Math Review Notes—Abstract Algebra

Gregory Faletto

Contents

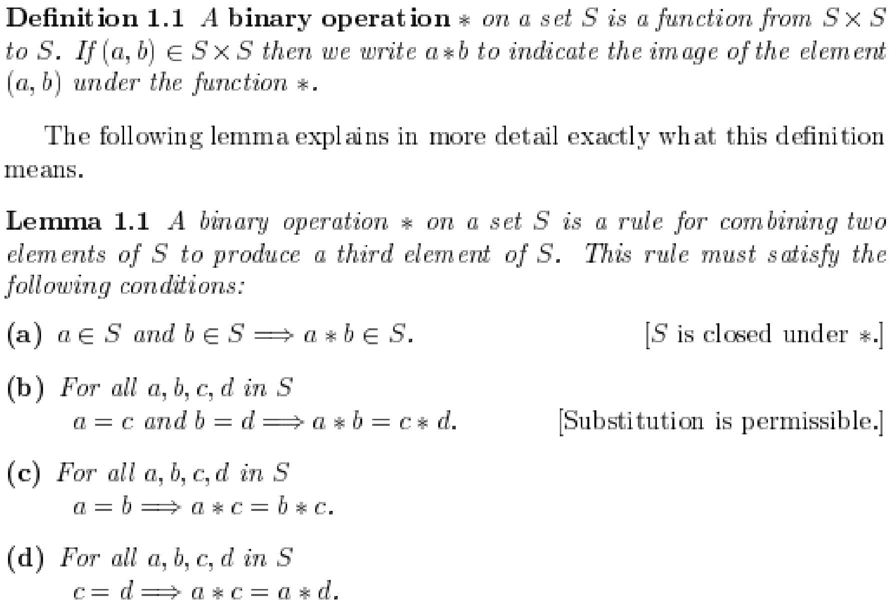
Last updated May 1, 2020

Chapter 1

Abstract Algebra

These are my notes from reading *Elementary Abstract Algebra* by W. Edwin Clark, available for free download on his website: http://shell.cas.usf.edu/~wclark/#ELEMENTARY_ABSTRACT_ALGEBRA

1.1 Chapter 1: Binary Operations



Definition 1.1 *A* **binary operation** $*$ *on a set S is a function from $S \times S$ to S. If $(a, b) \in S \times S$ then we write $a*b$ to indicate the image of the element (a, b) under the function $*$.*

The following lemma explains in more detail exactly what this definition means.

Lemma 1.1 *A binary operation $*$ on a set S is a rule for combining two elements of S to produce a third element of S. This rule must satisfy the following conditions:*

(a) $a \in S$ *and* $b \in S \Longrightarrow a * b \in S$. [$S$ is closed under $*$.]

(b) *For all* a, b, c, d *in* S
$a = c$ *and* $b = d \Longrightarrow a * b = c * d$. [Substitution is permissible.]

(c) *For all* a, b, c, d *in* S
$a = b \Longrightarrow a * c = b * c$.

(d) *For all* a, b, c, d *in* S
$c = d \Longrightarrow a * c = a * d$.

Definition: A **function** f from the set A to the set B is a rule which assigns to each element $a \in A$ an element $f(a) \in B$ in such a way that the following condition holds for all $x, y \in A$:

$$x = y \implies f(x) = f(y)$$

To indicate that f is a function from A to B we write $f : A \to B$. The set A is called the **domain** of f and the set B is called the **codomain** of f.

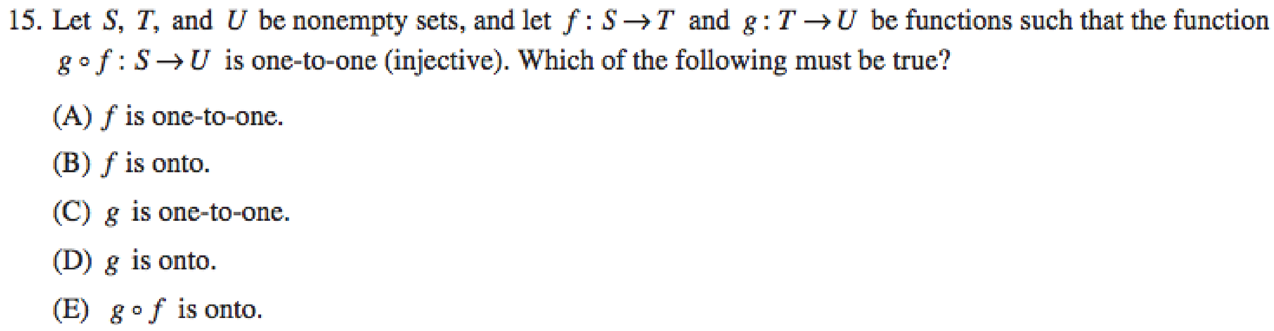
A function $f : A \to B$ is said to be **one-to-one** or **injective** if the following condition holds for all $x, y \in A$:

$$f(x) = f(y) \implies x = y$$

A function $f : A \to B$ is said to be **onto** or **surjective** if the following condition holds:

$$\forall\, b \in B\ \exists\, a \in A \mid f(a) = b$$

A function $f : A \to B$ is said to be **bijective** if it is both one-to-one and onto. Then f is sometimes said to be a **bijection** or a **one-to-one correspondence** between A and B.



15. Let S, T, and U be nonempty sets, and let $f : S \to T$ and $g : T \to U$ be functions such that the function $g \circ f : S \to U$ is one-to-one (injective). Which of the following must be true?

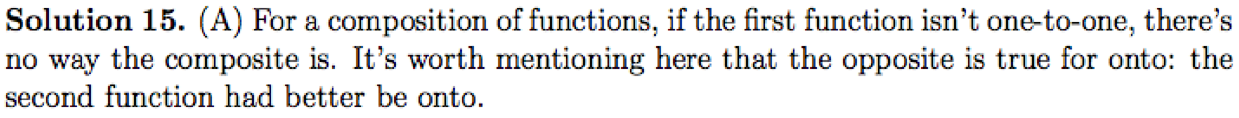
(A) f is one-to-one.

(B) f is onto.

(C) g is one-to-one.

(D) g is onto.

(E) $g \circ f$ is onto.



Solution 15. (A) For a composition of functions, if the first function isn't one-to-one, there's no way the composite is. It's worth mentioning here that the opposite is true for onto: the second function had better be onto.

Let S be a set. The **power set** $\mathcal{P}(S)$ of S is the set of all subsets of S (including S itself).

Definition 1.2 *Assume that $*$ is a binary operation on the set S.*

1. *We say that $*$ is* **associative** *if*

$$x * (y * z) = (x * y) * z \quad \textit{for all } x, y, z \in S.$$

2. *We say that an element e in S is an* **identity** *with respect to $*$ if*

$$x * e = x \textit{ and } e * x = x \quad \textit{for all } x \textit{ in } S.$$

3. *Let $e \in S$ be an identity with respect to $*$. Given $x \in S$ we say that an element $y \in S$ is an* **inverse** *of x if both*

$$x * y = e \textit{ and } y * x = e.$$

4. *We say that $*$ is* **commutative** *if*

$$x * y = y * x \quad \textit{for all } x, y \in S.$$

5. *We say that an element a of S is* **idempotent** *with respect to $*$ if*

$$a * a = a.$$

6. *We say that an element z of S is a* **zero** *with respect to $*$ if*

$$z * x = z \textit{ and } x * z = z \quad \textit{for all } x \in S.$$

For each integer $n \geq 2$ define the set

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

For all $a, b \in \mathbb{Z}_n$ let

$$a + b = \text{remainder when the ordinary sum of a and b is divided by n}$$

and

$$a \cdot b = \text{remainder when the ordinary product of a and b is divided by n.}$$

These binary operations are referred to as **addition modulo** n and **multiplication modulo** n. The integer n in $\mathbb{Z}_n$ is called the **modulus**. The plural of modulus is **moduli**.

