

Problems Related to Material from Chapters 6–16.

11/03/03 Radford

The first three exercises are exercises in simple proofs.

1. Let $f : X \rightarrow X'$ and $f' : X' \rightarrow X''$ be functions.
 - a) Suppose that f, f' are one-one. Show that $f' \circ f : X \rightarrow X''$ is one-one.
 - b) Suppose that f, f' are onto. Show that $f' \circ f : X \rightarrow X''$ is onto.(Thus if f, f' are bijective then $f' \circ f$ is bijective.)
2. Suppose that $f : G \rightarrow G'$ and $f' : G' \rightarrow G''$ are group homomorphisms.
 - a) Show that the composite $f' \circ f : G \rightarrow G''$ is a group homomorphism.
 - a) Suppose that f, f' are isomorphism. Show that $f' \circ f : G \rightarrow G''$ is an isomorphism.
 - c) Suppose that f is an isomorphism. Show that $f^{-1} : G' \rightarrow G$ is a group isomorphism. [Hint: You may assume that f^{-1} is bijective. For $g', h' \in G'$ note that $g' = f(f^{-1}(g'))$ and $h' = f(f^{-1}(h'))$. Use these facts to calculate $f^{-1}(g'h')$.]
3. Use Problem 2 to show that $G \sim G'$ if and only if there is an isomorphism $f : G \rightarrow G'$ defines an equivalence relation on any non-empty set of groups.

Recall that left cosets of a subgroup H of a group G partition G . The same is true of the right cosets of H in G .

4. Suppose that H is a subgroup of a group G and $[G:H] = 2$.
 - a) Show that the left cosets of H in G are H and $G \setminus H = \{g \in G \mid g \notin H\}$.
 - b) Show that the right cosets of H in G are $H, G \setminus H$.
 - c) Show that H is a normal subgroup of G .

5. Suppose that H is a subgroup of G and $|H| = 2$.
- Suppose that H is normal subgroup of G . Show that H is in the center of G .
 - Suppose that H is in the center of G . Show that H is a normal subgroup of G .
6. Let $G = \langle a \rangle$ be a cyclic group of order 15.
- How many cosets does the subgroup $H = \langle a^{-40} \rangle$ have in G by Lagrange's Theorem?
 - List the (left) cosets of H in G together with their elements.
7. Let H be a subgroup of a group G . Prove that H is a normal subgroup of G if and only if *any* left coset of H is *some* right coset of H . That is, if $a \in G$ then $aH = Hb$ for some $b \in G$.

An issue which comes up in connection with the First Isomorphism Theorem is whether or not a function is well-defined. The basic problem is this: a rule is defined on the basis of one of using one of several descriptions of an input value (free choice). For the rule to be a function the resulting output can not depend on the particular choice of description of an input value.

8. Let $G = \langle a \rangle$ be cyclic of order n and suppose that $f : G \rightarrow G'$ is a group homomorphism.
- Show that $f(a)$ has finite order and $|f(a)|$ divides $n = |a|$.
 - Suppose that $b \in G'$ has finite order and $|b|$ divides n . Show that the rule $\phi : G \rightarrow G'$ given by $\phi(a^m) = b^m$ is a *well-defined* group homomorphism. (Well-defined here means that $a^m = a^{m'}$ implies that $b^m = b^{m'}$.)
 - Show that the rule $\phi : \mathbf{Z}/7\mathbf{Z} \rightarrow \mathbf{Z}/8\mathbf{Z}$ given by $\phi(m+7\mathbf{Z}) = m+8\mathbf{Z}$ is not a well-defined function by finding specific integers m, m' such that $m+7\mathbf{Z} = m'+7\mathbf{Z}$ but $m+8\mathbf{Z} \neq m'+8\mathbf{Z}$.

If $\phi : G \rightarrow G'$ is a homomorphism of finite groups, recall that $G/\text{Ker } \phi \simeq \text{Im } \phi$ by the First Isomorphism Theorem. Thus

$$\frac{|G|}{|\text{Ker } \phi|} = |\text{Im } \phi|, \text{ or equivalently } |G| = |\text{Ker } \phi| |\text{Im } \phi|,$$

a multiplicative analog of the Rank–Nullity Theorem of linear algebra.

