ABSTRACT ALGEBRA MODULUS

SPRING 2006

by Jutta Hausen, University of Houston

Undergraduate abstract algebra is usually focused on three topics: Group Theory, Ring Theory, and Field Theory. Of the myriad of text books on the subject, the following references will be used:

[D] John R. Durbin, *Modern Algebra*, Fourth Edition, Wiley & Sons, New York, NY, 2000 (ISBN 0-471-32147-8).

[GG] J. Gilbert and L. Gilbert, *Elements of Modern Algebra*, Fifth Edition, Brooks/Cole, Pacific Grove, CA, 2000 (ISBN 0-534-37351-8).

[R] J. J. Rotman, *A First Course in Abstract Algebra*, Second Edition, Prentice Hall, Upper Saddle River, NJ, 2000 (ISBN 0-13-011584-3).

These notes are intended for mathematics students as a compact summary of undergraduate abstract algebra.

1. Fundamentals

The symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the set of all positive integers, all integers, all rational numbers, all real numbers, and all complex numbers, respectively. You are familiar with mathematical induction, with the fact that $\mathbb{N}$ is a well–ordered set, and concepts from elementary number theory like primes, greatest common divisors and the division algorithm.

Exercise 1. *Prove: If a, b and c are integers such that (i) a divides bc and (ii) a and b are relatively prime, then a divides c.* (Hint: Try to mimic the proof of Euclid's Lemma [R, page 43]).

You are also familiar with elementary set theory: intersection and union of sets, subsets, and set builder notation like $\{n : n \text{ is a positive integer}\}$ which of course equals $\mathbb{N}$. The cardinality (number of elements) of a set X is denoted by $|X|$. You are able to prove equalities like $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for all sets A, B, C. [GG, page 8, Example 13].

Exercise 2. *Prove: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ for all sets A, B, C.*

You also are familiar with functions (also called mappings or maps) and the concepts of a function $f : A \to B$ being one–to–one (injective), or onto (surjective), or a one–to–one correspondence (a bijection) [D, page 11–13]. Given functions $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ is defined by $(g \circ f)(a) = g(f(a))$ for all $a \in A$. The composition of two onto functions (when defined) is another onto function [D, page 16, 2.1].

Exercise 3. *Prove: If $f : A \to B$ and $g : B \to C$ are two functions which are both one–to–one, then the composition $g \circ f : A \to C$ is one–to–one.*

A function $f : A \to B$ is *invertible* if and only if it is both one–to–one and onto. If f is invertible, there exists a unique function $f^{-1} : B \to A$ such that $f \circ f^{-1} = 1_B$ and $f^{-1} \circ f = 1_A$ (1_X denotes the identity function on the set X.)

Exercise 4. *Prove: If $f : A \to B$ is a function, and if there exists a function $g : B \to A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$, then f is invertible and $g = f^{-1}$.*

An important relation on the set $\mathbb{Z}$ of all integers is *congruence modulo m,* where $m \geq 0$ denotes some fixed integer that is called *the modulus.* Define two integers a and b to be *congruent modulo m*, if m divides $a - b$. Write $a \equiv b \pmod{m}$ if a and b are congruent modulo m. Notice that $a \equiv b \pmod{0}$ if and only if $a = b$, while $a \equiv b \pmod{1}$ for any two integers a and b. Thus, in most cases, the modulus m is assumed to be ≥ 2. Congruence modulo m is an equivalence relation on $\mathbb{Z}$, i.e. the relation $\equiv \pmod{m}$ is reflexive, symmetric and transitive [R, page 63, 1.45]. The equivalence class containing a is denoted by $[a]$ and called the *congruence class of a modulo m.* Suppose $m \geq 2$ and let $a \in \mathbb{Z}$. By the division algorithm there exist unique integers q and r such that $a = qm + r$ and $0 \leq r < m$. This unique r is said to be *the remainder after dividing a by m* [R, p. 37, Definition]. Two integers a and b are congruent modulo m if and only if they have the same remainder after division by m [R, page 63, 1.46(iii)]. Each integer a is congruent modulo m to exactly one element in the set $\{0, 1, \ldots, m-1\}$ [R, page 64, 1.47]. It follows that the set $\mathbb{Z}_m = \{[a] : a \in \mathbb{Z}\}$ of all congruence classes modulo m is a finite set of cardinality m; in fact [GG, page 83]

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}\,.$$

Congruence modulo m is compatible with the operations of addition and multiplication of integers in the sense that $a \equiv b \pmod{m}$ and $a' \equiv b' \pmod{m}$ imply that $a + a' \equiv b + b' \pmod{m}$ and that $aa' \equiv bb' \pmod{m}$ [R, page 64, 1.48].

2. Groups

A *group* is a pair $(G, *)$ where G is a set and $*$ a binary operation on G which associates with every ordered pair $(a, b) \in G \times G$ a unique element $a * b \in G$ such that the following conditions hold:

a) For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

b) There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.

c) For every $a \in G$ there exists $a' \in G$ such that $a * a' = a' * a = e$.

If $a * b = b * a$ for all elements a, b in a group G, then G is said to be a *commutative* or an *abelian* group. The *order* of G is the cardinality of the set G.

Suppose $(G, *)$ is a group. One can show that there exists one and only one element $e \in G$ that has property b), and this is called the *identity element* of G; also, given $a \in G$, there exists one and only one $a' \in G$ satisfying c), and this a' is called the *inverse of* a; if the operation $*$ is considered to be a multiplication, a' is denoted by a^{-1}; if $*$ is considered to be an addition, one writes $a' = -a$ and calls a' the *additive inverse of* a or *the negative of* a.

Examples of Groups.

1. $(\mathbb{Z}, +)$, $e = 0$, inverse = negative.

2. $(\mathbb{Q}, +)$, $e = 0$, inverse = negative.

3. $(\mathbb{R}, +)$, $e = 0$, inverse = negative.

4. $(\mathbb{C}, +)$, $e = 0$, inverse = negative.

