Moshe Mason Rubin
MATH 330 Homework #9
23 November 2016

Exercise 11.10. If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.

Proof. Let γ be a generator for G. Then for each $g \in G$, $g = \gamma^n$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned}
\phi(g) &= \phi(\gamma^n) \quad \text{because } \gamma \text{ generates } G \\
&= \phi\left(\underbrace{\gamma \cdot \gamma \cdot \ldots \cdot \gamma}_{n \text{ times}}\right) \\
&= \underbrace{\phi(\gamma) \circ \phi(\gamma) \circ \cdots \circ \phi(\gamma)}_{n \text{ times}} \quad \text{as } \phi \text{ is a homomorphism so } \phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2) \\
&= \phi^n(\gamma)
\end{aligned}$$

So for all $\phi(g) \in \phi(G)$, we have $\phi(g) = \phi^n(\gamma)$ for some $n \in \mathbb{N}$. So $\phi(\gamma)$ generates $\phi(G)$; so $\phi(G)$ is cyclic. □

Lemma 11.1. *If G_1, G_2 are groups with an isomorphism $\phi : G_1 \to G_2$ and there exists $g_1 \in G_1$ such that* $\operatorname{ord}(g_1) = n$ *for some $n \in \mathbb{N}$. Then* $\operatorname{ord}(\phi(g_1)) = n$.

Proof. If $g_1^n = e_1$ then

$$\begin{aligned}
e_2 &= \phi(e_1) \quad \text{by Proposition 1.11.1} \\
&= \phi(g_1^n) \quad \text{because } \operatorname{ord}(g_1) = n \\
&= \phi^n(g_1) \quad \text{because } \phi \text{ is an isomorphism}
\end{aligned}$$

So $\operatorname{ord}(\phi(g_1)) = n$. □

Exercise 11.14. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{Q}$.

Proof. Consider $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ which has order 2 as $\left(\frac{1}{2} + \mathbb{Z}\right) + \left(\frac{1}{2} + \mathbb{Z}\right) = 1 + \mathbb{Z} \equiv \mathbb{Z}$ and $\mathbb{Z}$ is the identity in $\mathbb{Q}/\mathbb{Z}$. Consider for a contradiction that there exists a non-zero $q \in \mathbb{Q}$ with order 2. That is, $q + q = 0 \iff 2q = 0$ which has no solution in $\mathbb{Q} \setminus \{0\}$. So there is no element of order 2 in $\mathbb{Q}$. So by Lemma 11.1, the two groups cannot be isomorphic. □

Exercise 11.5 (Addition Exercises: Automorphism #5)**.** Let G be a group and i_g be an inner automorphism of G, and define a map

$$\psi : G \to \operatorname{Aut}(G)$$

by

$$g \mapsto i_g.$$

Prove that this map is a homomorphism with image $\operatorname{Inn}(G)$ and kernel $Z(G)$. Use this result to conclude that

$$G/Z(G) \simeq \operatorname{Inn}(G).$$

Proof. Recall

$$\begin{aligned}
\operatorname{Aut}(G) &:= \{\text{all isomorphisms } \phi : G \to G\} \\
\text{Given } g \in G, \quad i_g : G \to G &\quad \text{by} \quad x \mapsto gxg^{-1} \\
\operatorname{Inn}(G) &:= \{i_g \text{ for all } g \in G\} \\
Z(G) &:= \{x \in G : gx = xg \text{ for all } g \in G\}
\end{aligned}$$

ψ is a homomorphism as

$$\begin{aligned}
\psi(g_1 \cdot g_2) &= i_{g_1 \cdot g_2}(x) \quad \text{by definition of } \psi \\
&= (g_1 \cdot g_2) \cdot (x) \cdot (g_1 \cdot g_2)^{-1} \quad \text{by definition of } i_g \\
&= (g_1 \cdot g_2) \cdot (x) \cdot \left(g_2^{-1} \cdot g_1^{-1}\right) \\
&= g_1 \cdot \left(g_2 \cdot x \cdot g_2^{-1}\right) \cdot g_1^{-1} \quad \text{because } G \text{ is a group so elements associate} \\
&= g_1 \cdot (i_{g_2}(x)) \cdot g_1^{-1} \quad \text{by definition of } i_g \\
&= (i_{g_1} \circ i_{g_2})(x) \quad \text{by definition of } i_g
\end{aligned}$$

So ψ is a homomorphism.