9. Determine all group homomorphisms $\phi : \mathbf{Z}_{15} \rightarrow \mathbf{Z}_{20}$.

The units of the ring \mathbf{Z}_n are the generators of the additive group \mathbf{Z}_n .

10. Let $R = \mathbf{Z}_n$.

a) Show that $U(R) = \{1 \leq \ell < n \mid (\ell, n) = 1\}$.

b) List the elements of $U(\mathbf{Z}_{30})$. Is $U(\mathbf{Z}_{30})$ cyclic?

11. Consider the group $G = \mathbf{Z}_4 \oplus \mathbf{Z}_4$.

a) What are the possible orders of the subgroups of G according to Lagrange's Theorem?

b) List all *cyclic* subgroups of G for each of the orders of part a).

c) Show that G has a subgroup of every possible order arising from part a).

The (multiplicative) group $U(R \oplus S)$ is abelian when R, S are commutative rings with unity.

12. Let R, S be rings with unity.

a) Show that $U(R \oplus S) = U(R) \oplus U(S)$.

b) List the elements of $U(\mathbf{Z}_5 \oplus \mathbf{Z}_6)$.

c) Write $U(\mathbf{Z}_5 \oplus \mathbf{Z}_6)$ as a direct product of cyclic groups.

The ring of complex numbers can be modeled (constructed) as a subring of matrices.

13. Let $M(2, \mathbf{R})$ be the ring of 2×2 matrices with real coefficients and let $M = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbf{R} \right\}$.

a) Show that M is a subring with unity of $M(2, \mathbf{R})$.

b) Show that $\phi : \mathbf{C} \rightarrow M$ defined by $\phi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ is an isomorphism of rings with unity.

14. Let R be a ring and suppose that I, J are ideals of R . Show that $I + J$ and $I \cap J$ are ideals of R .

To show that a non-empty subset of a ring is not a subring it is necessary to show that at least one of the axioms fails to hold in at least one instance.

15. Determine whether or not $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in \mathbf{Z}, b, c \in \mathbf{R}, \right\}$ is:

a) an additive subgroup of $M(2, \mathbf{R})$;

a) a subring of $M(2, \mathbf{R})$.

16. Determine whether or not R described in each case below is (1) an additive subgroup of \mathbf{C} , (2) a subring with unity of \mathbf{C} :

a) $R = \{a + bi \mid a, b \in \mathbf{Q}\}$;

b) $R = \{a + bi \mid a \in \mathbf{Q}, b \in \mathbf{Z}\}$;

c) $R = \{a + bi \mid a \in \mathbf{Z}, b \in 2\mathbf{Z}\}$.

In each case that R is a subring with unity, list the elements of $U(R)$.

16. Let F be a field and let n be a positive integer. Show that the set G of roots of $x^n - 1$ in F is a multiplicative subgroup of F^* .

17. Let F be a field and suppose that $f(x), g(x) \in F[x]$ have degree at most n . Suppose that $a_1, \dots, a_{n+1} \in F$ are distinct and that $f(a_i) = g(a_i)$ for all $1 \leq i \leq n + 1$. Show that $f(x) = g(x)$. [Hint: Consider the difference $d(x) = f(x) - g(x)$.]

18. Suppose that R is a finite ring with unity and let $a \in R$ be non-zero. Show that $a \in U(R)$ or there is a non-zero $b \in R$ such that $ab = 0 = ba$. [Hint: Consider $1, a, a^2, a^3, \dots$. Since R is finite this list has only a finite

number of *values*. Thus $a^n = a^m$ for some $0 \leq m < n$. Let n be the smallest such integer and consider $a^n - a^m = 0$. Two basic cases: $m = 0$, $m > 0$.]

Every non-zero ring R has at least two different ideals, namely (0) and R . This may be it in some cases.

19. Show that the ring $M(2, \mathbf{R})$ has exactly two ideals.

Every ideal of $F[x]$, where F is a field, is generated by a single element.

20. Let $R = \mathbf{R}[x]$.

- a) Suppose that I is an ideal of R and $x^4 + 2, x^5 + 11x^9 - 23 \in I$. Show that $I = R$.
- b) Show that the set S of all polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in R$ such that $a_\ell = 0$ when ever ℓ is odd is a subring of R with unity but not an ideal of R .