PascGalois Project

Rings and Fields

So far we have focused on groups where only a single binary operation is used. However, there is a second classic algebraic structure that has two binary operations (usually denoted $+$ and $\cdot$) - namely a **ring** R. When just considering the first operation, $(R, +)$ is an abelian group. We always denote the identity element under addition by 0. We also require that the ring multiplication $\cdot$ is associative and R satisfies the distributive laws:

$$a(b + c) = ab + ac \qquad\qquad (a + b)c = ac + bc$$

for all $a, b, c \in R$. Examples of rings include the integers and real numbers (both under the standard addition and multiplication) and the set of all 2×2 matrices with integer entries (under matrix addition and matrix multiplication). Of course, these three examples are all infinite rings.

To see a finite example of a ring, consider the integers modulo n, i.e. $Z_n = \{0, 1, ..., n - 1\}$ for some $n \geq 2$. We already know that $(Z_n, \oplus)$ is an abelian group, where $\oplus$ denotes addition mod n. To obtain a ring structure, we need a second binary operation. Let $\odot$ denote multiplication mod n. For example, if $n = 12$ then $3\odot8 = 0$ and $2 \odot 9 = 6$. Since $\odot$ is associative and the distributive laws hold for $\oplus$ and $\odot$, it follows that $(Z_n, \oplus, \odot)$, which we willdenote by Z_n, is a ring.

Like groups, there are special classes of rings that mathematicians are particularly interested in. For instance, a ring R is *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in R$. Certainly the integers, real numbers, and Z_n all form commutative rings. The ring of 2×2 matrices under matrix addition and matrix multiplication does not form a commutative ring. Can you see why? A ring R is said to have unity if there exists some $1_R \in R$ such that $1_R \cdot a = a \cdot 1_R$ for all $a \in R$. Note that 1_R, if it exists, is the multiplicative identity element of R. To introduce the next class of rings we first need a definition.

> A nonzero element $a \in R$, where R is commutative, is called a *zero divisor* for R if there exists some nonzero $b \in R$ satisfying $ab = 0$.

A commutative ring R with unity is called an *integral domain* if it contains no zero divisors. Note that both the integers and real numbers are integral domains. However, even though Z_n is a commutative ring with unity, it is an integral domain only for certain values of n.

Question: For which values of n does Z_n have zero divisors. (Note: this will determine precisely when Z_n is an integral domain).
Finally, we define a *field* to be a commutative ring where the nonzero elements form a group with respect to multiplication. Note that a field necessarily has a unity element 1_R. In addition, if a is a nonzero element from a field R, then a must have a multiplicative inverse $a^{-1} \in R$ that satisfies $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. Note that every field is an integral domain. Also, every finite integral domain is a field (both of these results should be in your text as theorems and/or exercises).

PascalGT allows the user to experiment with Z_n ring multiplication and other binary operations on a sufficiently small finite set. The Z_n ring multiplication triangles are drawn by placing two elements a and b of $Z_n \setminus \{0\}$ down the sides of the triangle (what will happen if 0 is placed down one of the sides?).

Exercises:

1. Construct triangles (P_{Z_n}, a, b) using various nonzero ring values $a, b \in Z_n$. Note that the operation here is multiplication mod n rather than addition mod n. Try $n = 3, 4, 5, 6, 7, 8$, and 9. Record what happens for each value of n and each combination $a, b \in Z_n$ that you try.

2. Which of your pictures contain elements that are zero divisors? How does the presence of zero divisors affect the corresponding triangles?

3. Describe what your triangles look like when n is prime versus when n is composite. Does this relate to the presence of zero divisors?

4. Do any of the pictures you obtain look similar to Pascal's triangle mod n? Based on this, can you make a conjecture regarding which values of n make Z_n a field?

5. Construct a PascGalois triangle using Z_{15} ring multiplication with 2 down the left side of the triangle and 3 down the right. Give a description of

the resulting triangle. Does this example violate your conjecture from the previous exercise? Why or why not?