trivial, there is no $n \in \mathbb{N}$ such that $Z_n(G) = G$, becuase $Z_n(G) = \{1_G\} \neq G$ for every $n \in \mathbb{N}$. Therefore, G cannot be nilpotent. □

Let's consider $F(X)$ as a group of reduced words generated by X. $e \in F(X)$ is an identity (empty word). And the length of $w \in F(X)$ is n for a reduced word $w = x_1 x_2 \cdots x_n$ of $F(X)$. The length of empty word e is 0. Also, note that:

$$Z(F(X)) = \{w \in F(X) \mid \forall x \in F(X) : wx = xw\}$$

Since $|X| \geq 2$, there exists at least two distinct $x, y \in X$.

Suppose that $w \in F(X)$ such that the length of w is greater than 0.

Suppose that the first character of reduced w is x, there is $w' \in F(X)$ such that $w = xw'$. Then, for $u = yw \in F(X)$,

$$uw = (yxw')(xw') \neq (xw')(yxw') = wu$$

because the first characters are different. It indicates that there is a word u in $F(X)$ such that $uw \neq wu$.

Suppose that the first character of reduced w is x^{-1}, there is $w' \in F(X)$ such that $w = x^{-1}w'$. Then, for $u = yw \in F(X)$,

$$uw = (yx^{-1}w')(x^{-1}w') \neq (x^{-1}w')(yx^{-1}w') = wu$$

because the first characters are different. It indicates that there is a word u in $F(X)$ such that $uw \neq wu$.

Suppose that the first character of reduced w is neither x nor x^{-1}. Then, by taking $u = xw \in F(X)$,

$$uw = (xw)w \neq w(xw) = wu$$

because the first characters are different. It also indicates that there is a word u in $F(X)$ such that $uw \neq wu$.

Therefore, if the length of w is greater than 0, there is a word $u \in F(X)$ such that $uw \neq wu$. It implies that every element of $Z(F(X))$ has 0-length.

The 0-length word of $F(X)$, e, satisfies $\forall u \in F(X) : ue = u = eu$, because e is an identity.

In conclusion,

$$Z(F(X)) = \{e\}$$

and $F(X)$ cannot be nilpotent.

By Lemma 6, $Z(\mathrm{Aut}(F(X))) = \{\mathrm{Id}_{F(X)}\}$ because $Z(F(X)) = \{e\}$. Note that $\mathrm{Aut}(F(X))$ is non-trivial. ($\because$ The conjugation f_x of x is an automorphism by Lemma 5, and f_x is not an identity because $f_x(y) = xyx^{-1}$ is already reduced and $f_x(y) = xyx^{-1} \neq y$. Thus, $\mathrm{Aut}(F(X))$ has at least two automorphisms: $\mathrm{Id}_{F(X)}$ and f_x.) By Lemma 7, $\mathrm{Aut}(F(X))$ is not nilpotent because $\mathrm{Aut}(F(X))$ is non-trivial and $Z(\mathrm{Aut}(F(X)))$ is trivial. □

Problem 4

Let R be a nonzero integral domain and D be the set of all nonzero elements of R. Let $i : R \to D^{-1}R$ be the injective ring homomorphism defined by $i(r) = r/1$. Prove $D^{-1}R$ is the 'smallest' field containing R in the following sense: $D^{-1}R$ is a field, and for any injective ring homomorphism $f : R \to K$ for some field K, there exists a unique injective ring homomorphism $g : D^{-1}R \to K$ such that $g \circ i = f$.

Solution

Let R be a non-zero integral domain, and $D = R\backslash\{0\}$. Let $i : R \to D^{-1}R$ be a injective ring homomorphism such that $\forall r \in R : i(r) = r/1$.

Suppose that K be a field, and $f : R \to K$ be an injective ring homomorphism.

Let $g : D^{-1}R \to K$ be a function such that $g\left(\frac{r}{d}\right) = f(d)^{-1}f(r)$ for $r \in R$, $d \in D$. Then,

(i) g is well-defined.

Suppose that $r_1, r_2 \in R$ and $d_1, d_2 \in D$ satisfies $\frac{r_1}{d_1} = \frac{r_2}{d_2}$. It means, $r_1d_2 = r_2d_1$ as R is an integral domain. Then, $f(r_1d_2) = f(r_2d_1)$. Since f is a ring homomorphism, $f(r_1)f(d_2) = f(r_2)f(d_1)$. Also, since f is injective and $f(0) = 0_K$, $f(r) \neq 0_K$ for every non-zero $r \in R$. So $f(d_1), f(d_2)$ are non-zero, thus units, and $f(d_1)^{-1}f(r_1) = f(d_2)^{-1}f(r_2)$ holds. By the definition of g, $g(r_1/d_1) = g(r_2/d_2)$.

