# Topics in Algebra

David Cardozo

December 9, 2014

These are few notes and compilation of exercises of the book *Topics in Algebra.* by I. N. Herstein.

## 1 Preliminary notions

### 1.1 Set Theory

Given a set $S$ we shall use the notation throughout $a \in S$ to read "*a is an element of $S$*". The set $A$ will be said to be a *subset* of $S$ if every element in $A$ is an element of $S$, We shall write $A \subset S$. Two sets $A$ and $B$ are equal, if both $A \subset B$ and $B \subset A$. A set $D$ will be called *proper subset* of $S$ if $D \subset S$ but $D \neq S$. The null set is the set having no elements; it is a subset of every set. Given a set $S$ we shall use the notation $A\{a \in S | P(a)\}$ to read " $A$ is the set of all elements in $S$ for which the property $P$ holds.

**Definition 1.** *The **union** of the two sets $A$ and $B$, written as $A \cup B$, is the set $\{x | x \in A$ or $\in B\}$*

**Remark** when we say that x is in A or x is in B, we mean x is in at least one of A or B, and may be in both.

**Definition 2.** *The **intersection** of the two sets $A$ and $B$, written as $A \cap B$, is the set $\{x | x \in A$ and $x \in B\}$*
*Two sets are said to be* disjoint *if their intersection is empty.*

**Proposition 1.** *For any three sets, $A, B, C$ we have*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

*Proof.* We will prove first $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Observe $B \subset B \cup C$, so that $A \cap B \subset A \cap (B \cup C)$, in the same line of reasoning, $C \subset B \cap C$, so that $A \cap C \subset A \cap (B \cap C)$, and we conclude $(A \cap B) \cup (A \cap C) \subset (A \cap (B \cup C)) \cup (A \cap (B \cup C)) = A \cap (B \cup C)$. Now for the other direction, let $x \in A \cap (B \cup C)$, so that $x \in A$, and $x \in B \cup C$; suppose the former, and we have that $x \in (A \cap B)$. The second possibility, namely, $x \in C$,

implies that $x \in A \cap C$. Thus in either case, $x \in (A \cap C) \cup (A \cap B)$, whence $A \cap (B \cup C) \subset (A \cap B)(A \cap C)$. Combining the two concluding assertions, they give us the equality of both sets $\square$

Given a set $T$, we say that $T$ serves as an *index set* for the family $F = \langle A_\alpha \}$ of sets if for every $\alpha \in T$, there exist a set of $A_\alpha$ in the family $F$. By the iunion of the set $A_\alpha$, where $\alpha$ is in $T$, we mean the set $\{x | x \in A_\alpha$ for at least one $\alpha \in T\}$. We denote it by $\cup_{\alpha \in T} A_\alpha$. Similarly, we denote the intersection of the sets $A_\alpha$ by $\cap_{\alpha \in T} A_\alpha$. The sets $A_\alpha$ are mutually disjoint if for $\alpha \neq \beta$, $A_\alpha \cap A_\beta$ is the null set.

**Definition 3.** *Given the two sets $A$, $B$ then the **difference set**, $A - B$, is the set $\{x \in A | x \notin N\}$*

**Proposition 2.** *For any set $B$, the set $A$ satisfies*

$$A = (A \cap B) \cup (A - B).$$

*Proof.* Again, using the same strategy used before, we will show first $(A \cap B) \cup (A - B) \subset A$, Observe that $A \cap B \subset A$, and $A - B \subset A$ so that $(A \cap B) \cup (A - B) \subset A$ Now, for the converse, we want to see $A \subset (A \cap B)$, first observe that if we suppose that $x \in A$, then either $x \in (A - B)$ or $x \in A \cap B$, so that in either case, eventually $x \in ((A \cap B) \cup (A - B))$, so we conclude $A \subset (A \cap B)$. Finally, combining the concluding assertions we have $A = (A \cap B)$ which proves our proposition. $\square$

Observe $B \cap (A - B)$ is the null set. Observe than when $B \subset A$, we call $A - B$ the complement of $B$ in $A$.

**Definition 4.** *The binary relation $\sim$ on $A$ is said to be an* equivalence relation *on $A$ if for all $a, b, c$ in $A$*

- $a \sim a$

- $a \sim b$ *implies* $b \sim a$

- $a \sim b$ *and* $b \sim c$ *imply* $a \sim c$

*The first of these properties is called reflexivity, the second, symmetry, and the third, transitivity*

**Definition 5.** *If $A$ is a set and if $\sim$ is an equivalence relation on $A$, then the equivalence class of $a \in A$ is the set $\{x \in A | a \sim x\}$. We write it as cl(a).*

Now it comes the first big result.