Let K denote any one of the following: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$.

$$M_n(K)$$

is the set of all $n \times n$ matrices containing elements of K.

$$GL(n, K)$$

is the set of all matrices in $M_n(K)$ with non-zero determinant. $(GL(n, k), \cdot)$ is called the **general linear group of degree n over K**. It is non-abelian.

$$SL(n, K) = \{A \in GL(n, K) \mid \det(A) = 1\}$$

$SL(n, K)$ is called the **Special Linear Group of degree** n **over** K.

1.2 Chapter 2: Groups

Definition 1.2.1. Definition A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following properties:

1. **The binary operation is associative on G:** $\forall\ x, y, z \in G$,

$$x * (y * z) = (x * y) * z$$

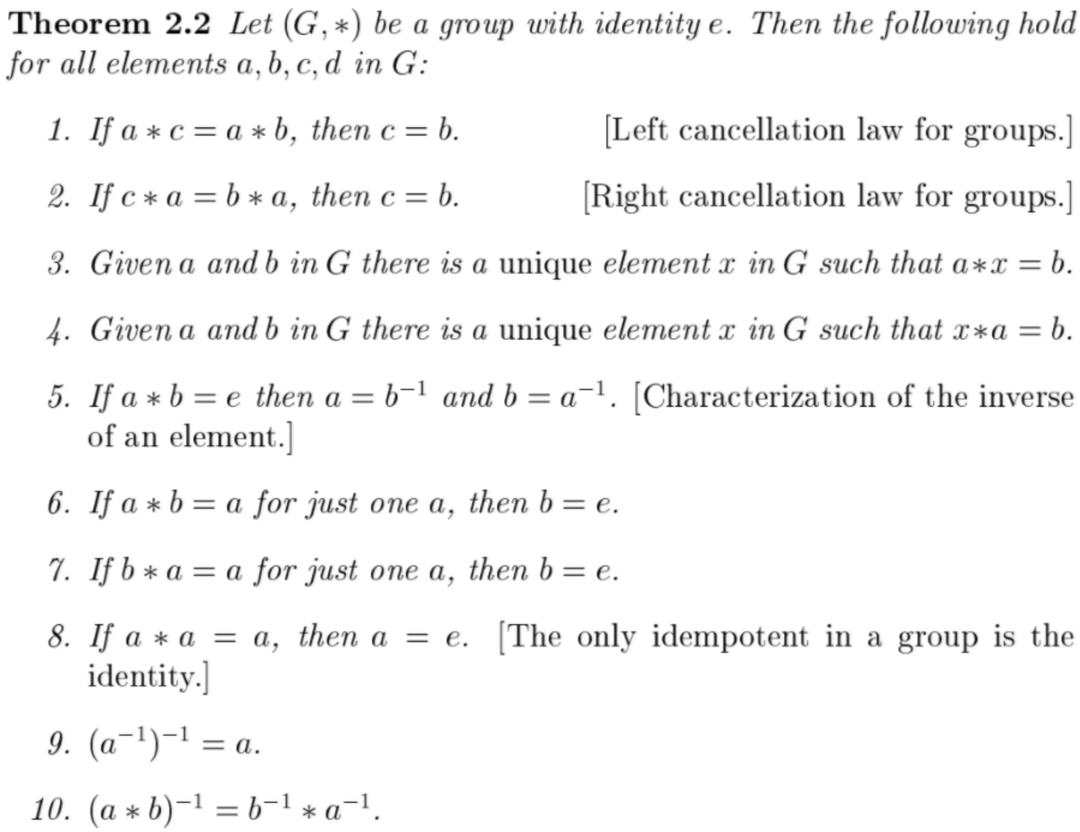
2. **The binary operation contains a (unique) identity in G:** $\exists\ e \in G \mid \forall\ x \in G$

$$e * x = x,\ x * e = x$$

3. **Every element in G has a (unique) inverse on $*$ in G:** $\forall\ x \in G\ \exists\ y \in G \mid$

$$x * y = e, y * x = e$$

A group $(G, *)$ is said to be **abelian** if $\forall\ x, y \in G,\ \ x * y = y * x$. A group is said to be **non-abelian** if it is not abelian.



Theorem 2.2 *Let $(G, *)$ be a group with identity e. Then the following hold for all elements a, b, c, d in G:*

1. *If $a * c = a * b$, then $c = b$.* [Left cancellation law for groups.]
2. *If $c * a = b * a$, then $c = b$.* [Right cancellation law for groups.]
3. *Given a and b in G there is a* unique *element x in G such that $a * x = b$.*
4. *Given a and b in G there is a* unique *element x in G such that $x * a = b$.*
5. *If $a * b = e$ then $a = b^{-1}$ and $b = a^{-1}$.* [Characterization of the inverse of an element.]
6. *If $a * b = a$ for just one a, then $b = e$.*
7. *If $b * a = a$ for just one a, then $b = e$.*
8. *If $a * a = a$, then $a = e$.* [The only idempotent in a group is the identity.]
9. *$(a^{-1})^{-1} = a$.*
10. *$(a * b)^{-1} = b^{-1} * a^{-1}$.*

1.3 Chapter 3: The Symmetric Groups

If n is a positive integer,

$$[n] = \{1, 2, \ldots, n\}$$

A **permutation** of $[n]$ is a one-to-one, onto function from $[n]$ to $[n]$, and

$$S_n$$

is the set of all permutations of $[n]$.

The identity of S_n is the so-called **identity function**

$$\iota : [n] \to [n]$$

which is defined by the rule

$$\iota(x) = x, \quad \forall\, x \in [n]$$

The inverse of an element $\sigma \in S_n$: Suppose $\sigma \in S_n$. Since σ is by definition one-to-one and onto, the rule

$$\sigma^{-1}(y) = x \iff \sigma(x) = y$$

defines a function $\sigma^{-1} : [n] \to [n]$. This function σ^{-1} is also one-to-one and onto and satisfies

$$\sigma\sigma^{-1} = \iota \text{ and } \sigma^{-1}\sigma = \iota$$

so it is the inverse of σ in the group sense also.

Since the binary operation of composition on S_n is associative $[(\gamma\beta)\alpha = \gamma(\beta\alpha)]$, S_n under the binary operation of composition is a group (it is associative, it has an inverse, and it has an identity).

Definition 3.2 *Let $i_1, i_2, \dots, i_k$ be a list of k distinct elements from $[n]$. Define a permuation σ in S_n as follows:*

$$\begin{aligned} \sigma(i_1) &= i_2 \\ \sigma(i_2) &= i_3 \\ \sigma(i_3) &= i_4 \\ \vdots & \quad \vdots \quad \vdots \\ \sigma(i_{k-1}) &= i_k \\ \sigma(i_k) &= i_1 \end{aligned}$$

and if $x \notin \{i_1, i_2, \dots, i_k\}$ then

$$\sigma(x) = x$$

Such a permutation is called a **cycle** *or a* k-**cycle** *and is denoted by*

$$(i_1 \ i_2 \ \cdots \ i_k).$$

If $k = 1$ then the cycle $\sigma = (i_1)$ is just the identity function, i.e., $\sigma = \iota$.

