

A Primer on Groups, Rings, and Fields

Groups, rings, and fields are familiar objects to us, we just haven't used those terms. Roughly, these are all sets of elements with additional structure (that is, various ways of combining elements to produce an element of the set). Studying this finer structure is the key to many deep facts in number theory.

Informal Definitions A **GROUP** is a set in which you can perform one operation (usually addition or multiplication mod n for us) with some nice properties. A **RING** is a set equipped with two operations, called addition and multiplication. A **RING** is a **GROUP** under addition and satisfies some of the properties of a group for multiplication. A **FIELD** is a **GROUP** under both addition and multiplication.

Definition 1. A **GROUP** is a set G which is **CLOSED** under an operation $*$ (that is, for any $x, y \in G$, $x * y \in G$) and satisfies the following properties:

- (1) *Identity* – There is an element e in G , such that for every $x \in G$, $e * x = x * e = x$.
- (2) *Inverse* – For every x in G there is an element $y \in G$ such that $x * y = y * x = e$, where again e is the identity.
- (3) *Associativity* – The following identity holds for every $x, y, z \in G$:

$$x * (y * z) = (x * y) * z$$

Examples:

- (1) $\mathbb{Z}/n\mathbb{Z}$, fancy notation for the integers mod n under addition.
- (2) $(\mathbb{Z}/n\mathbb{Z})^\times$, more fancy notation for the integers mod n under multiplication. **REMEMBER**, the elements of this set are relatively prime to n so there are $\phi(n)$ elements in this set.
- (3) \mathbb{Z} , the integers under addition. Groups don't have to be finite. Also note that you can't make the integers into a group under multiplication, since elements like 2 don't have an inverse ($1/2$). But we really only care about examples of the type above.

A group is said to be “abelian” if $x * y = y * x$ for every $x, y \in G$. All of the examples above are abelian groups.

Definition 2. A **RING** is a set R which is **CLOSED** under two operations $+$ and \times and satisfying the following properties:

- (1) R is an abelian group under $+$.
- (2) *Associativity of \times* – For every $a, b, c \in R$,

$$a \times (b \times c) = (a \times b) \times c$$

(3) *Distributive Properties* – For every $a, b, c \in R$ the following identities hold:

$$a \times (b + c) = (a \times b) + (a \times c)$$

and

$$(b + c) \times a = b \times a + c \times a.$$

Examples:

- (1) All the examples above of groups are also RINGS. Note that we don't require multiplicative inverses.
- (2) $\mathbb{Z}[x]$, fancy notation for all polynomials with integer coefficients. Multiplication and addition is the usual multiplication and addition of polynomials.

Definition 3. A **FIELD** is a set F which is closed under two operations $+$ and \times such that

- (1) F is an abelian group under $+$ and
- (2) $F - \{0\}$ (the set F without the additive identity 0) is an abelian group under \times .

Examples: $\mathbb{Z}/p\mathbb{Z}$ is a field, since $\mathbb{Z}/p\mathbb{Z}$ is an additive group and $(\mathbb{Z}/p\mathbb{Z}) - \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication. Sometimes when we (or Koblitz) want to emphasize that $\mathbb{Z}/p\mathbb{Z}$ is a field, we use the notation \mathbb{F}_p .

NON-Examples: If n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field, since $(\mathbb{Z}/n\mathbb{Z}) - \{0\} \neq (\mathbb{Z}/n\mathbb{Z})^\times$. There are, in general, lots of other elements than 0 which are not relatively prime to n and hence have no inverse under multiplication.

The theory of these abstract structures is sometimes simpler than dealing with specific examples because we've pared down and listed all the essential properties that should be used in proofs. Here's a simple result from group theory (though we don't bother with the proof since there's already enough notation so far in this document):

Theorem 1 (Corollary to Lagrange's Theorem). *If $x \in G$, a group of size N , then $x^N = e$.*

Notice that when G is $\mathbb{Z}/n\mathbb{Z}$, this is Euler's theorem, since the size of G is then $\phi(n)$ and the statement

$$x^N = e$$

translates to (since e , the identity under multiplication, is 1 in this case)

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$