**Theorem 1.** *The distinct equivalence classes of an equivalence relation on $A$ provide us with a decomposition of $A$ as a union of mutually disjoint subsets. Conversely, given a decomposition of $A$ as a union of mutually disjoint, nonempty subsets, we can define an equivalence relation on $A$ for which these subsets are the distinct equivalence classes.*

*Proof.* Let the equivalence relation on $A$ denoted by $\sim$. Observe first that $a \sim s$, so that $a \in \text{cl}(a)$, whence the union of all $\text{cl}(a)$'s is all of $A$. We will now prove that two equivalence classes are either equal or disjoint, so suppose for the contrary that two distinct classes cl(a) and cl(b) their intersection is nonempty; then there exist an element $x \in \text{cl(a)}$ and $x \in \text{cl(b)}$, that is, $x \sim a$ and $x \sim b$, and by transitivity property of the equivalence relationship, we have $a \sim b$, now let $y \in \text{cl(b)}$; thus we have $b \sim y$. But, from $a \sim b$, and $b \sim y$, we have then $a \sim y$, so that, $y \in \text{cl(a)}$, and we conclude $\text{cl(b)} \subset \text{cl(a)}$, we observe also that the argument for $y \in \text{cl(a)}$ is symmetric, so that cl(a) $\subset$ cl(b), and we have the contradiction that we took two distinct classes, but cl(a) = cl(b). We conclude then that the distinct cl(a)'s are mutually disjoint and their union is $A$. Now for the other part of the theorem.

Suppose that $A = \cup A_\alpha$, where the $a_\alpha$ are mutually disjoint, nonempty sets. We define an equivalence relation $\sim$ as: given $a \in A$ (since $a$ is in exactly one of the $A_\alpha$ ), we define $a \sim b$ if and only if $a$ and $b$ are in the same $A_\alpha$, we need to check if $\sim$ is an equivalence relation. First, observe $a \sim a$ since, again $a$ is in exactly one of the $A_\alpha$. Second, suppose $a \sim b$, that is $a, b \in A_\alpha$ for some unique $\alpha$, which is the same as $b \sim a$. Finally, suppose $a \sim b$, and $b \sim c$ so that $a, b, c \in A\alpha$ for some unique $\alpha$, and we can see that $a \sim c$.

Finally, let us observe that for any $a \in A$, cl(a) is a subset of $A$, so that cl(a) $\subset$ A, and $\bigcup_{\alpha \in A} cl(a) \subset A$; and let for $b \in A$, there exist a unique set cl(b) up to equivalence classes, so that $A \subset \bigcup_{\alpha \in A} cl(\alpha)$ $\qquad \square$

## 1.2 Problems of Set Theory

**5.** For a finite set $C$ let $|C|$ indicate the number of elements in $C$. If $A$ and $B$ are finite sets prove $|A \cup B| = |A| + |B| - |A \cap B|$

**Solution** Suppose $A$ and $B$ are finite sets, so that there exist $n, m \in \mathbb{N}$ for which $|A| = n$, and $|B| = m$. Let us remark that if $D, C$ are finite set which are disjoint, $|D \cup C|$ is $|D| + |C|$. Given this two facts, observe $A \cup B = (A - (A \cap B)) \cup B$, and $A - (A \cap B) \cap B = \emptyset$, so that $|A \cup B| = |A| - |A \cap B| + |B|$.

**6.** If $A$ is a finite set having $n$ elements, prove that $A$ has exactly $2^n$ distinct subsets.

**Solution** The proof is by induction. First, observe that if a set $A$ has one element, the subset of $A$ are $\{\emptyset, A\}$ which has $2^1$ elements, so that the assertion is true for $n = 1$, now suppose that if a set $A$ has $n$ elements, then there are exactly $2^n$ distinct subsets. Now consider the set with $n + 1$ elements given by $\{a\} \cup A$, with $a \notin A$. So that the subsets of $\{a\} \cup A$ are given by first taking the subsets of $A$, which we know have $2^n$ elements, and then taking a copy of these subset and adding the element $a$, so that there

exist:

$$2^n + 2^n = 2^n(1+1) = 2^n 2 = 2^{n+1}$$

so that for a set with $n + 1$ element, there are exactly $2^{n+1}$ subsets. Then, by the principle of mathematical induction, we have shown that If $A$ is a finite set having $n$ elements, prove that $A$ has exactly $2^n$ distinct subsets.

