Journal of Mathematics Research
http://ccsenet.org/jmr
Vol. 2, No. 1
February 2010

The Algebraic Construction of Commutative Group

Yanyan Shan
Department of Mathematics, School of Science, Inner Mongolia University of Technology
Hohhot 010052, China
E-mail: bigeye_mm@163.com

Abstract

The construction of the integers introduced by Dedekind is an algebraic one. Subtraction can not be done without restriction in natural numbers N. If we consider the definition of multiplication of integral domain Z, N with respect to subtraction is needed. It is necessary to give the definition of subtraction in N. Instead of starting from natural numbers, one could begin with any commutative semi-group and construct from it as the construction of the integers to obtain a commutative group. If the cancellation law does not hold in the commutative semi-group, some modifications are required. The mapping from the commutative semi-group to the commutative group is not injective and compatible with addition. In the relation between real numbers and decimals, N also plays an important role.

Keywords: Well-defined, Equivalence relation, Commutative group, Cancellation law, Injective, Compatible, Archimedean property

1. The construction and application of subtraction of natural numbers

1.1 Subtraction of natural numbers N

Definition $\quad a = b - c \Longleftrightarrow a + c = b. \quad \forall a, b, c \in N.$

If $a = b - c$ and also $a' = b - c$, then $a + c = b$ and $a' + c = b$. And we have $a = a'$ from $a + c = a' + c$, according to the cancellation law of N. Hence, subtraction of N is well-defined.

Besides, commutative law, association law and distribution law with respect to subtraction of N are satisfied.

Commutative law: $a = b - c \Leftrightarrow a + c = b. \quad a' = c - b \Leftrightarrow a' + b = c$. We have $a' + (a + c) = c \Rightarrow a' + a = 0$.
Namely, $(c - b) + (b - c) = 0, (c - b) = -(b - c)$.

Association law: $a = b-c \Leftrightarrow a+c = b. \Rightarrow d+b = d+(a+c) \Rightarrow d+b = (d+a)+c \Rightarrow d+a = (d+b)-c \Rightarrow d+(b-c) = (d+b)-c$.

Distribution law: $a = b - c \Leftrightarrow a + c = b. \Rightarrow d(a + c) = db \Rightarrow da + dc = db \Rightarrow da = db - dc \Rightarrow d(b - c) = db - dc$.

Similarly, $a = b - c \Leftrightarrow a + c = b. \Rightarrow (a + c)d = bd \Rightarrow ad + cd = bd \Rightarrow ad = bd - cd \Rightarrow (b - c)d = bd - cd$.

According to the operations of N, we can prove multiplication in Z is well-defined and integers form an integral domain with respect to addition and multiplication.

1.2 The integral domain Z

We should like $(a - b) \cdot (c - d)$ to be equal to $(ac + bd) - (ad + bc)$ and accordingly this leads to the following definition:
$[a, b] \cdot [c, d] = [ac + bd, ad + bc]$ for $a, b, c, d \in N$

This definition is independent of the particular choice of the representative pairs.

Next we will prove $[a, b] \cdot [c, d] = [ac + bd, ad + bc]$ for $a, b, c, d \in N$ is well-defined.

If $[a, b] = [a', b'], [c, d] = [c', d']$, then $[a, b] = [a', b'] \Rightarrow a + b' = a' + b \Rightarrow a = a' + b - b'$.
$[c, d] = [c', d'] \Rightarrow c+d' = c'+d \Rightarrow c = c'+d-d'$. $[a, b]\cdot[c, d] = [ac+bd, ad+bc], [a', b']\cdot[c', d'] = [a'c'+b'd', a'd'+b'c']$.

We have $ac + bd + a'd' + b'c' = (a' + b - b')(c' + d - d') + bd + a'd' + b'c' = a'c' + a'd - a'd' + bc' + bd - bd' - b'c' - b'd + b'd' + bd + a'd' + b'c' = a'c' + a'd + bc' + 2bd - bd' - b'd + b'd'$

$a'c' + b'd' + ad + bc = a'c' + b'd' + (a' + b - b')d + b(c' + d - d') = a'c' + b'd' + a'd + bd - b'd + bc' + bd - bd' = a'c' + b'd' + a'd + 2bd - b'd + bc' - bd'$

then $(ac + bd) + (a'd' + b'c') = (a'c' + b'd') + (ad + bc)$.Namely, $[ac + bd, ad + bc] = [a'c' + b'd', a'd' + b'c']$.
That is to say, $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$.

