Topics in Algebra

David Cardozo

December 8, 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 $\{x | x \in A \text{ } or \text{ } \in B\}$*

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 $\{x | x \in A \text{ } and \text{ } x \in B\}$*
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_α in the family F. By the iunion of the set A_α, where α 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_α by $\cap_{\alpha \in T} A_\alpha$. The sets A_α 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 $x \in$ cl(a) and $x \in$ 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 $y \in$ 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, $y \in$ cl(a), and we conclude cl(b) $\subset$ cl(a), we observe also that the argument for $y \in$ 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_α 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_α), we define $a \sim b$ if and only if a and b are in the same A_α, 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_α. Second, suppose $a \sim b$, that is $a, b \in A_\alpha$ for some unique α, 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 α, 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 $A \subset \bigcup_{\alpha \in A} cl(\alpha)$ □

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:

$$\begin{aligned}
A \cdot B + A \cdot C &= A \cap B + A \cap C \\
A \cap B + A \cap C &= (A \cap B - A \cap C) \cup (A \cap C - A \cap B) \\
(A \cap B - A \cap C) \cup (A \cap C - A \cap B) &= A \cap (B - C) \cup A \cap (C - B) \\
A \cap (B - C) \cup A \cap (C - B) &= A \cap ((B - C) \cup (C - B)) \\
A \cap (B - C) \cup A \cap (C - B) &= A \cdot (B + C)
\end{aligned}$$

$$A \cdot A = A$$

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), $\ldots$ 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 σ be a mapping from S to T; we denote this by writing $\sigma : S \to T$ or $S \xrightarrow{\sigma} T$