Two cycles $(i_1 \ i_2 \ \dots \ i_k)$ and $(j_1 \ j_2 \ \dots \ j_l)$ are said to be **disjoint** if the sets $\{i_1, i_2, \dots, i_k\}$ and $\{j_1, j_2, \dots, j_l\}$ are disjoint.

So for example, the cycles (1 2 3) and (4 5 8) are disjoint, but the cycles (1 2 3) and (4 2 8) are not disjoint.

If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.

Theorem 3.4 *Every element $\sigma \in S_n$, $n \geq 2$, can be written as a product*

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_m \tag{3.1}$$

where $\sigma_1, \sigma_2, \dots, \sigma_m$ are pairwise disjoint cycles, that is, for $i \neq j$, σ_i and σ_j are disjoint. If all 1-cycles of σ are included, the factors are unique except for the order. ■

The factorization (3.1) is called the **disjoint cycle decomposition of** σ.

An element of S_n is called a **transposition** if and only if it is a 2-cycle.

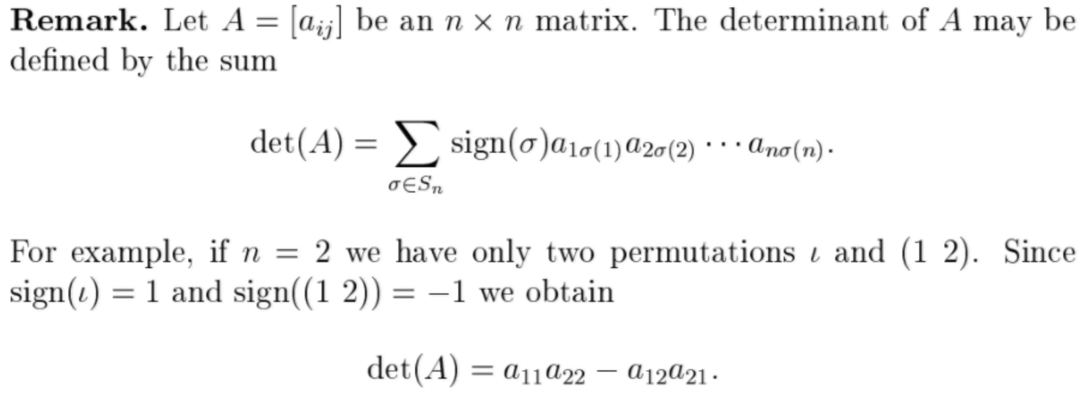
Every element of S_n can be written as a product of transpositions. The factors of such a product are not unique. However, if $\sigma \in S_n$ can be written as a product of k transpositions and if the same σ can also be written as a product of l transpositions, then k and l have the same parity.

A permutation is **even** if it is a product of an even number of transpositions and **odd** if it is a product of an odd number of transpositions. We define the function sign : $S_n \to \{1, -1\}$ by

$$\operatorname{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

If $n = 1$ then there are no transpositions. In this case, to be complete we define the identity permutation ι to be even.

If σ is a k-cycle, then $\operatorname{sign}(\sigma) = 1$ if k is odd and $\operatorname{sign}(\sigma) = -1$ if k is even.



Remark. Let $A = [a_{ij}]$ be an $n \times n$ matrix. The determinant of A may be defined by the sum

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

For example, if $n = 2$ we have only two permutations ι and $(1\ 2)$. Since $\operatorname{sign}(\iota) = 1$ and $\operatorname{sign}((1\ 2)) = -1$ we obtain

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Definition: If $(G, *)$ is a group, the number of elements in G is called the **order** of G. We use $|G|$ to denote the order of G. Note that $|G|$ may be finite or infinite.

Let

$$A_n$$

be the set of all even permutations in the group S_n. A_n is called the **alternating group of degree** n.

1.4 Chapter 4: Subgroups

Definition: Let G be a group. A **subgroup** of G is a subset H of G which satisfies the following three conditions:

1. $e \in H$

2. $a, b \in H \implies ab \in H$

3. $a \in H \implies a^{-1} \in H$

If H is a subgroup of G, we write $H \leq G$. The subgroups $\{e\}$ and G are said to be **trivial** subgroups of G.

Every finite subgroup may be thought of as a subgroup of one of the groups S_n.

Let A_n be the set of all even permutations in the group S_n. A_n is then a subgroup of S_n. A_n is called the **alternating group of degree** n.

Let a be an element of the group G. If $\exists\ n \in \mathbb{N} \mid a^n = e$ we say that a has **finite order** and we define

$$\mathrm{o}(a) = \min\{n \in \mathbb{N} \mid a^n = e\}$$

If $a^n \neq e\ \forall\ n \in \mathbb{N}$ we say that a has **infinite order** and we define

$$\mathrm{o}(a) = \infty$$

In either case we call $\mathrm{o}(a)$ the **order** of a. Note carefully the difference between the order of a group and the order of an element of a group. Note also that $a = e \iff \mathrm{o}(a) = 1$. So every element of a group other than e has order $n \geq 2$ or ∞.

Let a be an element of group G. Define

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

We call $\langle a \rangle$ the **subgroup of** G **generated by** a. Note that $e = a^0$ and a^{-1} are in $\langle a \rangle$.

Theorem. For each $a \in G$, $\langle a \rangle$ is a subgroup of G. $\langle a \rangle$ contains a and is the smallest subgroup of G containing a.

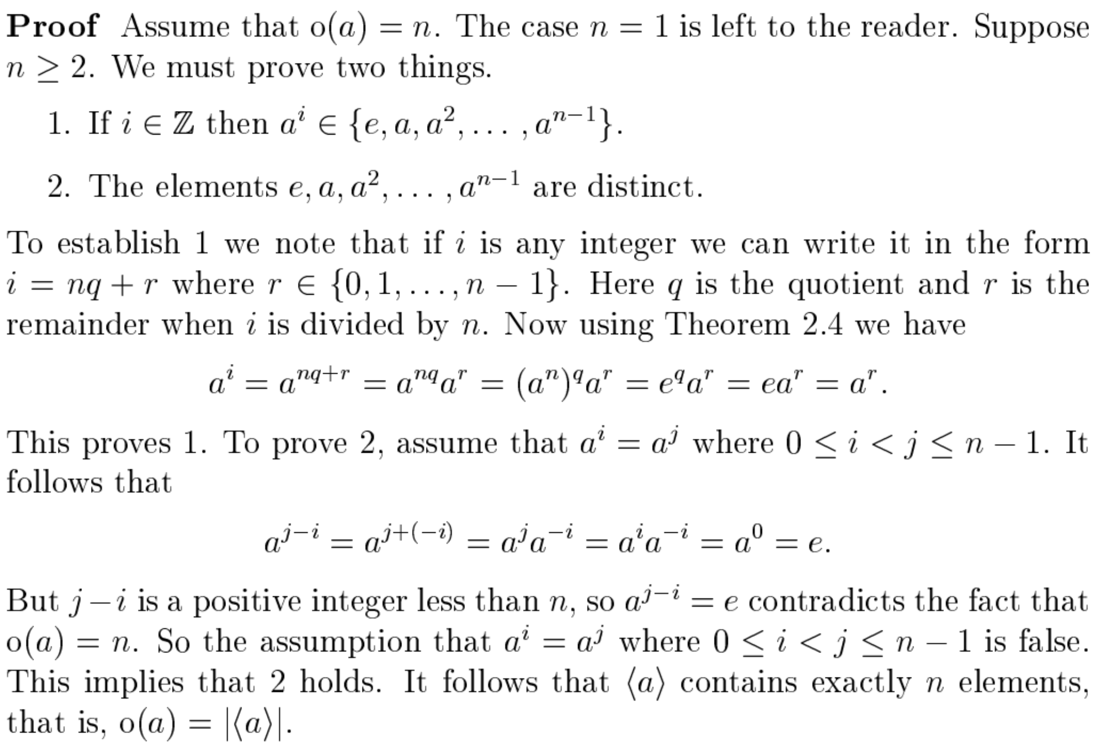
Proof of second statement. If H is any subgroup of G containing a, $\langle a \rangle \subseteq H$ since H is closed under taking products and inverses. That is, every subgroup of G containing a also contains $\langle a \rangle$. This implies that $\langle a \rangle$ is the smallest subgroup of G containing a.