5. $(\mathbb{Z}_m, +)$ where $1 \leq m \in \mathbb{Z}$, and for $[a], [b] \in \mathbb{Z}_m$, $[a] + [b] = [a + b]$; $e = [0]$, and $-[a] = [m - a] = [-a]$ for all $[a] \in \mathbf{Z}_m$.

6. Define $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ to be the set of all nonzero rationals, all nonzero reals, and all nonzero complex numbers, respectively. Then $(\mathbb{Q}^*, \cdot\,)$, $(\mathbb{R}^*, \cdot\,)$ and $(\mathbb{C}^*, \cdot\,)$ are groups with $e = 1$; the inverse of a is $\frac{1}{a} = a^{-1}$.

7. Define $\mathbb{Q}^+$ and $\mathbb{R}^+$ to be the set of all positive rationals and all positive reals, respectively. Then $(\mathbb{Q}^+, \cdot\,)$ and $(\mathbb{R}^+, \cdot\,)$ are groups with $e = 1$; the inverse of a is $\frac{1}{a} = a^{-1}$.

8. $(\{1\}, \cdot\,)$ and $(\{1, -1\}, \cdot\,)$ with $\{1, -1\} \in \mathbb{Z}$.

9. $(M_{m,n}(F)), +)$ where $M_{m,n}(F)$ denotes the set of all $m \times n$ matrices over a field F and the operation is matrix addition; e is the zero matrix of size $m \times n$; inverse of $A \in M_{m,n}(F)$ is $-A$.

10. $(GL(n, F), \cdot\,)$ where $GL(n, F)$ denotes the set of all invertible matrices of size $n \times n$ over the field F and the operation is matrix multiplication; $e = I$, the $n \times n$ identity matrix.

11. $(SL(n, F), \cdot\,)$ where $SL(n, F)$ denotes the set of all $n \times n$–matrices over the field F which have determinant 1 and the operation is matrix multiplication; $e = I$, the $n \times n$ identity matrix.

12. $(S_X, \circ)$ where X is a nonempty set and S_X is the set of all bijections $\beta : X \to X$ with operation composition of functions; $e = 1_X$, the identity function on X.

13. $(S_n, \circ)$ where $S_n = S_X$ with $X = \{1, 2, \ldots, n\}$, the group of all permutations of $\{1, 2, \ldots, n\}$ with operation composition of functions. If $\beta \in S_n$, use matrix notation for β. Write

$$\beta = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta(1) & \beta(2) & \ldots & \beta(n) \end{pmatrix}.$$

Note that S_n has order $n!$. In general, for $\alpha, \beta \in S_n$, $\alpha \circ \beta \neq \beta \circ \alpha$. The identity function is a bijection, thus

$$e = 1_{\{1,\ldots,n\}} = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

The inverse of $\beta \in S_n$ can be found by interchanging the rows of the matrix representing β. For example, the inverse of

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$$

is

$$\beta^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

which equals

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Let $(G, *)$ be a group. A *subgroup* of G is a subset H of G such that $(H, *)$ is a group on its own right. If H is a subgroup of G, this is indicated by writing $H \leq G$. For example, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$; similarly, $\{1\} \leq \{1, -1\} \leq \mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$, and $SL(n, F) \leq GL(n, F)$ when F is a field.

Exercise 5. *Prove: For every group G, $\{e\} \leq G$ and $G \leq G$.*

Exercise 6. *Is $\mathbb{Q}^+ \leq \mathbb{Q}$? Is $\mathbb{R}^+ \leq \mathbb{R}^*$? Is $\mathbb{Z}_3 \leq \mathbb{Z}_4$? Is $S_3 \leq S_4$?*

Two Subgroup Criteria. *For a subset $H \subseteq G$ of a multiplicative group G, the following conditions are equivalent:*

1) H is a subgroup of G.

2) H is nonempty, and $a, b \in H$ implies $ab \in H$ and $a^{-1} \in H$.

3) H is nonempty, and $a, b \in H$ implies $ab^{-1} \in H$. [GG, page 123f, 3.9 and 3.10].

If $(G, +)$ is an additive group and $H \subseteq G$, then $H \leq G$ is equivalent to the additive versions versions of 2) and 3), i.e.

2^+*) H is nonempty, and $a, b \in H$ implies that $a + b \in H$ and $-a \in H$.*

3^+*) H is nonempty, and $a, b \in H$ implies $a - b \in H$.*

Integral powers and multiples. Let $a \in G$ where $(G, \cdot)$ is a multiplicative group. Define $a^0 = e, a^1 = a, a^2 = a \cdot a$ etc., i.e. for $n \in \mathbb{N}$, a^n is the product of n factors each of which equals a; define $a^{-n} = (a^{-1})^n$. The *Laws of Exponents* hold: For all integers m and n, $a^{m+n} = a^m a^n$ and $a^{mn} = (a^m)^n$. If $a \in G$ where $(G, +)$ is an additive group, one writes integral multiples instead of powers. Thus, $0a = e, 1a = a, 2a = a + a$ etc., i.e. for $n \in \mathbb{N}$, na is the sum of n terms each of which equals a; define $(-n)a = n(-a)$. The *Laws of Multiples* are: For all integers m and n, $(m + n)a = ma + na$ and $(mn)a = m(na)$.

Cyclic Subgroups. Let $(G, \cdot)$ be a multiplicative group and $a \in G$. If H is a subgroup of G containing a, then, by the subgroup criteria, H also contains a^{-1}, and closure of the operation in H implies $a \cdot a^{-1} = e = a^0 \in H$; closure also implies that, for every positive integer n, a^n and $(a^{-1})^n = a^{-n}$ must belong to H. Thus,

$$\{a^k : k \in \mathbb{Z}\} \subseteq H\,.$$

It turns out that the set of all integral powers of a forms a subgroup of G called the *cyclic subgroup generated by* a and denoted by $\langle a \rangle$. This is the smallest subgroup of G containing the element a. If $(G, +)$ is an additive group, we write integral multiples instead of powers. In this case, the cyclic group generated by a is $\langle a \rangle = \{na : n \in \mathbb{Z}\}$. For example, for $2 \in \mathbb{Q}^+$,

$\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\}$, while for $2 \in \mathbb{Q}$, $\langle 2 \rangle = \{n2 : n \in \mathbb{Z}\}$ which is usually denoted by $2\mathbb{Z}$. (Is $(\mathbb{Q}, \cdot\,)$ a group?)