Theorem The integers form an integral domain with respect to addition and multiplication. (that is, a commutative ring without zero divisors and with identity element).

We have proved Z is a commutative group with respect to addition. Next we will consider Z with respect to multiplication.

Commutative law: $[a, b] \cdot [c, d] = [ac + bd, ad + bc] = [ca + db, cb + da] = [c, d] \cdot [a, b]. \quad \forall [a, b], [c, d] \in Z$

Associative law:
$([a, b] \cdot [c, d]) \cdot [e, f] = [ac + bd, ad + bc] \cdot [e, f] = [(ace + bde) + (adf + bcf), (acf + bdf) + (ade + bce)] = [(ace + adf) + (bcf + bde), (acf + ade) + (bce + bdf)] = [a, b] \cdot [ce + df, cf + de] = [a, b] \cdot ([c, d] \cdot [e, f]) \quad \forall [a, b], [c, d], [e, f] \in Z$

Distribution law:
$[a, b] \cdot ([c, d] + [e, f]) = [a, b] \cdot [c + e, d + f] = [a(c + e) + b(d + f), a(d + f) + b(c + e)] = [ac + ae + bd + bf, ad + af + bc + be] = [(ac + bd) + (ae + bf), (ad + bc) + (af + be)] = [ac + bd, ad + bc] + [ae + bf, af + be] = [a, b] \cdot [c, d] + [a, b] \cdot [e, f]$

Here we know Z is a commutative ring.

Besides, $[1, 0] \cdot [a, b] = [a, b] \cdot [1, 0] = [a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1] = [a, b]. \quad \forall [a, b] \in Z.$

Next we assume there exist zero-divisors in Z, that is to say, $\exists [a, b] \neq [0, 0]$, and $\exists [c, d] \neq [0, 0]$.

$[a, b] \cdot [c, d] = [ac + bd, ad + bc] = [0, 0], \quad \forall [a, b], [c, d] \in Z.$
Then $ac + bd + 0 = 0 + ad + bc, ac + bd = ad + bc, ac - ad = bc - bd, a(c - d) = b(c - d), a(c - d) - b(c - d) = 0, (c - d)(a - b) = 0. \Rightarrow c = d$ or $a = b$.

Which is contradictory to the assumption $[a, b] \neq [0, 0], [c, d] \neq [0, 0]$.

Hence, the assumption is not satisfied, there is no zero-divisors in Z.

Here we should also prove "If $m, n \in N$ and $mn = 0$ then $m = 0$ or $n = 0$. $\Leftrightarrow$ If $m \neq 0$ and $n \neq 0$, then $mn \neq 0$. " by induction.

Firstly, we should prove "If $m \neq 0$ and $n \neq 0$, then $m + n \neq 0$. " by induction.

If $m = 1, 1 + n = S(n) \neq 0$.
If $m = k, k + n \neq 0$.
When $m = k + 1, (k + 1) + n = (k + n) + 1 = S(k + n) \neq 0$.

So, "If $m \neq 0$ and $n \neq 0$, then $m + n \neq 0$. " is proved.

If $m = 1, 1 \cdot n = n \neq 0$.
If $m = k, k \cdot n \neq 0$.
When $m = k + 1, (k + 1) \cdot n = k \cdot n + n \neq 0$.

Hence, " ""If $m, n \in N$ and $mn = 0$ then $m = 0$ or $n = 0$." is proved.

2.The construction of commutative group

We begin with any commutative semi-group H and construct from it as the construction of the integers to obtain a commutative group G. If the cancellation law does not hold in H, we define$(a, b) \sim (c, d)$ if and only if there is an e such that $a + d + e = b + c + e$. However, in this case $\iota : H \longrightarrow G$ is not injective.

2.1 The relation defined on $H \times H$

We consider the relation $\sim$, defined on $H \times H$, by $(a, b) \sim (c, d)$ if and only if there is an e such that $a + d + e = b + c + e$.We then establish that this is an equivalence relation.

It may be proved as follows:

Reflexivity: There is an e such that $a + b + e = b + a + e \Rightarrow (a, b) \sim (a, b). \quad \forall (a, b) \in H$

Symmetry: If $(a, b) \sim (c, d)$, then there is an e such that $a + d + e = b + c + e$.
Hence, $c + b + e = d + a + e \Rightarrow (c, d) \sim (a, b). \quad \forall (a, b), (c, d) \in H$

Transitivity: If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ then by definition, there are g and h such that $a + d + g = b + c + g$ and $c + f + h = d + e + h$. $\quad \forall (a, b), (c, d), (e, f) \in H$

By addition we obtain $a + d + g + c + f + h = b + c + g + d + e + h$. And by letting $i = g + h + c + d$, we obtain there is an i such that $a + f + i = b + e + i$, that is $(a, b) \sim (e, f)$. (We have also made use of the commutativity and associativity of addition.)