Theorem. Let G be a group and let $a \in G$. If $\mathrm{o}(a) = 1$, then $\langle a \rangle = \{e\}$. If $\mathrm{o}(a) = n$ where $n \geq 2$, then

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

and the elements $e, a, a^2, \dots, a^{n-1}$ are distinct; that is,

$$\mathrm{o}(a) = |\langle a \rangle|$$



Proof Assume that $\mathrm{o}(a) = n$. The case $n = 1$ is left to the reader. Suppose $n \geq 2$. We must prove two things.

1. If $i \in \mathbb{Z}$ then $a^i \in \{e, a, a^2, \dots, a^{n-1}\}$.
2. The elements $e, a, a^2, \dots, a^{n-1}$ are distinct.

To establish 1 we note that if i is any integer we can write it in the form $i = nq + r$ where $r \in \{0, 1, \dots, n-1\}$. Here q is the quotient and r is the remainder when i is divided by n. Now using Theorem 2.4 we have

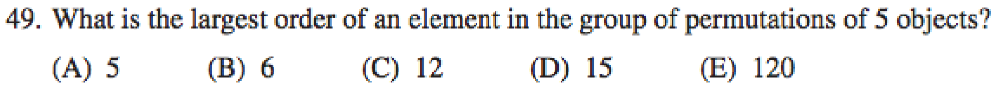
$$a^i = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

This proves 1. To prove 2, assume that $a^i = a^j$ where $0 \leq i < j \leq n-1$. It follows that

$$a^{j-i} = a^{j+(-i)} = a^j a^{-i} = a^i a^{-i} = a^0 = e.$$

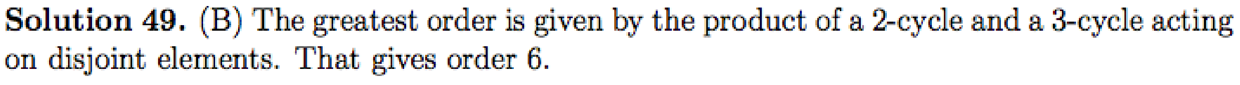
But $j - i$ is a positive integer less than n, so $a^{j-i} = e$ contradicts the fact that $\mathrm{o}(a) = n$. So the assumption that $a^i = a^j$ where $0 \leq i < j \leq n-1$ is false. This implies that 2 holds. It follows that $\langle a \rangle$ contains exactly n elements, that is, $\mathrm{o}(a) = |\langle a \rangle|$.

Theorem. If G is a finite group, then every element of G has finite order.



49. What is the largest order of an element in the group of permutations of 5 objects?

(A) 5 (B) 6 (C) 12 (D) 15 (E) 120



Solution 49. (B) The greatest order is given by the product of a 2-cycle and a 3-cycle acting on disjoint elements. That gives order 6.

1.5 Chapter 5: The Group of Units of $\mathbb{Z}_n$

Let $n \geq 2$. An element $a \in \mathbb{Z}_n$ is said to be a **unit** if $\exists\ b \in \mathbb{Z}_n \mid ab = 1$ (where the product is multiplication modulo n).

The set of all units in $\mathbb{Z}_n$ is denoted by

$$U_n$$

and is a group under multiplication modulo n called the **group of units of** $\mathbb{Z}_n$.

Theorem. For $n \geq 2$, $U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$

Theorem. p is a prime $\implies \exists\ a \in U_p \mid U_p = \langle a \rangle$

Theorem. If $n \geq 2$ then U_n contains an element a satisfying $U_n = \langle a \rangle$ if and only if a has one of the following forms: $2,\ 4,\ p^k$, or $2p^k$ where p is an odd prime and $k \in \mathbb{N}$.

1.6 Chapter 6: Direct Products of Groups

If $G_1, G_2, \ldots, G_n$ is a list of n groups we make the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ into a group by defining the binary operation

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

Here for each $i \in \{1, 2, \ldots, n\}$ the product $a_i \cdot b_i$ is the product of a_i and b_i in the group G_i. We call this group the **direct product** of the groups $G_1, G_2, \ldots, G_n$.

The direct product contains an identity and an inverse, and is associative (since it is composed of groups which must themselves be associative), so it is a group per below:

Theorem. If $G_1, G_2, \ldots, G_n$ is a list of n groups, the direct product $G = G_1 \times G_2 \times \cdots \times G_n$ as defined above is a group. Moreover, if for each i, e_i is the identity of G_i, then $e_1, e_2, \ldots, e_n$ is the identity of G, and if

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in G$$

then the inverse of $\boldsymbol{a}$ is given by

$$\boldsymbol{a}^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$$

where a_i^{-1} is the inverse of a_i in the group G_i.

1.7 Chapter 7: Isomorphism of Groups

Let $G = \{g_1, g_2, \dots, g_n\}$. Let $\mathrm{o}(g_i) = k_i$ for $i = 1, 2, \dots, n$. We say that the sequence $(k_1, k_2, \dots, k_m)$ is the **order sequence** of the group G. To make the sequence unique we assume the elements are ordered so that $k_1 \leq k_2 \leq \dots \leq k_n$.

Let $(G, *)$ and $(H, \bullet)$ be groups. A function $f : G \to H$ is said to be a **homomorphism** from G to H if

$$f(a * b) = f(a) \bullet f(b)$$

for all $a, b \in G$. If in addition f is one-to-one and onto, f is said to be an **isomorphism** from G to H.

We say that G and H are **isomorphic** if and only if there is an isomorphism from G to H. We write $G \cong H$ to indicate that G is isomorphic to H.

Isomorphism is an equivalence relation: If G, H, and K are groups then

1. $G \cong G$
2. If $G \cong H$ then $H \cong G$, and
3. If $G \cong H$ and $H \cong K$, then $G \cong K$.

Theorem. Let $(G, *)$ and $(H, \bullet)$ be groups and let $f : G \to H$ be a homomorphism. Let e_G denote the identity of G, and let e_H denote the identity of H. Then

1. $f(e_G) = e_H$

   Proof: Let $x_G \in G$ and let $f(x_G) = x_H \in H$. Then
   $x_H = f(x_G) = f(e_G * x_G) = f(e_G) \bullet f(x_G) = f(e_G) \bullet x_H = e_H \bullet x_H$.

2. $f(a^{-1}) = f(a)^{-1}$

   Proof: $f(a)^{-1} \bullet f(a) = e_H = f(e_G) = f(a^{-1} * a) = f(a^{-1}) \bullet f(a)$

3. $f(a^n) = f(a)^n \ \forall \ n \in \mathbb{Z}$

   Proof by induction.