The image of ψ is clearly $\text{Inn}(G)$ as $\text{Im}(\psi) := \{\psi(g) \text{ for all } g \in G\} = \{i_g \text{ for all } g \in G\} =: \text{Inn}(G)$.

$\ker(\psi) := \{g \in G : \psi(g) = id\}$ and $\psi(g) = id \iff gxg^{-1} = x \iff gx = xg$. So $\ker(\psi) = Z(G)$.

By the First Isomorphism Theorem, $G/\ker(\psi) \simeq \text{Im}(\psi)$, so we have $G/Z(G) \simeq \text{Inn}(G)$. ☐

Exercise 13.3. Find all of the abelian groups of order 720 up to isomorphism.

Solution. $720 = 2^4 \cdot 3^2 \cdot 5$, so, by The Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of order 720 up to isomorphism are:

1. $\mathbb{Z}_2^4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
2. $\mathbb{Z}_4 \times \mathbb{Z}_2^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
3. $\mathbb{Z}_4^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
4. $\mathbb{Z}_8 \times Z_2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
5. $\mathbb{Z}_{16} \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
6. $\mathbb{Z}_2^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
7. $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
8. $\mathbb{Z}_4^2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
9. $\mathbb{Z}_8 \times Z_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
10. $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$ ☐

Exercise 13.5. Show that the infinite direct product $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ is not finitely generated.

Proof. Suppose for a contradiction that G is finitely generated and has n generators. Because G is abelian and every element is of order 2, so $|G| \leq 2^n$, which is a contradiction to the assumption that G is infinite. ☐

Exercise 13.14. Let G be a solvable group. Prove that any sub-group of G is also solvable.

Proof. content... ☐

Exercise 14.2. Computer all the X_g and all G_x for each of the following permutation groups.

(a) $X = \{1, 2, 3\}$,
$G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

(b) $X = \{1, 2, 3, 4, 5, 6\}$,
$G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$

Solution. Recall $X_g := \{x \in X \text{ such that } gx = x\}$ and $G_x := \{g \in G \text{ such that } gx = x\}$

(a)
- $X_{(1)} = X$
- $X_{(12)} = \{3\}$
- $X_{(13)} = \{2\}$
- $X_{(23)} = \{1\}$
- $X_{(123)} = X_{(132)} = \emptyset$
- $G_1 = \{(1), (23)\}$
- $G_2 = \{(1), (13)\}$
- $G_3 = \{(1), (12)\}$

(b)
- $X_{(1)} = X$
- $X_{(12)} = \{3, 4, 5, 6\}$
- $X_{(345)} = X_{(354)} = \{1, 2, 6\}$
- $X_{(12)(345)} = X_{(12)(354)} = \{6\}$
- $G_1 = G_2 = \{(345), (354)\}$
- $G_3 = G_4 = G_5 = \{(1), (12)\}$
- $G_6 = G$ ☐

Exercise 14.5. Let $G = A_4$ and suppose that G acts on itself by conjugation; that is, $(g, h) \mapsto ghg^{-1}$.

(a) Determine the conjugacy classes (orbits) of each element of G.

(b) Determine all the isotropy sub-groups for each element of G.

Proof. Recall if $\sigma = (\sigma_1, \ldots, \sigma_n)$ and $\tau = (\tau_1, \ldots, \tau_n)$ are permutations then $\tau\sigma\tau^{-1} = (\tau(\sigma_1), \ldots, \tau(\sigma_n))$.

(a) $A_4 = \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\}$, so

- $\mathcal{O}_{id} = \{id\}$
- $\mathcal{O}_{(234)} = \{(234), (423), (241), (213), (431), (132), (314), (124), (143), (412), (321), (234)\} = \{(234), (124), (132), (143)\}$
- $\mathcal{O}_{(243)} = \{(324), (243), (214), (231), (413), (123), (341), (142), (134), (421), (312), (243)\} = \{(243), (142), (123), (134)\}$

- $\mathcal{O}_{(12)(34)} = \{(13)(42), (14)(23), (32)(41), (42)(13), (24)(31), (41)(32), (23)(14), (31)(24), (12)(34), (43)(12), (43)(12), (12)(34)\} = \{(13)(24), (14)(23), (12)(34)\}$

(b) Recall given an element $x \in G$, G_x is the isotropy sub-group defined by $G_x := \{g \in G \text{ such that } gx = x\}$

$\square$

Exercise 16.1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$

(d) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$

(e) $\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$

(f) $R = \left\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\right\}$

Proof.