Homomorphisms. Throughout, $(G, \circ)$ and $(H, *)$ are groups with identity elements e_G and e_H, respectively. Notation will mostly be multiplicative, e.g. write a^{-1} for the inverse of a group element a. A *homomorphism* from G to H is a mapping $\alpha : G \to H$ such that $\alpha(a \circ b) = \alpha(a) * \alpha(b)$ for all $a, b \in G$.

Examples. Each of the following maps is a homomorphism.

1. $(G, \circ) = (\mathbb{Z}, +)$ and $(H, *) = (\mathbb{R}^+, \cdot\,)$, define $\alpha : \mathbb{Z} \to \mathbb{R}^+$ by $\alpha(n) = 2^n$ for all $n \in \mathbb{Z}$.

2. $(G, \circ) = (GL(2, \mathbb{R}), \cdot\,)$ and $(H, *) = (\mathbb{R}^*, \cdot\,)$, define $\beta : GL(2, \mathbb{R}) \to \mathbb{R}^*$ by $\beta(A) = \det(A)$ for each $A \in GL(2, \mathbb{R})$.

3. $(G, \circ) = (\mathbb{Z}, +)$ and $(H, *) = (\mathbb{Z}_m, +)$, where $m \geq 1$ is some fixed integer. Then define $\gamma : \mathbb{Z} \to \mathbb{Z}_m$ by $\gamma(k) = [k]$ for all $k \in \mathbb{Z}$.

4. $(G, \circ) = (\mathbb{Z}_4, +)$ and $(H, *) = (\mathbb{C}^*, \cdot\,)$, define $\delta : \mathbb{Z}_4 \to \mathbb{C}^*$ by $\delta([k]) = i^k$ for all $[k] \in \mathbb{Z}_4$ where $i = \sqrt{-1}$.

5. $(G, \circ) = (\mathbb{R}^+, \cdot\,)$ and $(H, *) = (\mathbb{R}, +)$, define $\varphi : \mathbb{R}^+ \to \mathbb{R}$ by $\varphi(x) = \ln x$ for each $x \in \mathbb{R}^+$.

Exercise 7. *Prove that each of the five maps is a (well–defined) homomorphism.*

Notice that the first and the fourth maps are one–to–one but not onto; the second and third maps are onto but not one–to–one; and the last map is a homomorphism which is both one–to–one and onto. This prompts:

Definition. An *isomorphism* from G to H is a homomorphism from G to H which is both one–to–one and onto. Two groups G and H are *isomorphic* if there exists an isomorphism from G onto H. If G and H are isomorphic, this is symbolized by writing $G \cong H$.

Thus, from Example 5, the groups $(\mathbb{R}^+, \cdot\,)$ and $(\mathbb{R}, +)$ are isomorphic, and so are the groups $(\mathbb{Z}_4, +)$ and the cyclic subgroup $\langle i \rangle$ of $\mathbb{C}^*$ generated by $i = \sqrt{-1}$.

Exercise 8. *Suppose that $\alpha : G \to H$ is an isomorphism. Prove that $\alpha^{-1} : H \to G$ is an isomorphism.*

Definition. Let $\alpha : G \to H$ be a homomorphism. Then:

(a) The *image* of α is $\mathrm{Im}\,(\alpha) = \{h \in H : h = \alpha(g) \text{ for some } g \in G\}$.

(b) The *kernel* of α is the set $\mathrm{Ker}\,(\alpha) = \{g \in G : \alpha(g) = e_H\}$.

Exercise 9. *Find the image and the kernel of each of the five homomorphisms in the Examples above.*

Proposition. *Let $\alpha : G \to H$ be a homomorphism. Then*

1) $\alpha(e_G) = e_H$;

2) For all $g \in G$, $\alpha(g^{-1}) = \alpha(g)^{-1}$;

3) $Im\,(\alpha)$ is a subgroup of H;

4) $Ker\,(\alpha)$ is a subgroup of G;

5) α is one–to–one if and only if $Ker(\alpha) = \{e_G\}$;
6) For all $k \in Ker(\alpha)$ and for all $x \in G$, $x \circ k \circ x^{-1} \in Ker(\alpha)$.

Exercise 10. *Prove this proposition.*

Definition. A *normal subgroup* of a group $(G, \circ)$ is a subgroup N of G such that $x \circ n \circ x^{-1} \in N$ for all $x \in G$ and for all $n \in N$.

Thus, the last part of the Proposition above may be restated by saying that the kernel of a group homomorphism is always a normal subgroup of the domain group. Note that every subgroup of an abelian group is normal. Also, for any group G, the *trivial subgroup* $\{e_G\}$ and the group G itself are normal subgroups of G.

Cosets. Let K be a subgroup of a group $(G, \circ)$ and let $x \in G$. The *left coset of K in G containing x is the set*

$$x \circ K = \{x \circ k \, : \, k \in K\} \, .$$

Notice that $e_G \circ K = K$ so that the subgroup K itself is a left coset of K in G.

Examples. 1. Let $m = 5$ and $K = 5\mathbb{Z} \leq \mathbb{Z}$. For any $z \in \mathbb{Z}$, the congruence class of z modulo 5 is $[z] = z + K$, the left coset of K in $\mathbb{Z}$ containing z.

2. Let $K = S(2, \mathbb{R}) \leq G(2, \mathbb{R})$. For a matrix $A \in S(2, \mathbb{R})$, the left coset $A \cdot S(2, \mathbb{R})$ consists of all matrices in $G(2, \mathbb{R})$ which have the same determinant as A.