Theorem. Let $(G, *)$ and $(H, \bullet)$ be groups and let $f : G \to H$ be an isomorphism. Then $\mathrm{o}(a) = \mathrm{o}(f(a)) \ \forall \ a \in G$. It follows that G and H have the same number of elements of each possible order.

Theorem. If G and H are isomorphic groups, and G is abelian, then so is H.

Proof: Let $a_G, b_G \in G$ and let $f(a_G) = a_H \in H, f(b_G) = b_H \in H$.
$a_H \bullet b_H = f(a_G) \bullet f(b_G) = f(a_G * b_G) = f(b_G * a_G) = f(b_G) \bullet f(a_G) = b_H \bullet a_H$.

Definition 1.7.1 (Cyclic groups and generators). A group G is **cyclic** if there is an element $a \in G \mid \langle a \rangle = G$. If $\langle a \rangle = G$ then we say that a is a **generator** for G.

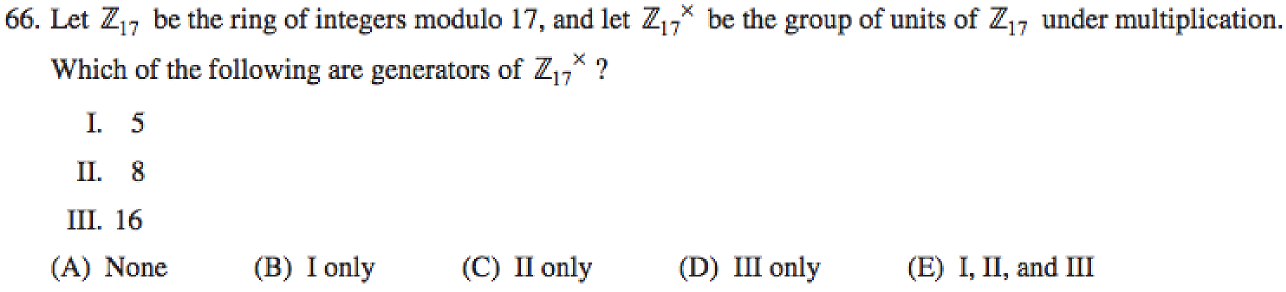
Theorem. If G and H are isomorphic groups and G is cyclic then H is cyclic.

Theorem. Let a be an element of group G.

1. $\text{o}(a) = \infty \implies \langle a \rangle \cong \mathbb{Z}$.

2. $\text{o}(a) = n \in \mathbb{N} \implies \langle a \rangle \cong \mathbb{Z}_n$

Cayley's Theorem. If G is a finite group of order n, then there is a subgroup H of S_n such that $G \cong H$.



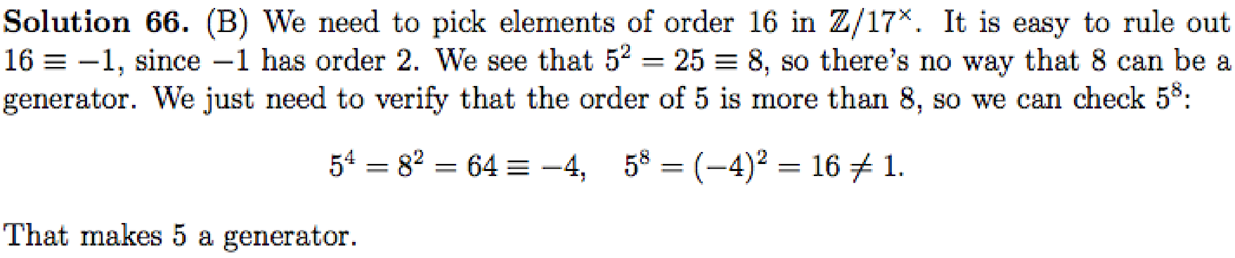
66. Let $\mathbb{Z}_{17}$ be the ring of integers modulo 17, and let $\mathbb{Z}_{17}{}^{\times}$ be the group of units of $\mathbb{Z}_{17}$ under multiplication. Which of the following are generators of $\mathbb{Z}_{17}{}^{\times}$?

I. 5

II. 8

III. 16

(A) None (B) I only (C) II only (D) III only (E) I, II, and III



Solution 66. (B) We need to pick elements of order 16 in $\mathbb{Z}/17^{\times}$. It is easy to rule out $16 \equiv -1$, since -1 has order 2. We see that $5^2 = 25 \equiv 8$, so there's no way that 8 can be a generator. We just need to verify that the order of 5 is more than 8, so we can check 5^8:

$$5^4 = 8^2 = 64 \equiv -4, \quad 5^8 = (-4)^2 = 16 \neq 1.$$

That makes 5 a generator.

1.8 Chapter 8: Cosets and Lagrange's Theorem

Let G be a group and let H be subgroup of G. For each element a of G we define

$$aH = \{ah \mid h \in H\}$$

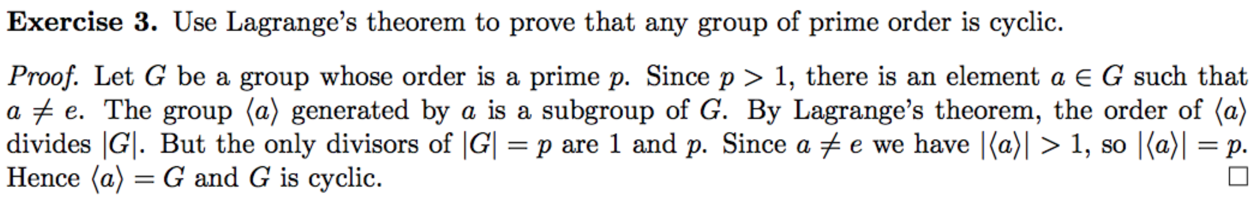
We call aH the **coset of H in G generated by** a.

Let $a, b \in G$. Then

1. $a \in aH$ (since H must contain an identity; specifically, the identity of G)
2. $|aH| = |H|$ (since ah is unique)
3. $aH \cap bH \neq \emptyset \implies aH = bH$

Lagrange's Theorem. If G is a finite group and $H \leq G$ then $|H|$ divides $|G|$.

Any group of prime order is cyclic; therefore, there is only one such group up to isomorphism.



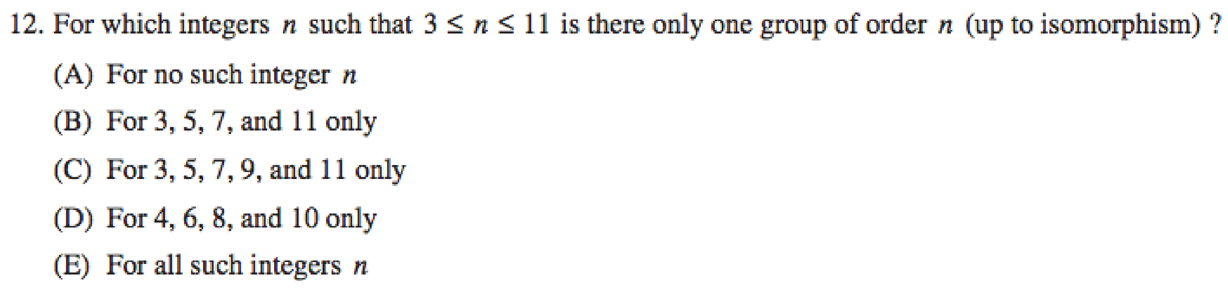
Exercise 3. Use Lagrange's theorem to prove that any group of prime order is cyclic.