(b) $\mathbb{Z}_{18}$ is a ring; however it is not a field because not every every element has an inverse.

(c) $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is both a ring and a field: the inverse of any given $a + b\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ is given by $\frac{a}{a^2 - 2b^2} + \frac{b}{2b^2 - a^2}\sqrt{2}$. Notice this is always well defined except when $a^2 - 2b^2 = 0$, which cannot be the case because $a, b \in \mathbb{Q}$.

(d) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$ is a ring but not a field. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is closed as one can check that

$$\begin{aligned}\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right)\left(\alpha + \beta\sqrt{2} + \gamma\sqrt{2} + \delta\sqrt{2}\right) &= (a\alpha + 2b\beta + 3c\gamma + 6d\delta) + (b\alpha + a\beta + 3d\gamma + 3c\delta)\sqrt{2} \\ &\quad + (c\alpha + 2d\beta + a\gamma + 2b\delta)\sqrt{3} + (d\alpha + c\beta + b\gamma + a\delta)\sqrt{6} \\ &\in \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)\end{aligned}$$

However, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is not closed under inverses so it is not a field.

(e) $\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$ is a ring but not a field.

(f) $R = \left\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\right\}$ is a ring but not a field. $\square$

Exercise 16.2. Let R be the ring of 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a sub-ring S of R with an identity.

Proof. Consider $S := \{\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] \text{ such that } c \in \mathbb{R}\} \subseteq R$. By Proposition 16.2, to show that $S \subseteq R$ is a sub-ring of R, it is sufficient to show

1. $S \neq \emptyset$
2. $rs \in S$ for all $r, s \in S$
3. $r - s \in S$ for all $r, s \in S$

1. $S \neq \emptyset$ as $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓
2. S is closed under multiplication as for $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c\gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓
3. S is closed under subtraction as for $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] - \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c-\gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓

So S is a sub-ring of R. Furthermore, S is a sub-ring with unity as for any $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]$. $\square$

Exercise 16.3. List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$.

Proof. (a) The units of $\mathbb{Z}_{10}$ are $\{x \in \mathbb{Z}_{10} \text{ such that } \gcd(10, x) = 1\} = \{1, 3, 7, 9\}$.

(b) The units of $\mathbb{Z}_{12}$ are $\{x \in \mathbb{Z}_{12} \text{ such that } \gcd(12, x) = 1\} = \{1, 5, 7, 11\}$.

(c) The units of $\mathbb{Z}_7$ are $\{x \in \mathbb{Z}_7 \text{ such that } \gcd(7, x) = 1\} = \mathbb{Z}_7$ as 7 is prime.

(d) The units of $\mathbb{M}_2(\mathbb{Z})$ are $GL_2(\mathbb{Z})$

(e) The units of $\mathbb{M}_2(\mathbb{Z}_2)$ are $GL_2(\mathbb{Z}_2) = \mathbb{M}_2(\mathbb{Z}_2) \setminus \{\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]\}$ ☐

Exercise 16.4. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

Proof.

(a) The ideals of $\mathbb{Z}_{18}$ are $\{0\}, \mathbb{Z}_{18}, 2\mathbb{Z}_{18}, 3\mathbb{Z}_{18}, 6\mathbb{Z}_{18}$, and $9\mathbb{Z}_{18}$.

(b) The ideals of $\mathbb{Z}_{25}$ are $\{0\}, \mathbb{Z}_5$, and $\mathbb{Z}_{25}$.

☐

Exercise 16.9. What is the characteristic of the field formed by the set of matrices

$$F = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

with entries in $\mathbb{Z}_2$?

Proof. The characteristic of F is 2 because $2r = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ for all $r \in F$. ☐