A *partition* of a nonempty set X is a collection $\mathcal{P}$ of subsets of X such that (i) no member of $\mathcal{P}$ is empty, (ii) any two distinct members of $\mathcal{P}$ are disjoint, and (iii) the union of all subsets in $\mathcal{P}$ equals X. Let $(G, \circ)$ be a group with subgroup K and $x \in G$, then $x = x \circ e_G \in x \circ K$ proving $x \circ K$ is a nonempty subset of G. In fact, one has the following result [R, page 140, Lemma 2.31]:

Proposition. *Let K be a subgroup of the group $(G, \circ)$. Then the set*

$$\mathcal{P} = \{x \circ K \, : \, x \in G\}$$

of all left cosets of K in G forms a partition of G.

Exercise 11. *Suppose that $(G, \circ)$ is a finite group, K is a subgroup of G, and $x \in G$. Prove that $|x \circ K| = |K|$.*

Lagrange's Theorem. *Let K be a subgroup of the finite group $(G, \circ)$ and let $\mathcal{P}$ denote the set of all left cosets of K in G. Then $|G| = |K| \cdot |\mathcal{P}|$.*

Exercise 12. *Prove Lagrange's Theorem.*

Exercise 13. *Suppose G is a group of finite order 12 and K is a subgroup of G. Find all integers m which might be equal the order of K.*

Quotient Groups. Let $(G, \circ)$ be a group and let N be a normal subgroup of G. Consider the set of all left cosets of N in G and denote it by G/N:

$$G/N = \{x \circ N \,|\, x \in G\} \, .$$

Exercise 14. *Find G/N in each of the following cases:*

a) $(G, \circ) = (S_3, \circ)$ *and* $N = \langle \beta \rangle$ *with* $\beta(1) = 2, \beta(2) = 3, \beta(3) = 1$.

b) $(G, \circ) = (\mathbb{Z}, +)$ *and* $N = m\mathbb{Z}$ *where* $m \geq 2$ *is some fixed integer.*

Theorem. *Let* $(G, \circ)$ *be a group and let* N *be a normal subgroup of* G. *Define an operation, also denoted by* $\circ$, *on the set* G/N *by* $(x \circ N) \circ (y \circ N) = (x \circ y) \circ N$ *for all* $x, y \in G$. *Then:*

a) This product of cosets is well defined.

b) $(G/N, \circ)$ *is a group with identity* $e_{G/N} = e_G \circ N = N$; *for each* $x \in G$, $(x \circ N)^{-1} = x^{-1} \circ N$.

c) The mapping $\nu : G \to G/N$ *defined by* $\nu(x) = x \circ N$ *for all* $x \in G$ *is a surjective homomorphism from* G *to* G/N, *and* $Ker(\nu) = N$.

Exercise 15. *Prove this theorem.*

Definition. The group $(G/N, \circ)$ of the Theorem above is called the *quotient group* (or factor group) of G modulo N, and the surjective homomorphism $\nu : G \to G/N$ is said to be the *natural homomorphism* from G to its quotient group G/N.

The Isomorphism Theorem for Groups. A *homomorphic image* of the group $(G, \circ)$ is any group $(G', *)$ with the property that there exists a homomorphism $\eta : G \to G'$ from G onto G', i.e. $G' = \operatorname{Im} \eta$. Thus, if $\alpha : G \to H$ is a homomorphism of groups, then $\operatorname{Im} \alpha$ is a homomorphic image of G.

Examples. From the five examples of homomorphisms on page 5 of these notes, one observes:

1. $\langle 2 \rangle \leq \mathbb{R}^+$ is a homomorphic image of $(\mathbb{Z}, +)$.

2. $\mathbb{R}^*$ is a homomorphic image of $GL(2, \mathbb{R})$.

3. For each integer $m \geq 1$, $(\mathbb{Z}_m, +)$ is a homomorphic image of $(\mathbb{Z}, +)$.

4. The cyclic subgroup $\langle i \rangle \leq \mathbb{C}^*$ is a homomorphic image of $(\mathbb{Z}_4, +)$.

5. $(\mathbb{R}, +)$ is a homomorphic image of $(\mathbb{R}^+, \cdot)$.

The following fact is of fundamental importance in group theory. For a proof, see [R, page 166, Theorem 2.53] or [D, page 109, Theorem 23.1].

The (First) Isomorphism Theorem. *Let* $(G, \circ)$ *and* $(H, *)$ *be groups and let* $\alpha : G \to H$ *be a homomorphism. Then* $Ker\,\alpha$ *is a normal subgroup of* G, *and* $Im\,\alpha$ *is a subgroup of* H *which is isomorphic to the quotient group* $G/Ker\,\alpha$.

Exercise 16. *Consider the five examples of homomorphisms on page 5 of these notes. For each of these, (i) find a quotient group of* G *which is isomorphic to the image; and (ii) specify a mapping from this quotient group of* G *to the image which is an isomorphism.*

Exercise 17. *Let* $(G, \cdot)$ *be a multiplicative group with identity element* $e \in G$.

a) Is $G \cong G/\{e\}$? *Justify your answer.*

b) Describe the quotient group G/G. *What is its order?*

Exercise 18. *Let* $(G, \cdot)$ *be a multiplicative group with identity element* e, *and let* $a \in G$. *Prove:*

a) If $\langle a\rangle$ is an infinite set, then $\langle a\rangle$ is isomorphic to the additive group $\mathbb{Z}$ of all integers.

b) If $\langle a\rangle$ has finite order m, then $\langle a\rangle$ is isomorphic to the additive group $\mathbb{Z}_m$. (Hint: Argue that $\phi : k \mapsto a^k$, $k \in \mathbb{Z}$, is a surjective homomorphism from $(\mathbb{Z}, +)$ to $\langle a\rangle$, and that $\operatorname{Ker}\phi = m\mathbb{Z}$.)