Proof. Let G be a group whose order is a prime p. Since $p > 1$, there is an element $a \in G$ such that $a \neq e$. The group $\langle a \rangle$ generated by a is a subgroup of G. By Lagrange's theorem, the order of $\langle a \rangle$ divides $|G|$. But the only divisors of $|G| = p$ are 1 and p. Since $a \neq e$ we have $|\langle a \rangle| > 1$, so $|\langle a \rangle| = p$. Hence $\langle a \rangle = G$ and G is cyclic. □

We say that there are k **isomorphism classes of groups of order** n if there are k groups $G_1, G_2, \ldots, G_k$ such that

1. if $i \neq j$ then G_i and G_j are not isomorphic, and
2. Every group of order n is isomorphic to G_i for some $i \in \{1, 2, \ldots, k\}$.

This is sometimes expressed by saying that "there are k groups of order n up to isomorphism" or that "there are k non-isomorphic groups of order n."



12. For which integers n such that $3 \leq n \leq 11$ is there only one group of order n (up to isomorphism) ?

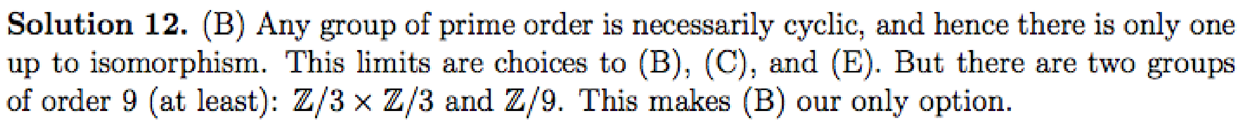
(A) For no such integer n

(B) For 3, 5, 7, and 11 only

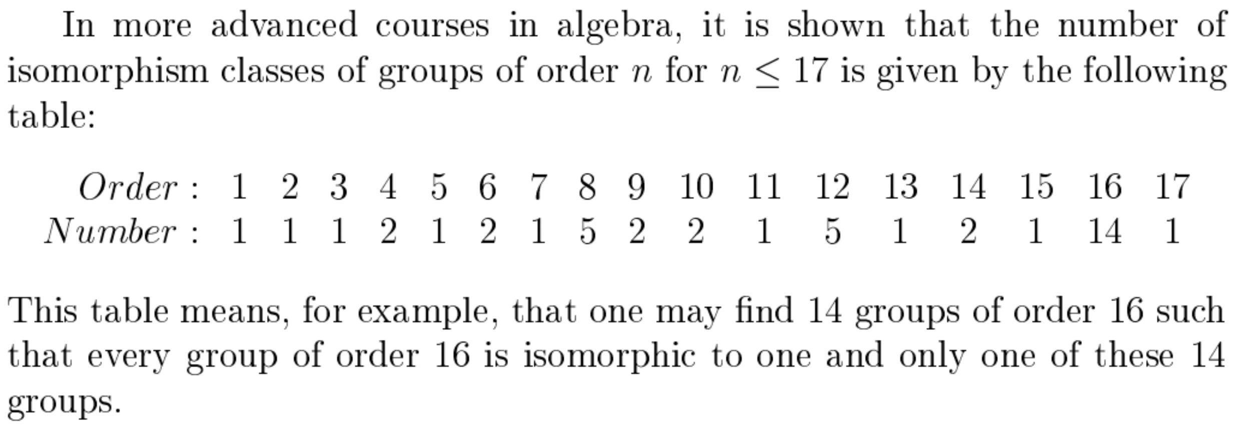
(C) For 3, 5, 7, 9, and 11 only

(D) For 4, 6, 8, and 10 only

(E) For all such integers n



Solution 12. (B) Any group of prime order is necessarily cyclic, and hence there is only one up to isomorphism. This limits are choices to (B), (C), and (E). But there are two groups of order 9 (at least): $\mathbb{Z}/3 \times \mathbb{Z}/3$ and $\mathbb{Z}/9$. This makes (B) our only option.



In more advanced courses in algebra, it is shown that the number of isomorphism classes of groups of order n for $n \leq 17$ is given by the following table:

Order :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Number :	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1

This table means, for example, that one may find 14 groups of order 16 such that every group of order 16 is isomorphic to one and only one of these 14 groups.

There is only one isomorphism class of groups of order n if n is prime. But there are some non-primes that have this property; for example, 15.

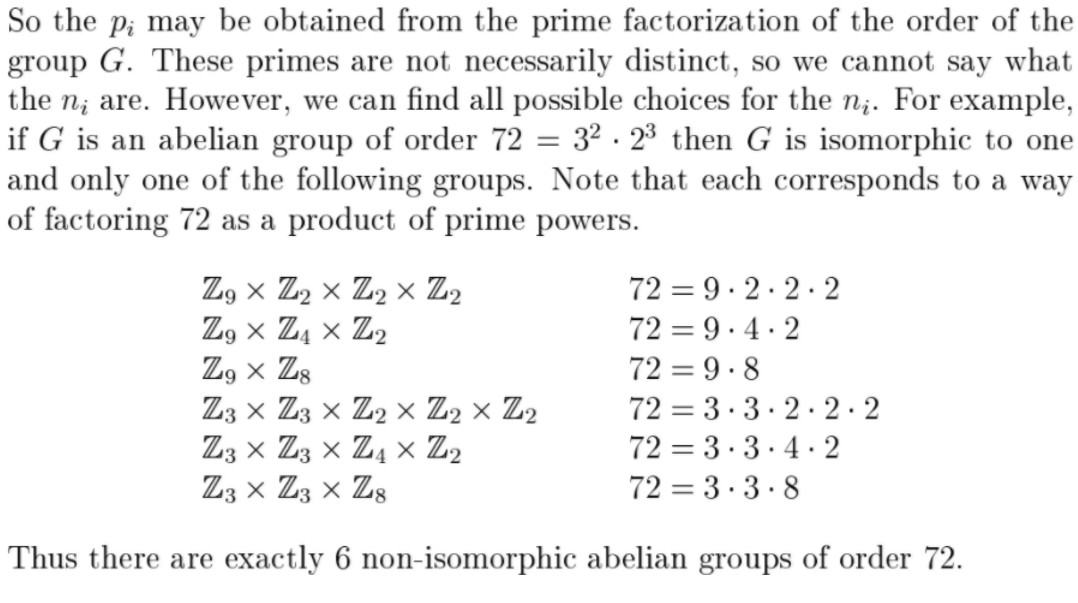
The Fundamental Theorem of Finite Abelian Groups. If G is a finite abelian group of order at least 2, then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_s^{n_s}}$$

where for each i, p_i is a prime and n_i is a positive integer. Moreover, the prime powers $p_i^{n_i}$ are unique except for the order of the factors.