**10** Let $S$ be a set and let $S^*$ be the set whose elements are the various subsets of $S$. In $S^*$ we define an addition and multiplication as follows: If $A, B \in S^*$:

- $A + B = (A - B) \cup (B - A)$

- $A \cdot B = A \cap B$

Prove the following laws:

$$(A + B) + C = A + (B + C)$$

**Proof** Observe that $x \in A + B$ if and only if, $x \notin A \cap B$, so that $x \in ((A+B)+C)$ if and only if $x \notin (A+B) \cap C$, or in other words, $x \notin (A \cap B \cap C)$, which by the property that $\cap$ is associative, we have then $x \in (A+(B+C))$. So we conclude then $(A + B) + C = A + (B + C)$.

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

**Proof** Observe:

$$A \cdot B + A \cdot C = A \cap B + A \cap C$$
$$A \cap B + A \cap C = (A \cap B - A \cap C) \cup (A \cap C - A \cap B)$$
$$(A \cap B - A \cap C) \cup (A \cap C - A \cap B) = A \cap (B - C) \cup A \cap (C - B)$$
$$A \cap (B - C) \cup A \cap (C - B) = A \cap ((B - C) \cup (C - B))$$
$$A \cap (B - C) \cup A \cap (C - B) = A \cdot (B + C)$$

$$A \cdot A = A$$

**Proof** By definition. $A \cdot A = A \cap A = A$

$$A + A = \emptyset$$

**Proof** By definition. $A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

If $A + B = A + C$, then $B = C$ **Proof** Suppose is false that $B = C$, without loss of generalization, say that $x \in B$, but $x \notin C$. So two cases can happen:

i) if $x \in A + B$, observe that $x \notin A$. Note that $x \in A + B$ is equivalent to $x \in A + C$, so that $x \in C$. A contradiction.

ii) if $x \notin A + B$, we have that $x \notin A + C$, so that $x \in A \cap C$, which implies again $x \in C$. A contradiction.

We conclude then, if $A + B = A + C$, then $B = C$. (The system just described is an example of a *Boolean Algebra*.) **12.** Let $S$ be the set of all integers an let $n > 1$ be a fixed integer. Define for $a, b \in S$, $a \sim b$ if $a - b$ is a multiple of $n$.

**Proposition 3.** *$\sim$ is an equivalence relation*

   **Proof** First, observe that $a \sim a$ since $a - a = 0$ ad $0 \cdot n = 0$, second, suppose $a \sim b$, or in other words, $kn = a - b$ for some integer $k$, observe $-kn = b - a$, and we have then $b \sim a$. Finally, suppose $a \sim b$ and $b \sim c$, more explicitly, $kn = a - b$ and $gn = b - c$ for some integers $k$ and $g$, take note that $kn + gn = (k + g)n = a - c$, so that $a \sim c$.

**Proposition 4.** *There are exactly n distinct classes*

   **Proof** Let cl(0), ...,cl(n-1), be the $n$ different equivalence classes, defined by $\sim$ as above, observe that for an integer $x \geq n$, cl(x) is: $\{m \in \mathbb{Z} | x \sim m\}$, note that if $x \geq n$ is equivalent to say that, there exist integers $E = 0, 1, ...$ and $K = 0, ..., n - 1$ such that $x = En + K$. Since $x \sim m$, $En + K \sim m$, which by definition is: there exist an integer $R$ for which $Rn = (En+K)-m$, or $(R - E)n = K - m$, so that $K \sim m$, and since $K = 0, ..., n - 1$, w have shown for $x \geq n$, $x$ is in the any of the equivalence classes of cl(0), cl(1), ... cl$(n - 1)$.

## 1.3   Mappings

We introduce the concept of a mapping of one set into another. Informally, a mapping from one set, $S$, into another, $T$, is a ruler that associates with each element in $S$ a *unique* element $t$ in $T$.

**Definition 6.** *If $S$ and $T$ are nonempty sets, then a **mapping** from $S$ to $T$ is a subset, M, of $S \times T$ such that for every $s \in S$ there is a unique $t \in T$ such that the ordered pair $(s, t)$ is in M.*

   Alternatively and for pedagogical reasons, we think of a mapping as a rule that associates any element $s \in S$ some element $t \in T$. We shall say that $t$ is the image of $s$ under the mapping. **Notation Remarks** Let $\sigma$ be a mapping from $S$ to $T$; we denote this by writing $\sigma : S \to T$ or $S \xrightarrow{\sigma} T$, strangely enough, if $t$ is the image of $s$ under $\sigma$ we shall represent this fact by $t = s\sigma$. Algebraists often write mappings on the right.
   Given a mapping $\tau : S \to T$ we define for $t \in T$, the inverse image of $t$ with respect to $\tau$ to be the set $\{s \in S | t = s\tau\}$

**Definition 7.** *The mapping $\tau$ of $S$ into $T$ is said to be **onto** $T$ if given $t \in T$ there exits an element $s \in S$ such that $t = s\tau$*

Observe that we call the subset $S\tau = \{x \in T | x = s\tau$ for some $s \in S\}$ the **image** of $S$ under $\tau$, then $\tau$ is onto if the image of $S$ under $\tau$ is all of $T$.