G may now be defined as equivalence classes of the relation $\sim$. The class represented by (a, b) is denoted by $[a, b]$. G is a set of equivalence classes.

2.2 Addition on $H \times H$

We can define on $H \times H$ a component-wise addition, $(a, b) + (c, d) := (a + c, b + d)$.

The commutative and associative laws hold, and the zero element is $(0, 0)$.

Commutative law: $(a, b) + (c, d) := (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$.

Associative law:
$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f) = (a + (c + e), b + (d + f)) = (a, b) + (c + e, d + f)) = (a, b) + ((c, d) + (e, f))$.

Zero element: $(0, 0) + (a, b) = (a, b) + (0, 0) = (a, b)$.

This addition is compatible with the relation $\sim$, that is to say, if $(a', b') \sim (a, b)$ and $(c', d') \sim (c, d)$ then $(a' + c', b' + d') \sim (a + c, b + d)$.

$(a', b') \sim (a, b), (c', d') \sim (c, d) \Rightarrow a' + b = b' + a, c' + d = d' + c \Rightarrow (a' + c') + (b + d) = (b' + d') + (a + c)$
$\Rightarrow (a' + c', b' + d') \sim (a + c, b + d)$.

It is therefore meaningful to introduce in G, an addition $G \times G \longrightarrow G, [a, b] + [c, d] := [a + c, b + d]$,which is likewise commutative and associative and which has $[0, 0]$ as zero element.

Commutative law: $[a, b] + [c, d] := [a + c, b + d] = [c + a, d + b] = [c, d] + [a, b]$.

Associative law:
$([a, b] + [c, d]) + [e, f] = [a + c, b + d] + [e, f] = [a + (c + e), b + (d + f)] = [a + (c + e), b + (d + f)] = [a, b] + ([c, d] + [e, f])$.

Zero element: $[0, 0] + [a, b] = [a, b] + [0, 0] = [a, b]$.

Next we will prove the addition in G is well-defined.

If $[a, b] = [a', b']$ and $[c, d] = [c', d']$, we should check $[a, b] + [c, d] = [a', b'] + [c', d']$.

Solution: $[a, b] = [a', b'] \Rightarrow$ there is an e such that $a + b' + e = a' + b + e$.

$[c, d] = [c', d'] \Rightarrow$there is an f such that $c + d' + f = c' + d + f$.

Then there is a $g = e + f$ such that $a + c + b' + d' + g = a' + c' + b + d + g$.
And $[a, b] + [c, d] = [a + c, b + d], [a', b'] + [c', d'] = [a' + c', b' + d']$. Hence$[a, b] + [c, d] = [a', b'] + [c', d']$.

By passing to equivalence classes we have gained more. Each $[a, b]$ has an inverse, namely $[b, a]$. We have established the following.

2.3 Commutative group G

Theorem G forms a commutative group with respect to addition.

The element inverse to $\alpha \in G$ is uniquely determined, and is denoted by $-\alpha$. Subtraction in G is defined by $\alpha - \beta := \alpha + (-\beta)$.

Proof: (1)$\forall [a, b], [c, d] \in G, [a, b] + [c, d] \in G$.

(2)$\forall [a, b], [c, d] \in G, [a, b] + [c, d] = [c, d] + [a, b]$.

(3)$\forall [a, b], [c, d], [e, f] \in G, ([a, b] + [c, d]) + [e, f] = [a, b] + ([c, d] + [e, f])$.

(4)$\forall [a, b] \in G, \exists [0, 0] \in G, [0, 0] + [a, b] = [a, b] + [0, 0] = [a, b]$. And $[0, 0] = [0, 0] + [0, 0]' = [0, 0]'$, the zero element is unique.

(5)$\forall [a, b] \in G, \exists [b, a] = -[a, b] \in G, [a, b] + (-[a, b]) = (-[a, b]) + [a, b] = [0, 0]$.

In fact, $[a, b] + [b, a] = [a + b, b + a]$ and $a + b + 0 = b + a + 0$. Then there exists an $e = 0$ such that $a + b + 0 + 0 = b + a + 0 + 0$. Hence $[a, b] + [b, a] = [0, 0]$.