Exercise 19. *Prove: Being isomorphic is an equivalence relation on the collection of all groups.*

Exercise 20. *Prove: If $\langle a\rangle$ and $\langle b\rangle$ are two cyclic groups of equal order, then $\langle a\rangle$ and $\langle b\rangle$ are isomorphic.* (Hint: Exercise 18 above.)

Exercise 21. *Prove: The multiplicative group of all nonzero real numbers is isomorphic to the quotient group $GL(2,\mathbb{R})/SL(2,\mathbb{R})$.*

3. Rings

A *ring* is a triple $(R, +, \cdot\,)$ where R is a set and $+$ and $\cdot$ are two binary operations on R satisfying the following conditions:

a) $(R, +)$ is an abelian group with identity element $0 = 0_R$.

b) For all $a, b, c \in R$, $(ab)c = a(bc)$.

c) For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If there exists an element $1 = 1_R \in R$ such that $1a = a1 = a$ for all $a \in R$, then R is said to be a *ring with identity*; if $ab = ba$ for all $a, b \in R$, then R is said to be a *commutative ring*.

Examples. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings with identity; the ring $\mathbb{E}$ of even integers is commutative but does not have an identity. Given a ring R, the set $M_n(R)$ of all $n \times n$–matrices with entries in R is a ring under the usual addition and multiplication of matrices. If $n \geq 2$ and R is a ring with identity $1 \neq 0$, then $M_n(R)$ is a ring with identity, namely the $n \times n$ identity matrix, but $M_n(R)$ is not commutative. The set $\mathbb{R}[x]$ of all polynomial functions in the indeterminate x with real coefficients is a ring under the usual addition and multiplication of polynomials. For any integer $m \geq 1$, $(\mathbb{Z}_m, +, \cdot\,)$ is a commutative ring with identity when multiplication is defined by $[k] \cdot [\ell] = [k \cdot \ell]$ for all $k, \ell \in \mathbb{Z}$.

Excercise 22. *Prove that multiplication in $\mathbb{Z}_m$ is well defined.*

If R is a ring with identity 1, one can show that 1 is unique. A *unit* of a ring R with identity is any element $u \in R$ for which there exists $v \in R$ satisfying $uv = vu = 1$. Again, one can show that, given a unit u, the element v with the property $uv = vu = 1$ is unique; thus, v is called the inverse of u and denoted by $v = u^{-1}$.

Exercise 23. *Let R be a ring with identity* 1. *Prove:*

a) $1_R = 0_R$ if and only if $R = \{0_R\}$.

b) The set $U(R)$ of all units in R is a group under the operation of multiplication defined in R.

A *field* is a commutative ring F with identity $1_F \neq 0_F$ such that every nonzero element of F is a unit, i.e. $U(F) = F - \{0\}$. Examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$ when p is a prime.

Ring Homomorphisms. Let $(R, +, \cdot\,)$ and $(S, +, \cdot\,)$ be rings. A *ring homomorphism* from R to S is a mapping $\alpha : R \to S$ such that $\alpha(a+b) = \alpha(a) + \alpha(b)$ and $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in R$.

Examples. Each of the following maps is ring a homomorphism.

1. Let R be the ring of integers and let $S = \mathbb{Z}_m$ be the ring of integers modulo m for some $m \geq 1$. Define $\alpha : \mathbb{Z} \to \mathbb{Z}_m$ by $\alpha(k) = [k]$ for all $k \in \mathbb{Z}$.

2. Let $R = \mathbb{R}$ and let $S = M_2(\mathbb{R})$ be the ring of all real 2×2–matrices. Define $\alpha : \mathbb{R} \to M_2(\mathbb{R})$ by by $\alpha(x) = \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)$ for all $x \in \mathbb{R}$.

3. Let $R = \mathbb{Z}$ and $S = M_n(\mathbb{C})$, and define $\alpha : \mathbb{Z} \to M_n(\mathbb{C})$ by $\alpha(k) = kI$, $k \in \mathbb{Z}$, where I denotes the $n \times n$ identity matrix.

4. Let $R = S = \mathbb{C}$ and define $\alpha : \mathbb{C} \to \mathbb{C}$ by $\alpha(a + bi) = a - bi$ where $a, b \in \mathbb{R}$.

Exercise 24. *Prove that each of the four maps is a ring homomorphism.*

Definition. A *ring isomorphism* from a ring R to a ring S is a ring homomorphism $\alpha : R \to S$ which is both one–to–one and onto. Two rings R and S are *isomorphic* if there exists a ring isomorphism from R onto S. If R and S are isomorphic, this is symbolized by writing $R \cong S$.

Examples. These rings are isomorphic.

1. Given an n–dimensional vector space V over a field F, the set $L(V, V))$ of all linear transformations $T : V \to V$ (with pointwise addition and composition of mappings as multiplication) is a ring which is isomorphic to the ring $M_n(F)$ of all $n \times n$–matrices over F.

2. Example 4 above is an isomorphism from the field of complex numbers to itself, also called an *automorphism*.

Exercise 25. *Prove: If* $\alpha : R \to S$ *is an isomorphism of rings, then* $\alpha^{-1} : S \to R$ *is an isomorphism of rings.*

Definition. Let $\alpha : R \to S$ be a ring homomorphism. Define:

(a) The *image* of α is the set $\mathrm{Im}\,(\alpha) = \{y \in S : y = \alpha(x) \text{ for some } x \in R\}$.

(b) The *kernel* of α is the set $\mathrm{Ker}\,(\alpha) = \{x \in R : \alpha(x) = 0_S\}$.

Notice that, if $\alpha : R \to S$ is a ring homomorphism, then α is also homomorphism from $(R, +)$ to $(S, +)$. Thus, kernels and images of ring homomorphisms give nothing new.

A *subring* of a ring R is a subset S of R which is a ring under the same operations as those in R.