**Definition 8.** *The mapping $\tau$ of $S$ into $T$ is said to be a **one-to-one mapping** if whenever $s_1 \neq s_2$, then $s_1\tau = s_2\tau$.*

**Remark** Observe that the mapping $\tau$ is one-to-one if for any $t \in T$ the inverse image of $t$ is either empty or is a set consisting of one element.

**Definition 9.** *The two mappings $\sigma$ and $\tau$ of $S$ into $T$ are said to be **equal** if $s\sigma = s\tau$ for every $s \in S$.*

**Definition 10.** *If $\sigma : S \to T$ and $\tau : T \to U$ then the **composition** of $\sigma$ and $\tau$ (also called their product) is the mapping $\sigma \circ \tau : S \to U$ defined by means of $s(\sigma \circ \tau) = (s\sigma)\tau$ for every $s \in S$*

Remark that it is read from left to right; that is, $\sigma \circ \tau$: first perform $\sigma$ and then do $\tau$.

For mappings of sets, provided the products make sense, the following holds:

**Proposition 5** (Associative Law). *If $\sigma : S \to T$, $\tau : T \to U$, and $\mu : U \to V$, then $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.*

*Proof.* So, lt us see that the composition makes sense to be equal, observe that $\sigma \circ \tau$ takes an element of $s \in S$ to $t \in T$ so that $(\sigma \circ \tau) \circ \mu$ make sense and takes $S$ into $V$. Similarly $\tau \circ \mu$ takes $T$ into $V$ and $\sigma \circ (\tau \circ \mu)$ takes also $S$ into $V$, so we are rest to check if both functions are equal. So, we start with an element $s$ in $S$ and we want to see that $s((\sigma \circ \tau) \circ \mu) = s(\sigma \circ (\tau \circ \mu))$.

By definition of the composition of maps $s((\sigma \circ \tau) = (s(\sigma \circ \tau))\mu = ((s\sigma)\tau)\mu$, whereas $s(\sigma \circ (\tau \circ \mu)) = (s\sigma)(\tau \circ \mu) = (((s\sigma)\tau)\mu$. Thus, we conclude $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$. $\square$

**Proposition 6.** *Let $\sigma : S \to T$ and $\tau : T \to U$; then*

- *$\sigma \circ \tau$ is **onto** if each of $\sigma$ and $\tau$ is onto.*

- *$\sigma \circ \tau$ is **one-to-one** if each of $\sigma$ and $\tau$ is one-to-one.*

*Proof.*     • Suppose $\sigma$, and $\tau$ both are onto functions, that is, $S\sigma = T$, and $T\tau = U$, so we establish that $(S\sigma)\tau = U$, or equivalently, $S(\sigma \circ \tau) = U$, and we have then $\sigma \circ \tau$ is onto.

- Suppose that $s_1, s_2$ ar elements of $S$, and that $s_1 \neq s_2$. By the one-to-one property of $\sigma$, $s_1\sigma \neq s_2\sigma$. Since $\tau$ is also one-to-one, and $s_1\sigma, s_2\sigma$ are distinct elements of $T$, $(s_1\sigma)\tau \neq (s_2\sigma)\tau$, therefore $s_1(\sigma \circ \tau) = (s_1\sigma)\tau \neq (s_2\sigma)\tau = s_2(\sigma \circ \tau)$, and we establish the lemma. $\square$