Besides, $[a, b] + [c, d] = [0, 0] \Rightarrow [b, a] + ([a, b] + [c, d]) = [b, a] + [0, 0] \Rightarrow [b, a] + [a, b] + [c, d] = [b, a] \Rightarrow [c, d] = [b, a]$. The inverse of $[a, b]$ is also unique.

2.4 The mapping from H to G

The mapping $\iota : H \longrightarrow G, a \longrightarrow [a, 0]$ is not injective and compatible with addition.

If the cancellation law does not hold in H, that is to say, there are $a, b, c \in H$ such that $a + c = b + c$ and $a \neq b$.
Then $[a, 0] = [b, 0]$ and $a \neq b$, namely, $\iota(a) = \iota(b)$ and $a \neq b$. Hence, ι is not injective.
Besides, ι is compatible with addition, because of $\iota(a) = [a, 0], \iota(b) = [b, 0], \iota(a + b) = [a + b, 0] = [a, 0] + [b, 0] \Rightarrow \iota(a + b) = \iota(a) + \iota(b)$.

3. The relation between real numbers and decimals

The relation between real numbers and decimals has been generally pointed out in *The principle of mathematical analysis*. Since the importance of application of Archimedean property of R and the relationship between real numbers and decimals, the method of how to choose $n_1, ..., n_{k-1}$ of "Having chosen $n_0, n_1, ..., n_{k-1}$, let n_k be the largest integer such that $n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k} \leq x$"as been given, and the proof of "Let E be the set of these numbers $n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k}(k = 0, 1, 2, \cdots)(5)$ .Then $x = supE$."as been indicated, which Rudin have not mentioned totally. In the proof of the two questions natural numbers also play an important role.

3.1 The existence of n_0.

Theorem 1.20 (a) If $x \in R, y \in R$ and $x > 0$ then there is a positive integer n such that $nx > y$.
Part (a) is usually referred to as the Archimedean property of R.

Let $x > 0$ be real.

According to the Archimedean property of $R, x \in R, 1 \in R, 1 > 0$, then there is a positive integer n such that $n \cdot 1 > x$.

Hence $x \in [0, 1) \cup [1, 2) \cup \cdots \cup [n-1, n)$, then there is $n_0 \in Z^{+} \cup 0$ such that $x \in [n_0, n_0 + 1)$.
And n_0 is the largest integer such that $n_0 \leq x < n_0 + 1$.

3.2 The method of choosing $n_1, \cdots, n_{k-1}$.

$0 \leq x - n_0 < 1, 0 \leq 10(x - n_0) < 10, 10(x - n_0) \in [0, 1) \cup [1, 2) \cup \cdots \cup [9, 10)$.

Then there exists $n_1 \in Z$ and $0 \leq n_1 < 10$ such that $10(x - n_0) \in [n_1, n_1 + 1)$, and n_1 is the largest integer such that
$n_1 \leq 10\,(x - n_0) < n_1 + 1, \frac{n_1}{10} \leq x - n_0 < \frac{n_1}{10} + \frac{1}{10}, 0 \leq x - n_0 - \frac{n_1}{10} < \frac{1}{10}, 0 \leq 100(x - n_0 - \frac{n_1}{10}) < 10$.

In the similar way, there is a largest integer n_2 such that
$0 \leq n_2 \leq 100(x - n_0 - \frac{n_1}{10}) < n_2 + 1, \frac{n_2}{100} \leq x - n_0 - \frac{n_1}{10} < \frac{n_2}{100} + \frac{1}{100}, 0 \leq x - n_0 - \frac{n_1}{10} - \frac{n_2}{100} < \frac{1}{100}, 0 \leq 1000(x - n_0 - \frac{n_1}{10} - \frac{n_2}{100}) < 10$.

There is a largest integer n_3 such that $0 \leq n_3 \leq 1000(x - n_0 - \frac{n_1}{10} - \frac{n_2}{100}) < n_3 + 1$.

Do the same actions till we obtain n_{k-1} such that $0 \leq n_{k-1} \leq 10^{k-1}(x - n_0 - \frac{n_1}{10} - \cdots - \frac{n_{k-2}}{10^{k-2}}) < n_{k-1} + 1$.