Exercise 26. *Let* R *be a ring and let* $S \subseteq R$. *Prove:* S *is a subring of* R *if and only if: (i)* $(S, +)$ *is a subgroup of* $(R, +)$*, and (ii)* $(S, \cdot\,)$ *is closed, i.e.* $x, y \in S$ *implies* $xy \in S$.

Examples. Each of these are subrings.

1. The set $5\mathbb{Z}$ is a subring of the ring of integers.

2. The set of all upper triangular matrices in $M_n(\mathbb{R})$ is a subring of the ring of all real $n \times n$–matrices. (Ditto for the set of all lower triangular matrices and the set of all diagonal matrices in $M_n(\mathbb{R})$.)

Proposition. *Let R and S be rings and let $\alpha : R \to S$ be a ring homomorphism. Then*

1) $\alpha(0_R) = 0_S$.
2) For all $a \in R$, $\alpha(-a) = -\alpha(a)$.
3) $Im(\alpha)$ is a subring of S.
4) $Ker(\alpha)$ is a subring of R.
5) α is one–to–one if and only if $Ker(\alpha) = \{0_R\}$
6) For all $k \in Ker(\alpha)$ and for all $x \in R$, $xk \in Ker(\alpha)$ and $kx \in Ker(\alpha)$.

Exercise 27. *Let R be a ring.*
a) Prove: $a \cdot 0_R = 0_R = 0_R \cdot a$ for all $a \in R$.
b) Prove the Proposition on ring homomorphisms stated above.

Ideals. An *ideal* of a ring R is a subring I of R which is "closed under external–internal multiplication" in the sense that $i \in I$ implies that $xi \in I$ and $ix \in I$ for all $x \in R$. Thus, part 6) of the the proposition above implies that the kernel of a ring homomorphism is always an ideal of the domain ring. Given any ring R, both $\{0_R\}$ and R are ideals of R. For any fixed integer n, the set $n\mathbb{Z}$ of all integral multiples of n is an ideal of the ring of integers. For example, the ring $\mathbb{E} = 2\mathbb{Z}$ of even integers is an ideal of $\mathbb{Z}$.

In ring theory, ideals take on the role that normal subgroups play in group theory, namely they allow you to define quotient structures.

Quotient Rings. Let R be a ring and let I be an ideal of R. Then $(I, +)$ is a subgroup of $(R, +)$ which must be normal since $(R, +)$ is a commutative group. Thus, the set

$$R/I = \{a + I \,|\, a \in R\}$$

of all left cosets of I in the group $(R, +)$ is a group under the operation $(a+I)+(b+I) = (a+b)+I$; and $(R/I, +)$ is an abelian group since $(R, +)$ is abelian. Also from group theory, the mapping $\nu : R \to R/I$ defined by $\nu(a) = a + I$ for all $a \in R$ is a surjective group homomorphism from $(R, +)$ to $(R/I, +)$.

Exercise 28. *Let I be an ideal of the ring R and let $a, a', b, b' \in R$ such that $a + I = a' + I$ and $b + I = b' + I$. Prove that $(ab) + I = (a'b') + I$.*

Theorem. *Let R be a ring and let I be an ideal of R. Define a multiplication on the quotient group R/I by $(a+I)(b+I) = (ab)+I$ for all $a, b \in R$. Then:*
a) This multiplication is well defined.
b) R/I is a ring with $0_{R/I} = 0_R + I = I$; if R is a ring with identity 1_R, then so is R/I and $1_{R/I} = 1_R + I$.
c) The mapping $\nu : R \to R/I$ defined by $\nu(a) = a + I$ for all $a \in R$ is a surjective ring homomorphism from R to R/I, and $Ker(\nu) = I$.

Exercise 29. *Prove this theorem.*

Definition. The ring R/I of the Theorem is called the *quotient ring* of R modulo I.

The Isomorphism Theorem for Rings. Let R and S be rings. A *homomorphic image of* R is any ring R' with the property that there exists a ring homomorphism $\eta : R \to R'$ from R *onto* R'.

Examples. From the first three examples of ring homomorphisms above, one observes:

1. For every integer $m \geq 1$, the ring $\mathbb{Z}_m$ is a homomorphic image of $\mathbb{Z}$.

2. The subring of $M_2(\mathbb{R})$ consisting of all real diagonal 2×2–matrices with $(2,2)$–entry zero is a homomorphic image of the field $\mathbb{R}$.

3. The set of all matrices of the form $kI \in M_n(\mathbb{C})$ with k an integer and I the identity matrix is a subring of $M_n(\mathbb{C})$ and a homomorphic image of $\mathbb{Z}$.

A proof of the following theoreom can be found in [R, page 280, Theorem 3.71] or [GG, page 251, Theorem 6.13].

The (First) Isomorphism Theorem for Rings. *Let R and S be rings and let $\alpha : R \to S$ be a ring homomorphism from R to S. Then $Ker\,\alpha$ is an ideal of R, and $Im\,\alpha$ is a subring of S which is isomorphic to the quotient ring $R/Ker\,\alpha$.*

Exercise 30. *Let R be a commutative ring with identity $1 \neq 0$, and let I be an ideal of R. Prove: If $I \neq R$, then R/I is a commutative ring with identity $1 \neq 0$.*

Exercise 31. *Let R be a commutative ring with identity $1 \neq 0$, and let $a \in R$. Prove:*

a) The set $Ra = \{ra : r \in R\}$ is an ideal of R containing a. (Ra is called the principal ideal generated by a and is also denoted by (a)).

b) If R has no ideals other than R and $\{0\}$, then R is a field.

Exercise 32. *Let R be a ring and let I be an ideal of R.*

a) Prove: If J is an ideal of R such that $I \subseteq J$, then the set $J/I = \{j+I : j \in J\}$ is an ideal of R/I.

b) Suppose $\overline{J} \subseteq R/I$ is an ideal of R/I. Define $J = \{x \in R : x + I \in \overline{J}\}$. Prove: $I \subseteq J$ and J is an ideal of R.