Now, let us suppose that $\sigma$ is a one-to-one mapping of $S$ *onto* $T$; we call $\sigma$ a **one-to-one correspondence** between $S$ and $T$. so observe that for any $t \in T$, there exist $s \in S$ such that $t = s\sigma$; and by the property of one-to-one, this $s$ is unique. We define the mapping $\sigma^{-1} : T \to S$ by $s = t\sigma^{-1}$ if and only if $t = s\sigma$. This map, is called the **inverse** of $\sigma$. Observe $\sigma \circ \sigma^{-1}$ maps $S$ to $S$, note that $s(\sigma \circ \sigma^{-1}) = (s\sigma)\sigma^{-1} = t\sigma^{-1} = s$. so that $\sigma \circ \sigma^{-1}$ is the identity operator on $S$, similarly $\sigma^{-1} \circ \sigma$ is again the identity mapping of $T$. Conversely, if $\sigma : S \to T$ is such that there exist $\mu : T \to S$ with the property that $\sigma \circ \mu$ and $\mu \circ \sigma$ are the identity mappings on $S$ and $T$ respectively, we claim that $\sigma$ is a one-to-one correspondence between $S$ and $T$. First, observe that $\sigma$ is onto, this given by the fact that, let $t \in T$, so that $= t = tI_t = t(\mu \circ \sigma) = (t\mu)\sigma$, and we take note that $t\mu \in S$ so that we shown that there exist $s \in S$ such that $t = s\sigma$ for any $t$ and we conclude, $\sigma$ is onto. Second, suppose $s_1\sigma = s_2\sigma$; take note that $s_1 = s_1 I_s = s_1(\sigma \circ \mu) = (s_1\sigma)\mu = (s_2\sigma)\mu = s_2(\sigma \circ \mu) = s_2 I_s = s_2$ The preceding discussion proves then:

**Proposition 7.** *The mapping $\sigma : S \to T$ is a **one-to-one correspondence** between $S$ and $T$ if and only if there exist a mapping $\mu : T \to S$ such that $\sigma \circ \mu$ and $\mu \circ \sigma$ are the identity mappings on $S$ and $T$ respectively.*

**Definition 11.** *If $S$ is a nonempty set then $A(S)$ is the **set of all one-to-one mappings** of $S$ onto itself.*

$A(S)$ plays a universal type of role in groups. We state the following theorem as the recollection of th previous lemma and results:

**Theorem 2.** *If $\sigma, \tau, \mu$ are elements of $A(S)$, then:*

- *$\sigma \circ \tau$ is in $A(S)$.*

- *$(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.*

- *There exist an element $i$ (the identity map) in $A(S)$ such that $\sigma \circ i = i \circ \sigma = \sigma$.*

- *There exist an element $\sigma^{-1} \in A(S)$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = i$.*

*Proof.* • Given by Proposition 6

- Given by Proposition 5 *em Given by Proposition 7*

- *Given by Proposition 7*

$\square$

**Proposition 8.** *If $S$ has more than two elements we can find two elements $\sigma, \tau$ in $A(S)$ such that $\sigma \circ \tau \neq \tau \circ \sigma$.*

*Proof.* Consider $U$ subset of $S$, with $S$ having more than three elements, let us also suppose that the cardinality of $U$ is 3. Define $T$ as the complement of U with respect to S, that is, $T = S - U$. Now consider $F$ the set of all one-to-one mappings and onto functions on $S$ that fix $T$, i.e if $f \in F$ then $f(t) = t$ for all $t \in T$. Observe then that all functions on $F$ are uniquely determined by the values of $f|_U : S \rightarrow S$. Let us rename the elements of $U$ with $x_1, x_2, x_3$, define the mapping $\sigma \in F$ by $\sigma : S \rightarrow S$ by $x_1\sigma = x_2$, $x_2\sigma = x_3$, $x_3\sigma = x_1$, and the rest is determined already since $\sigma \in F$. Define the mapping $\tau : S \rightarrow S$, and $\tau \in F$ by $x_2\tau = x_3$, $x_3\tau = x_2$ and $x_1\tau = x_1$. Take note, $x_1(\sigma \circ \tau) = x_3$ but that $x_1(\tau \circ \sigma) = x_2 \neq x_3$. Thus $\sigma \circ \tau \neq \tau \circ \sigma$ $\quad\square$

## 1.4   Problems of Mappings

**2** If $S$ and $T$ are nonempty sets, prove that there exists a correspondence between $S \times T$ and $T \times S$

**Proof** Let us define the following mappings:

$$\sigma : (S \times T) \rightarrow (T \times S)$$
$$(s, t) \longmapsto (t, s)$$

and

$$\mu : (T \times S) \rightarrow (S \times T)$$
$$(t, s) \longmapsto (s, t)$$

Observe first that, $\sigma \circ \mu = i_{(S \times T)}$, since $(s, t)(\sigma \circ \mu) = ((s, t)\sigma)\mu = (t, s)\mu = (s, t) = (s, t)i_{(S \times T)}$, similarly for $\mu \circ \sigma = i_{(T \times S)}$