Therefore, g is well-defined.

(ii) $g(d/d) = f(1)$ for $d \in D$.

By definition, $g(d/d) = f(d)^{-1}f(d) = f(d)^{-1}f(d)f(1) = f(1)$ holds.

(iii) $f(1)g(1/d)^{-1} = g(d/1)$ for $d \in D$.

$f(1) = g(d/d) = g((d/1)(1/d)) = g(d/1)g(1/d)$. Thus $f(1)g(1/d)^{-1} = g(d/1)$.

(iv) g is a ring homomorphism.

Let $r_1, r_2 \in R$, $d_1, d_2 \in D$, and $q_1 = r_1/d_1$, $q_2 = r_2/d_2$.

$$\begin{aligned} g(q_1 + q_2) = g(\frac{r_1}{d_1} + \frac{r_2}{d_2}) &= g(\frac{d_2r_1 + d_1r_2}{d_1d_2}) \\ &= f(d_1d_2)^{-1}f(d_2r_1 + d_1r_2) \\ &= f(d_1)^{-1}f(d_2)^{-1}(f(d_2)f(r_1) + f(d_1)f(r_2)) \\ &= f(d_1)^{-1}f(d_2)^{-1}f(d_2)f(r_1) + f(d_1)^{-1}f(d_2)^{-1}f(d_1)f(r_2) \\ &= f(d_1)^{-1}f(r_1) + f(d_2)^{-1}f(r_2) = g(\frac{r_1}{d_1}) + g(\frac{r_2}{d_2}) = g(q_1) + g(q_2) \end{aligned}$$

$$\begin{aligned} g(q_1q_2) = g(\frac{r_1}{d_1}\frac{r_2}{d_2}) &= g(\frac{r_1r_2}{d_1d_2}) \\ &= f(d_1d_2)^{-1}f(r_1r_2) \\ &= f(d_1)^{-1}f(d_2)^{-1}f(r_1)f(r_2) \\ &= (f(d_1)^{-1}f(r_1))(f(d_2)^{-1}f(r_2)) = g(\frac{d_1}{r_1})g(\frac{d_2}{r_2}) = g(q_1)g(q_2) \end{aligned}$$

Also, since i and f are ring homomorphisms, $i(1) = 1/1$ and $f(1)$ are unities. And, $g(1/1) = g(i(1)) = f(1)$ holds. Thus g also preserve unity.

Thus, g is a ring homomorphism.

(v) g is injective.

It's enough to show that $\ker g = \{0\}$.

Let $r \in R$ and $d \in D$ such that $g(r/d) = 0_K$. Then, $g(r/d) = f(d)^{-1}f(r) = 0_K$, and $f(r) = 0_K$ and $f(r) \in \ker f$ because $f(d)$ is non-zero in the field K. Since f is injective, $\ker f = \{0\}$. Thus, $f(r) = 0_K$ implies $r = 0$. Therefore, $\ker g = \{0\}$.

(vi) $g \circ i = f$.

Let $r \in R$. Then,

$$g(i(r)) = g(r/1) = f(1)^{-1}f(r) = f(1)^{-1}f(r \cdot 1) = f(1)^{-1}f(r)f(1) = f(r)$$

(i), (iv), (v), (vi) implies that g is a well-defined injective ring homomorphism such that $g \circ i = f$.

Suppose that $g' : D^{-1}R \to K$ is an injective ring homomorphism such that $g' \circ i = f$. Let $r/d \in D^{-1}R$ such that $r \in R$, $d \in D$.

$$\begin{aligned} g(r/d) = g(r/1)g(1/d) &= g(r/1)g(d/1)^{-1}g(d/1)g(1/d) \\ &= g(r/1)g(d/1)^{-1}g(d/d) \\ &= g(r/1)g(d/1)^{-1}g(1/1) \\ &= g(i(r))g(i(d))^{-1}g(i(1)) \\ &= f(r)f(d)^{-1}f(1) \\ &= f(r \cdot 1)f(d)^{-1} \\ &= f(r)f(d)^{-1} \end{aligned}$$

$$\begin{aligned} g'(r/d) = g'(r/1)g'(1/d) &= g'(r/1)g'(d/1)^{-1}g'(d/1)g'(1/d) \\ &= g'(r/1)g'(d/1)^{-1}g'(1/1) \\ &= g'(i(r))g'(i(d))^{-1}g'(i(1)) \\ &= f(r)f(d)^{-1}f(1) \\ &= f(r)f(d)^{-1} \end{aligned}$$

Therefore,

$$g(r/d) = f(r)f(d)^{-1} = g'(r/d)$$

holds for every $r/d \in D^{-1}R$. Thus, $g = g'$.