4. Fields

One of the most useful applications of the Isomorphism Theorem for Rings occurs in the study of fields. One reason is that the set $F[x]$ of all polynomials in an indeterminate x over a field F is a commutative ring with identity $1 \neq 0$ which has the property that (i) the product of any two nonzero elements is nonzero, and (ii) every ideal of $F[x]$ is principal (see Exercise 31 of these notes). A commutative ring with identity $1 \neq 0$ which satisfies conditions (i) and (ii) is called a *principal ideal domain*, or a PID for short.

Throughout, F will denote a field. For p prime, $\mathbb{Z}_p$ is a field. Many texts replace congruence classes modulo p by their unique representatives in the set $\{0, \ldots, p-1\}$ so that $\mathbb{Z}_p = \{0, \ldots, p-1\}$.

Polynomials over F. A *polynomial* over F in the indeterminate x is an expression of the form

$$f = a_0 + a_1 x + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i \tag{1}$$

where $n \geq 0$ is an integer and $a_i \in F$, $i = 0, \ldots, n$. If

$$g = b_0 + b_1 x + \cdots + b_m x^m = \sum_{i=0}^{m} b_i x^i \tag{2}$$

is another polynomial over F, then we agree that $f = g$ if and only if there exists an integer k such that $a_i = b_i$ for all $i = 0, \ldots, k$ and $a_j = 0$ and $b_j = 0$ for all $j > k$. The *zero polynonial* is $0 = 0 + 0x = 0 + 0x + \cdots + 0x^n$. If f is a nonzero polynimial, then one can write

$$f = a_0 + a_1 x + \ldots a_n x^n, \; a_n \neq 0 \tag{3}$$

and n is called the *degree* of f, in symbols $n = \deg(f)$. A *constant polynomial* is one of the form $h = c$ with $c \in F$. Nonzero constant polynimials have degree one, and the degree of the zero polynomial is undefined.

If $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ are polynomials over F, one defines $f+g = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i$, and $fg = \sum_{i=0}^{n+m} c_i x^i$ where, for $i = 0, \ldots, n+m$, $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$. This definition, of course, requires $a_t = 0$ when $t > n$ and $b_t = 0$ when $t > m$.

For the proof of the following proposition, see [GG, page 294, 8.4, page 296, 8.5, and page 298, 8.7] noting that fields are integral domains.

Proposition. *The polynomial ring $F[x]$ over a field F is a commutative ring with identity $1 = 1_F$ and $0 = 0_F$. The set of constant polynomials is a subring of $F[x]$ which is isomorphic to F. In fact, for $a \in F$, the constant polynomial $h = a$ will identified with $a \in F$. If $f, g \in F[x]$ are nonzero, their product fg is nonzero, and deg(fg) = deg(f) + deg(g).*

Every polynomial f over F gives rise to a polynomial function from F to F, namely define $f(z) = \sum_{i=0}^{n} a_i z^i$ for $z \in F$ if $f = \sum_{i=0}^{n} a_i x^i$. If $F = \mathbb{R}$, it is true that two polynomials are equal if and only if they yield the same function from $\mathbb{R}$ to $\mathbb{R}$. Thus, a polynomial over $\mathbb{R}$ is identified with its polynomial function and written not just as f but as $f(x)$. This is done in calculus. However, if $F = \mathbb{Z}_2 = \{0, 1\}$, the polynomials $1+x, 1+x^2, 1+x^3, \ldots$ all define the same polynomial function when evaluated on $\mathbb{Z}_2$. But by our definition of polynomials over a field, these are distinct.

The Division Algorithm. *Let F be a field and let $f \in F[x]$ be a nonzero polynomial. Then, given any $g \in F[x]$, there exist unique $q, r \in F[x]$ such that $g = f \cdot q + r$, and either (i) $r = 0$, or (ii) $r \neq 0$ and deg$\,r <$ deg$\,f$.*

For a proof, see [GG, page 301]. Also note Example 1 [GG, page 303] which may serve as a model for your solution of Exercise 33.

Exercise 33. Let $f = 2x + 2$ and $g = x^3 + 2x + 2$.

a) Find $q, r \in \mathbb{R}$ such that $g = fq + r$.

b) Find $q, r \in \mathbb{Z}_3$ such that $g = fq + r$.

A consequence of the Division Algorithm is the following fact. See [R, page 245, 3.39] for a proof.

Corollary. *If F is a field then $F[x]$ is a Principal Ideal Domain (PID).*

Exercise 34. *Prove that $f \in F[x]$ is a unit if and only f is a nonzero constant polynomial.*

Irreducible Polynomials. A polynomial p over a field F is said to be *irreducible* if (i) p has positive degree (thus, p is not a constant polynomial, hence not zero and not a unit in $F[x]$), and (ii) $p = g \cdot h$ with $g, h \in F[x]$ implies that either g is a constant or h is a constant. Given any nonzero constant c, every $p \in F[x]$ has the trivial factorization $p = c(c^{-1}p)$. The point is that these are the only factorizations that p admits if p is irreducible.

Theorem. *Every polynomial f of positive degree over F is either irreducible or is a product of irreducible polynomials over F.*

The proof is by induction on the degree of f. There is even a uniqueness property which holds for this factorization but we shall not need this. See [D, page page 166], [GG, page 312, 8.24], or [R, page 261, 3.52] for a proof.

Maximal Ideals. An ideal M in a ring R is said to be a *maximal ideal* of R if (i) $M \neq R$, and (ii) $M \subseteq I$ with I an ideal of R implies $M = I$ or $I = R$. For example, if p is a prime, then $(p) = p\mathbb{Z}$ is a maximal ideal of Z.

Exercise 35. *Prove: If F is a field, then $\{0\}$ is a maximal ideal of F.*

Exercise 36. *Let R be a commutative ring with identity $1 \neq 0$ and let M be a maximal ideal of R. Prove: The quotient ring R/M is a field.* (Hint: Exercises 31 and 32 of these notes.)