3.3 The proof of $x = supE$.

Let n_k be the largest integer such that $0 \leq n_k \leq 10^k(x - n_0 - \frac{n_1}{10} - \cdots - \frac{n_{k-1}}{10^{k-1}}) < n_k + 1$.
$x - n_0 - \frac{n_1}{10} - \cdots - \frac{n_{k-1}}{10^{k-1}} \geq \frac{n_k}{10^k}, x \geq n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k}$.
Let E be the set of these numbers $n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k}(k = 0, 1, 2, \cdots)(5)$

$E = \left\{n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k} | k = 0, 1, 2, \cdots\right\}$

We have known x is an upper bound of E . Next we will prove x is the smallest upper bound of E.

$\forall y < x, x - y > 0 \Rightarrow \frac{1}{x-y} > 0$.
According to Archimedean property $\frac{1}{x-y} \in R, 1 \in R, 1 > 0$, then there is a positive integer n such that $1 \cdot n > \frac{1}{x-y}$.
We let $a_k = n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k}, k = 0, 1, 2, \cdots$.
$n(x - y) > 1, nx - ny > 1, nx - 1 > ny \Rightarrow y < x - \frac{1}{n}(*)$

We have known $10^k(x - (n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}})) < n_{k+1} \Rightarrow x - (n_0 + \frac{n_1}{10} + \cdots + \frac{n_{k-1}}{10^{k-1}} + \frac{n_k}{10^k}) < +\frac{1}{10^k} \Rightarrow x - a_k < \frac{1}{10^k}(**)$

Next we will proof $10^k \geq n$ by the principle of complete induction to complete the proof. If a certain property is possessed by the number 0(the commencement of the induction) and if, for every number n which has the property, its successor also has the property(the induction step), then the property is possessed by all the natural numbers.

Step 1 When $n = 0, 10^k \geq 0$, it is satisfied.

Step 2 Assume $n = k, 10^k \geq k$, is satisfied.

Step 3 Then $10^{k+1} - k + 1 = 10 \cdot 10^k - k - 1 = 10^k - k + 9 \cdot 10^k - 1 > 9 \cdot 1 - 1 = 8 > 0.10^{k+1} \geq k + 1$.

Hence, the proof of $10^k \geq n$ is complete.

Then $\frac{1}{10^k} \leq \frac{1}{n} \Rightarrow x - a_k < \frac{1}{n}$(because of $(**)$) $\Rightarrow x - \frac{1}{n} < a_k \Rightarrow y < a_k$(because of $(*)$).
Namely, $\forall y < x$. y is not an upper bound of E .

Hence, x is the smallest upper bound of E. $x = supE$.

The decimal expansion of x is $n_0 \cdot n_1 n_2 n_3 \cdots (6)$.

Conversely, for any infinite decimal(6) the set of number (5)is bounded above, $(0 \leq n_1, n_2, \cdots, n_k < 10$ and $n_1, n_2, \cdots, n_k \in Z)$
$(n_0 + 1) - a_k = n_0 + 1 - (n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k}) = 1 - \frac{n_1}{10} - \frac{n_2}{100} - \cdots - \frac{n_k}{10^k} \geq 1 - \frac{9}{10} - \frac{9}{100} - \cdots - \frac{9}{10^k} = 1 - 9(\frac{1}{10} + \frac{1}{100} + \cdots + \frac{1}{10^k})$

$= 1 - 9 \cdot \frac{\frac{1}{10}\cdot(1-\frac{1}{10^k})}{1-\frac{1}{10}} = 1 - (1 - \frac{1}{10^k}) = \frac{1}{10^k} > 0$

We have $\forall k = 0, 1, 2, \cdots, a_k < n_0 + 1$.

And (6) is the decimal expansion of $supE$.

Acknowledgment

Acknowledgment Professor Osami Yasukura and Yutaka Saburi of Fukui University of Japan have proposed some improvements, I express here my heartfelt gratitude.

References

Akitsuki Yasuo. (1963). *Abstract Algebra*. Tokyo: Inc. p103-109. (in Japanese).

Heinz-Dieter Ebbinghaus, & John H.Ewing. (1991). *Numbers*. (Reprint ed.). Tokyo: Springer, (Chapter 1-2).

Rudin Walter. (1976). *Principles of Mathematical Analysis*.(International ed.). Singapore: McGraw-Hill Book Co,(Chapter 1).

Rudin Walter. (2004). *Real and Complex Analysis*.(3rd ed.). China: McGraw-Hill Book Co, (Chapter 1).

Shoji Maehara. (2003). *On the basis of mathematical induction*. Tokyo: Inc. 2003. p79-86. (in Japanese).