In conclusion, for any injective ring homomorphism $f : R \to K$ for some field K, there is an injective ring homomorphism $g : D^{-1}R \to K$ such that $g \circ i = f$, and g satisfies UMP in the sense that if $g' : D^{-1}R \to K$ is an injective ring homomorphism such that $g' \circ i = f$, $g = g'$ holds. □

Problem 5

Let R be a principle ideal domain. Prove that there exists only one maximal ideal in R if and only if there exists $r \in R$ such that any nonzero proper ideal of R is equal to (r^n) for some integer $n \geq 1$.

Solution

Let R be a PID. Because R is a PID $\Rightarrow$ UFD $\Rightarrow$ a commutative ring with unity, every ideal in R can be represented as $(a) = aR$ for some $a \in R$, and every element of R has a unique factorization up to association.

($\Longrightarrow$)

Suppose that R has only one maximal ideal, and let $M = (r)$ be the maximal ideal of R.

Note that, r is prime iff r is irreducible iff an ideal (r) is prime iff an ideal (r) is maximal for $r \in R$ because R is a PID. Because we picked r such that (r) is the maximal ideal of R, r is an irreducible element of R. Also, suppose that x is an arbitrary irreducible element of R. Because x is irreducible, (x) is a maximal ideal. But because there is only one maximal ideal (r) in R, $(x) = (r)$ should hold. Thus, x and r must associate. This shows that every irreducible element of R associate with each other.

Let $I \subsetneq R$ be an arbitrary non-zero proper ideal of R. Then, there is $a \in R$ such that $I = (a)$ because R is a PID. Trivially, a cannot be a zero (If not, $(a) = \{0\}$ but we assumed I is a non-zero ideal), and cannot be a unit (If not, $(a) = R$ but we assumed I is a proper ideal). Let $a = ux_1 \cdots x_m$ be a factorization of R where $u \in R$ is a unit and $x_1, \cdots, x_m$ are irreducible elements of R. As R is a UFD, the factorization exists and unique up to association and because a is non-zero non-unit, $m \geq 1$. As we showed that every irreducible elements of R associates, $x_1, \cdots, x_m$ associate to r. Let $u_1, \cdots, u_m$ be units of R such that $x_1 = u_1 r, \cdots, x_m = u_m r$. Let $u' = uu_1 \cdots u_m$. Then, u' is a unit because there is $u^* = u_m^{-1} \cdots u_1^{-1} u^{-1} \in R$ which is the multiplicative inverse of u'. Since R is commutative,

$$a = ux_1 \cdots x_m = u(u_1 r) \cdots (u_m r) = (uu_1 \cdots u_m) r^m = u' r^m$$

Thus, a associates to r^m, and $I = (a) = (r^m)$ holds for such $m \geq 1$. □

($\Longleftarrow$)

Suppose that there is $r \in R$, which satisfies that there exists $n \in \mathbb{N}$ such that $I = (r^n)$ for any nonzero proper ideal I of R.

Suppose that R has no nonzero proper ideal I of R. It means, R has only two ideals: trivial ideal $\{0\}$ and R. Thus, R is a field. And because the field R contains only one proper ideals $\{0\}$, $\{0\}$ is the unique maximal ideal of R.

Let's assume that R has nonzero proper ideals.

First, if r is a unit, r^n is also a unit for any $n \in \mathbb{N}$. ($\because (r^n)^{-1} = (r^{-1})^n$) But in this case, $(r^n) = R$. ($\because \forall x \in R : x = r^n((r^n)^{-1}x) \in r^n R = (r^n)$) Then, for every $n \in \mathbb{N}$, $\{0\} \neq (r^n) = R$. However it's a contradiction because we assumed that $\exists n \in \mathbb{N} : I = (r^n)$ for any proper ideal I of R. Thus, r cannot be a unit.

For any $n \in \mathbb{N}$, $(r^n) \subseteq (r)$. Because if $a \in (r^n)$, then there exists $b \in R$ such that $a = r^n b = r(r^{n-1}b) \in rR = (r)$.

Let M be a maximal ideal of R. Then, there is $m \in \mathbb{N}$ such that $M = (r^m)$. But as we showen above, $M = (r^m) \subseteq (r) \subsetneq R$. Because M is maximal, $M = (r)$ or $(r) = R$. Since r is a non-unit, $(r) \neq R$, and $M = (r)$ must hold. Therefore, if M is a maximal ideal of R, it must be (r). Therefore, R has only one maximal ideal, (r). □