If the group G in the above theorem has order n then

$$n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_2}$$



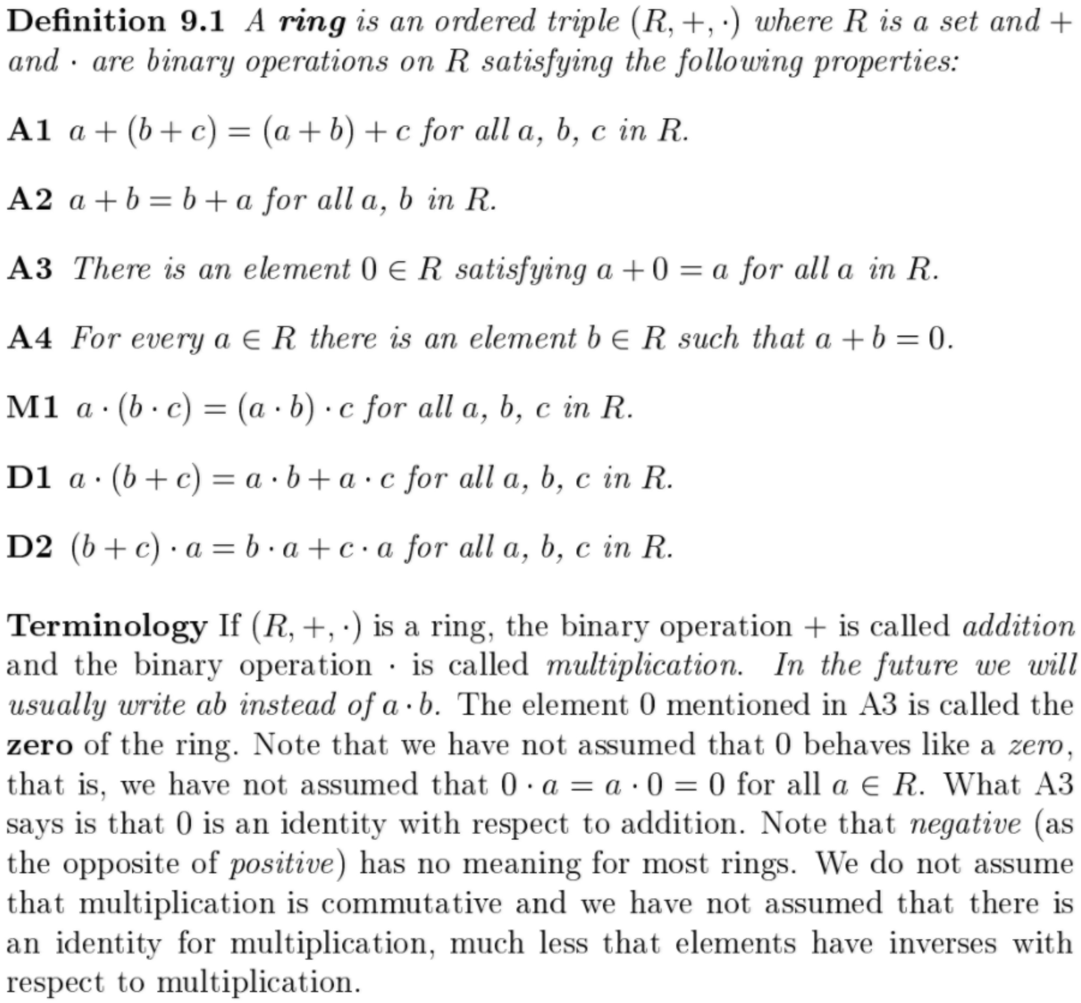
So the p_i may be obtained from the prime factorization of the order of the group G. These primes are not necessarily distinct, so we cannot say what the n_i are. However, we can find all possible choices for the n_i. For example, if G is an abelian group of order $72 = 3^2 \cdot 2^3$ then G is isomorphic to one and only one of the following groups. Note that each corresponds to a way of factoring 72 as a product of prime powers.

$\mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 9 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 9 \cdot 4 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_8$	$72 = 9 \cdot 8$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 4 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8$	$72 = 3 \cdot 3 \cdot 8$

Thus there are exactly 6 non-isomorphic abelian groups of order 72.

Corollary. For $n \geq 2$, the number of isomorphism classes of abelian groups of order n is equal to the number of ways to factor n as a product of prime powers (where the order of the factors does not count).

1.9 Chapter 9: Introduction to Ring Theory



Definition 9.1 *A* ***ring*** *is an ordered triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are binary operations on R satisfying the following properties:*

A1 $a + (b + c) = (a + b) + c$ *for all* a, b, c *in* R.

A2 $a + b = b + a$ *for all* a, b *in* R.

A3 *There is an element* $0 \in R$ *satisfying* $a + 0 = a$ *for all* a *in* R.

A4 *For every* $a \in R$ *there is an element* $b \in R$ *such that* $a + b = 0$.

M1 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* a, b, c *in* R.

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* a, b, c *in* R.

D2 $(b + c) \cdot a = b \cdot a + c \cdot a$ *for all* a, b, c *in* R.

Terminology If $(R, +, \cdot)$ is a ring, the binary operation $+$ is called *addition* and the binary operation $\cdot$ is called *multiplication. In the future we will usually write ab instead of* $a \cdot b$. The element 0 mentioned in A3 is called the **zero** of the ring. Note that we have not assumed that 0 behaves like a *zero*, that is, we have not assumed that $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$. What A3 says is that 0 is an identity with respect to addition. Note that *negative* (as the opposite of *positive*) has no meaning for most rings. We do not assume that multiplication is commutative and we have not assumed that there is an identity for multiplication, much less that elements have inverses with respect to multiplication.

Definition 1.9.1 (Ring; definition from Section 2.1 of Lang [2005], p. 98 of pdf, p. 83 of book)). A **ring** A is a set, together with two laws of composition called multiplication and addition respectively, and written as a product and as a sum respectively, satisfy the following conditions:

1. With respect to addition, A is a commutative group.
2. The multiplication is associative, and has a unit element.
3. For all $x, y, z \in A$, we have $(x+y)z = xz+yz$ and $z(x+y) = zx+zy$. (This is called **distributivity**.

As usual, we denote the unit element for addition by 0, and the unit element for multiplication by 1. We do not assume that $1 \neq 0$.

Definition 1.9.2. Let A be a ring, and let U be the set of elements of A which have both right and left inverse. Then U is a multiplicative group. Indeed, if a has a right inverse b, so that $ab = 1$, and a left inverse c, so that $ca = 1$, then $c = cab = b$, so $c = b$, and we see that c (or b) is a two-sided inverse, and that c itself has a two-sided inverse, namely a. Therefore U satisfies all the axioms of a multiplicative group, and is called the group of **units** of A. It is sometimes denoted by A^*, and is also called the group of **invertible** elements of A. A ring A such that $1 \neq 0$ and such that every non-zero element is invertible is called a **division ring**.

Definition 1.9.3. A ring A is said to be **commutative** if $xy = yx$ for all $x, y \in A$. A commutative division ring is called a **field**. We observe that by definition, a field contains at least two elements, namely 0 and 1.

Definition 1.9.4. A subset B of a ring A is called a **subring** if it is an additive subgroup, if it contains the multiplicative unit, and if $x, y \in B$ implies $xy \in B$. If that is the case, then B itself is a ring, the laws of operation in B being the same as the laws of operation in A.

For example, the **center** of a ring A is the subset A consisting of all elements of $a \in A$ such that $ax = xa$ for all $x \in A$. (One sees immediately that the center of A is a subring.)

Definition 1.9.5 (Ideal; definition from Section 2.1 of Lang [2005], p. 101 of pdf, p. 86 of book)). A **left ideal** a in a ring A is a subset of A which is a subgroup of the additive group of A, such that $Aa \subset a$ (and hence $Aa = a$ since A contains 1). To define a right ideal, we require $aA = a$, and a **two-sided ideal** is a subset which is both a left and a right ideal. A two-sided ideal is called simply an **ideal**. Note that (0) and A itself are ideals.

