Bring a Nonempty Set, Get a Ring

Manoranjan Singha

Assistant Professor, Department of Mathematics, University of north Bengal
West Bengal, India, PIN-734013

Abstract— A nonempty set equipped with two binary operations which satisfy certain well known properties is called ring. Now a question may arise that 'Is it possible to define binary operations on any nonempty set so that the corresponding algebraic structure becomes a ring?'. This article answers the question in affirmative sense and establishes some results in this context. Bijection between two sets having same cardinality plays the main role in this article.

Keywords — *Binary operation, Ring, Cardinality.*

Mathematics subject classification 2010: 97H20

Main results:
Let's begin with two lemmas which will be used as the main tools to reveal the answer of the aforementioned question.

Lemma 1. There exists commutative ring of any pre-assigned order (except singular and limit cardinals) with identity.
Proof. The rings $(\{0\},+,\cdot)$, $\mathbb{Z}_n$ $(n \geq 2)$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ ensure the existence of commutative ring of order upto c other than 1. Now for any $X \neq \Phi$ consider the set $\{\mathbb{Z}_2\}^X$ of all functions having domain X and codomain $\mathbb{Z}_2$ and define binary operations $\bigoplus$ and $\bigodot$ on it by
$(f \bigoplus g)(x) = f(x) + g(x), \ \forall\ x \in X$ and
$(f \bigodot g)(x) = f(x).g(x), \ \forall\ x \in X.$
Then $(\{\mathbb{Z}_2\}^X, \bigoplus, \bigodot)$ is a commutative ring of order $2^{|X|}$ with identity $I(x) = \bar{1} \in \mathbb{Z}_2 \ \forall\ x \in X$, where $|X|$ denotes the cardinality of X.
Now generalized continuum hypotheses completes the proof.

Lemma 2. There exists commutative ring of any preassigned order.
Proof. Let X be any infinite set and R be the collection of all elements of $\{\mathbb{Z}_2\}^X$ with finite support. Then $(R, @, *)$ is a commutative ring of order $|X|$ where,
$(f@g)(x) = f(x) + g(x), \ \forall\ x \in X$ and
$(f * g)(x) = f(x).g(x), \ \forall\ x \in X.$

Theorem 1. Any nonempty set can be made a commutative ring.
Proof. Suppose X be any nonempty set and consider a commutative ring $(R, +, .)$ so that $|X| = |R|$ (by **Lemma 2**). Let us choose a bijection $f: X \to R$ and define binary operations $\circledS$ and $\star$ in X as follows
$x \circledS y = f^{-1}(f(x) + f(y)), \ \forall\ x, y \in X$ and
$x \star y = f^{-1}(f(x).f(x)), \ \forall\ x, y \in X.$
Then $(X, \circledS, \star)$ is a commutative ring.

Example 1. Consider the bijection $f: \mathbb{N} \to \mathbb{Z}$ defined by
$$f(n) = \frac{n}{2}, \text{ if } n \text{ is even,}$$
$$= \frac{1-n}{2}, \text{ if } n \text{ is odd.}$$
Define a binary operation $\diamond$ on the set $\mathbb{N}$ by
$m \diamond n = f^{-1}(f(m) + f(n)), \ \forall\ m,\ n \in \mathbb{N};$ that is,
$m \diamond n = m + n - 1,$ if m and n are odd,
$\quad = m + n,$ if m and n are even,

$= o - e$, if $o > e$ and

$= 1 - (o - e)$, if $o < e$,

where $o =$Odd$\{m, n\}$ and $e =$Even$\{m, n\}$. It can be verified that $(\mathbb{N}, \diamond)$ is a cyclic group generated by 2 or 3. The identity element of this group is 1 and the inverse of one member of every pair $\{2n, 2n+1\}$ is the other, $n \in \mathbb{N}$.