Proposition. *Let $p \in F[x]$ be irreducible. Then the principal ideal (p) of $F[x]$ generated by p is maximal.*

Proof. Suppose $p \in F[x]$ is irreducible. Then $(p) \neq F[x]$ for otherwise $1 \in (p)$ and p would be a unit contradicting $\deg(p) > 0$ (see Exercise 34). Let I be an ideal of $F[x]$ containing (p). Since $F[x]$ is a PID, there exists $f \in F[x]$ such that $I = (f)$. Now, $p \in (p) \subseteq I$ implies $p = fg$ for some $g \in F[x]$. Irreducibility implies that f is a unit or g is a unit. If f is a unit, then $I = (f) = F[x]$; if g is a unit, then $f = pg^{-1} \in (p)$ from which we obtain that $I = (f) \subseteq (p) \subseteq I$ and $I = (p)$. This proves (p) is maximal.

Roots of Polynomials. If $f = \sum_{i=0}^{n} a_i x^i \in F[x]$ and $u \in F$, define $f(u) = \sum_{i=0}^{n} a_i u^i$. Clearly, $f(u) \in F$. A *root* of f in F is any element $v \in F$ such that $f(v) = 0$. You all have heard of the question vexing mathematicians before they invented irrational numbers: How could there be a root of the polynomial $f = x^2 - 2 \in \mathbb{Q}[x]$? The same struggle took place when mathematicians were disputing whether there could be a "number," called i for imaginary, that's a root of $x^2 + 1 \in \mathbb{R}[x]$. The conclusion of this refresher course on undergraduate algebra will consist of an argument that for any nonconstant polynomial f over any field F, there exists an extension field E of F in which f has a root.

The amount of work needed to prove this will depend on the definition of the word "extension field".

Let K be a field. A *subfield* of K is a subset L of K with the property that L is a field under the same operations of addition and multiplication which are defined for K.

Exercise 37. *A subset L of a field K is a subfield of K if and only if: (i)* $1_K \in L$, *(ii)* $a, b \in L$ *implies* $a - b \in L$*; and (iii) if u and v are nonzero elements in L, then* $uv^{-1} \in L$.

Define E to be an *extension field* of F if there exists an injective ring homomorphism $\phi : F \to E$.

Lemma. *Let E be a field and let* $\phi : F \to E$ *be an injective ring homomorphism. Then:*

a) $Im\,\phi = \overline{F}$ *is a subfield of E which is isomorphic to F.*

b) The map $\overline{\phi} : F[x] \to \overline{F}[x]$ *defined by* $\overline{\phi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \phi(a_i)x^i$, $a_i \in F$*, is a ring isomorphism.*

Exercise 38. *Prove this Lemma.*

Proposition. *If* $f = \sum_{i=0}^{n} a_i x^i \in F[x]$ *is a polynomial of positive degree over a field F, then there exists a field E and an injective ring homomorphism* $\phi : F \to E$ *such that* $\sum_{i=0}^{n} \phi(a_i)v^i = 0$ *for some* $v \in E$.

Proof. Assume the hypothesis. By the theorem on page 13, $f = p_1 \dots p_r$ with $r \geq 1$ and each $p_i \in F[x]$ irreducible. Let $p = p_1$ and define $E = F[x]/(p)$. By Exercise 36 and the Proposition on page 13 of these notes, E is a field, and the natural map $\nu : F[x] \to E$ is a surjective ring homomorphism with kernel (p). Let $\phi : F \to E$ be the restriction of ν to F, i.e. $\phi(u) = \nu(u) = u + (p)$ for all $u \in F$. Then ϕ is an injective ring homomorphism. Since $f = p(p_2 \dots p_r) \in (p) = \operatorname{Ker}\nu$, we have $\nu(f) = f + (p) = 0_E$. Hence

$$0 = f + (p) = \sum_{i=0}^{n} a_i x^i + (p) = \sum_{i=0}^{n} (a_i + (p))(x + (p))^i\,.$$

Define $v = x + (p)$. Then $v \in E$, and substituting we obtain

$$0 = \phi(a_0) + \phi(a_1)v + \cdots + \phi(a_n)v^m$$

as claimed.

Using some elementary set theory and logic, one can prove the following result (see Hausen's Class Diary for MATH 6303, Spring 2005–available upon request by email to hausen@uh.edu).

Lemma. *Let E and F be fields and suppose* $\phi : F \to E$ *is an injective ring homomorphism. Then there exists a field K with the following properties: (i) F is a subfield of K; and (ii) there exists a ring isomorphism* $\sigma : K \to E$ *such that* $\sigma(a) = \phi(a)$ *for all* $a \in F$.

This Lemma allows one to construct a field K containing F as a subfield in which the nonconstant polynomial f over F has a root:

Theorem. *Given a polynomial $f = \sum_{i=0}^{n} a_i x^i$ of positive degree over the field F, there exists a field K containing F as a subfield such that $f(w) = 0$ for some $w \in K$.*

Proof. Assume the hypothesis of the theorem. Use the notation of the Proposition on page 14 and its proof, and recall that the inverse of a ring isomorphism is a ring isomorphism (Exercise 25, page 9). Then the Lemma implies that

$$0_K = \sigma^{-1}(0_E) = \sigma^{-1}(\sum_{i=0}^{n} \phi(a_i)v^i) = \sum_{i=0}^{n} \sigma^{-1}\phi(a_i)(\sigma^{-1}(v))^i .$$

Since $\phi(a) = \sigma(a)$ for all $a \in F$,

$$0_K = \sum_{i=0}^{n} \sigma^{-1}\sigma(a_i)(\sigma^{-1}(v))^i = \sum_{i=0}^{n} a_i(\sigma^{-1}(v))^i = f(\sigma^{-1}(v)) .$$

Hence, $w = \sigma^{-1}(v) \in K$ is a root of f in K.

The End