Definition 1.9.6 (Generator; definition from Section 2.1 of Lang [2005], p. 101 of pdf, p. 86 of book)). If A is a ring and $a \in A$, then Aa is a left ideal, called **principal**. We say that a is a generator of a (over A). Similarly, AaA is a principal two-sided ideal of we define AaA to be the set of all sums $\sum x_i a y_i$ with $x_i, y_i \in A$. More generally, let $a_1, \ldots, a_n$ be elements of A. We denote by $(a_1, \ldots, a_n)$ the set of elements of A which can be written in the form

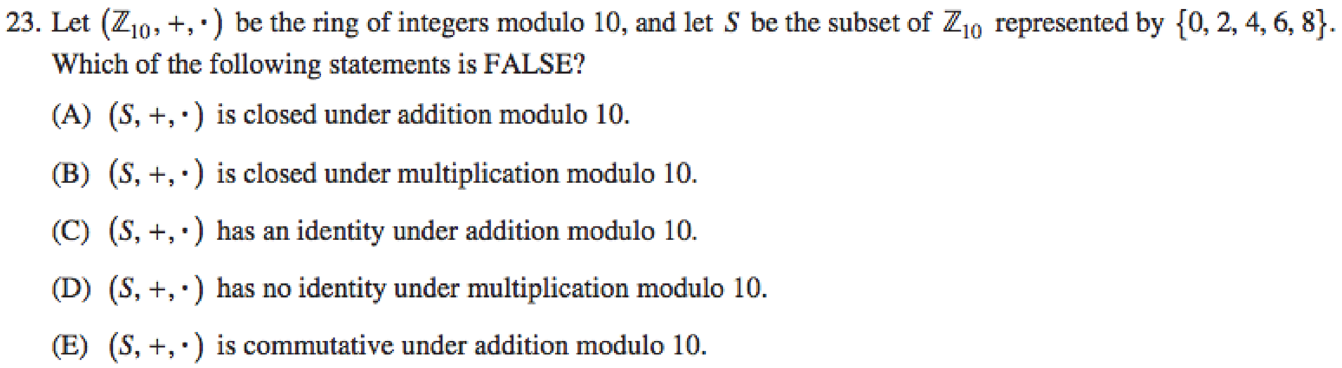
$$x_1 a_1 + \ldots + x_n a_n, \qquad x_i \in A.$$

Then this set of elements is immediately verified to be a left ideal, and $a_1, \ldots, a_n$ are called **generators** of the left ideal.

See also Definition 1.7.1.

If $\{a_i\}_{i \in I}$ is a family of ideals, then their intersection $\bigcap_{i \in I} a_i$ is also an ideal. Similarly for left ideals. It is easy to verify that if $a = (a_1, \ldots, a_n)$ then a is the intersection of all left ideals containing the elements $a_1, \ldots, a_n$.

Definition 1.9.7. A ring A is said to be **commutative** if $xy = yx$ for all $x, y \in A$. In that case, every left or right ideal is two-sided. A commutative ring such that every ideal is principal and such that $1 \neq 0$ is called a **principal** ring.



23. Let $(\mathbb{Z}_{10}, +, \cdot)$ be the ring of integers modulo 10, and let S be the subset of $\mathbb{Z}_{10}$ represented by $\{0, 2, 4, 6, 8\}$. Which of the following statements is FALSE?

(A) $(S, +, \cdot)$ is closed under addition modulo 10.

(B) $(S, +, \cdot)$ is closed under multiplication modulo 10.

(C) $(S, +, \cdot)$ has an identity under addition modulo 10.

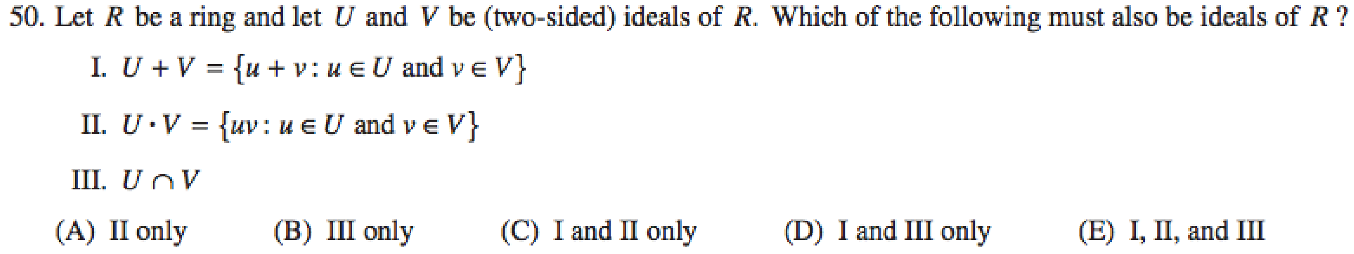
(D) $(S, +, \cdot)$ has no identity under multiplication modulo 10.

(E) $(S, +, \cdot)$ is commutative under addition modulo 10.

Solution 23. (D) Examining the choices, we see $S \subset \mathbb{Z}/10$ is a subgroup of an abelian group. Therefore it still have an additive identity and the operation is commutative. It is also closed under addition and multiplication. While S does not contain the multiplicative identity of $\mathbb{Z}/10$, it does have a multiplicative identity. $6 \in S$ is such an identity, as

$$6x = (5+1)x = 5x + x.$$

Since $x \in S$ are all even, $5x = 0$, so $6x = x$.



50. Let R be a ring and let U and V be (two-sided) ideals of R. Which of the following must also be ideals of R ?

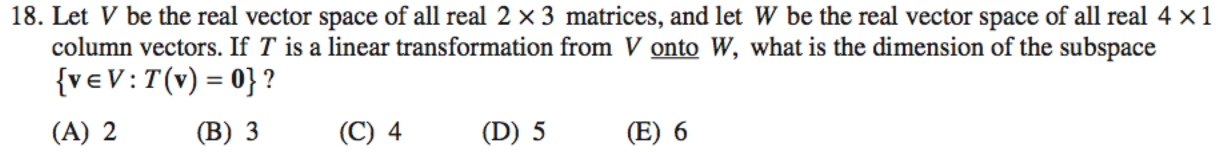
I. $U + V = \{u + v : u \in U \text{ and } v \in V\}$

II. $U \cdot V = \{uv : u \in U \text{ and } v \in V\}$

III. $U \cap V$

(A) II only (B) III only (C) I and II only (D) I and III only (E) I, II, and III

Solution 50. (D) The sum of the ideals is still an ideal: it is clearly closed under addition (using commutativity of addition), and still under left and right multiplication due to the distributive property. The intersection of ideals is still an ideal, which is not too hard to work out. The product of ideals, however, need not be closed under addition. Consider, for example, $R = \mathbb{Z}[X]$, $U = (2, X)$, and $V = (3, X)$ (the ideals generated by two elements). Then we know that $-2X \in U \cdot V$ and $3X \in U \cdot V$, and hence we should expect $3X - 2X = X \in U \cdot V$. However, there is no way to get X as the product of an element of U and an element of V.



18. Let V be the real vector space of all real 2×3 matrices, and let W be the real vector space of all real 4×1 column vectors. If T is a linear transformation from V onto W, what is the dimension of the subspace $\{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}$?

(A) 2 (B) 3 (C) 4 (D) 5 (E) 6

Solution 18. (A) We see that $\dim V = 6$ and $\dim W = 4$. Since $\dim \operatorname{im} T = \dim W = 4$, we must have $\dim \ker T = 6 - 4 = 2$.

Bibliography

S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN 9780387953854. URL https://books.google.com/books?id=Fge-BwqhqIYC.