Again define a binary operation $\square$ on $\mathbb{N}$ by

$m \square n = f^{-1}(f(m).f(n)), \ \forall\ n \in \mathbb{N};$ that is,

$m \square n = 1$, if at least one of m and n is 1,

$$= \frac{(m-1).(n-1)}{2}, \text{ if both are odd and } m \neq 1,\ n \neq 1$$

$$= \frac{m.n}{2}, \text{ if } m \text{ and } n \text{ both are even,}$$

$$= 1 + \frac{(o-1).e}{2}, \text{ if one of } m \text{ and } n \text{ is odd and other is even,}$$

where $o =$Odd$\{m, n\}$ and $e =$Even$\{m, n\}$. Then $(\mathbb{N}, \diamond, \square)$ is a commutative ring with identity 2.

Some results that can be worked out in similar fashion are listed in the following.

Theorem 2. (1) For any nonempty set X and any element e of it there is a binary operation o so that (X, o) forms a group with identity element$e$. If $|X| \leq a$ then o can be defined on X in such a way that (X, o) forms a cyclic group generated by g with identity element e where g and e are any preassigned distinct (if there) elements of X.

(2) Let Y be a nonempty subset of a finite set X so that $|Y|/|X|$. Then there is a binary operation $*$ on X such that Y becomes a subgroup of the group $(X,*)$; if $|X| = a$ or c then replacement of the condition $|Y|/|X|$ by $|X - Y| = a$ or c respectively will not make an exception.

(3) Any set X such that $|X| = p^n$, a or c, where p is a prime and n is any natural number, can be achieved the designation of a field.

Proof. Proofs of (1) and (3) intuitionally follow from the above discussion, rather, let's prove (2). For the first part consider the additive cyclic group $\mathbb{Z}_{|X|}$ and a subgroup H of it so that $|H| = |Y|$. Choose bijections $g: Y \to H$, $h: X - Y \to \mathbb{Z}_{|X|} - H$ and define desired binary operation $*$ on X as follows

$x * y = f^{-1}(f(x) + f(y)), \ \forall\ x, y \in X,$

where the bijection $f: X \to \mathbb{Z}_{|X|}$ is defined by

$f(x) = g(x)$, whenever $x \in Y$

$= h(x)$, whenever $x \in X - Y$

To prove the next part let's begin with the case when $|X| = a$ and Y is a nonempty finite subset of X with $|Y| = n$. Consider the group $(G, .)$ and its subgroup $C_n = \{z; z^n - 1 = 0\}$ where $G = \bigcup_{n \in \mathbb{N}} C_n$ and ' . ' denotes the complex multiplication. Choose bijections $i: Y \to C_n$, $j: X - Y \to G - C_n$, then, construct a bijection $f: X \to G$ defined by

$f(x) = i(x)$, whenever $x \in Y$

$= j(x)$, otherwise.

Then $(X,*)$ is a group and Y is a subgroup of it where

$x * y = f^{-1}(f(x).f(y)), \ \forall\ x, y \in X.$

If $|X| = a = |Y|$ where Y is a subset of X satisfying $|X - Y| = a$ then replace G by the additive group $\mathbb{Q}$ of rational numbers and C_n by the additive group $\mathbb{Z}$ of integers. If $|X| = c$ and Y is nonempty finite then replace G by the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers. If $|X| = c$ and $|Y| = a$ then replace G by the multiplicative group $\mathbb{C}^*$ or $\mathbb{R}^*$ and C_n by $\mathbb{Q}^*$. At the end, if $|X| = c = |Y|$ where Y is a subset of X so that $|X - Y| = c$ then replace G by the multiplicative group $\mathbb{C}^*$ and C_n by $\mathbb{R}^*$.

I conclude proposing the following.

Problem 1: Let X be an infinite set of cardinality greater than c and Y be any nonempty subset of it. Is it possible to define a binary operation o on X so that Y becomes a subgroup of the group (X, o) ?

Problem 2: Is it possible to define binary operations on any infinite set of cardinality greater than c to make it a field ?

Acknowledgement: I am grateful to Professor Alan Dow for suggesting the technique for the proofs of **Lemma 1** and **Lemma 2**.

References

[1] Hewitt, E. and K. Stromberg, Real and Abstract Analysis, Berlin: Springer-Verlag, 1969.

[2] Baumgartner J. E. and Prikry K., Singular cardinals and the generalized continuum hypothesis, Amer. Math. Monthly, 84 (1977), 108-113.

[3] W. B. Easton, Powers of regular cardinals, Ann. Math. Logic 1 (1970), 139-178.