David O.H. Cutler

Math 146: Lecture 1

January 24, 2024

(The Units of a Ring form a Group) L. et R be a ring, and let $R^\times$ be the set of units in R. Then $R^\times$ is a group under the inherited multiplication.

Proof. Note that $1_R \in R^\times$, and it fulfills the property of the identity. Also, the ring guarentees our multiplicaton is associative, so nothing to prove there.

If u is a unit then, just note so is u^{-1}. We just check then the product of units is a unit, but this is clear as $(u_1u_2)^{-1} = u_2^{-1}u_1^{-1}$. □

Definition A. ring R is called a field if:

1. R is commutative.
2. $R^\times = \{a \in R, a \neq 0\}$.

Definition I. f R is a ring, a *zero-divisor* in R is an element $a \in R$ such that there exists $b \in R, b \neq 0$ where either $ab = 0$ or $ba = 0$.

Example: In $\mathbb{Z}_m$ the zero divisors are those elements with indices that are **not** relatively prime to m.

Lemma I. f R is a ring and $u \in R^\times$, then it is not a zero divisor.

Proof. Note for $ub = 0$, for $b \neq 0$, multiplication by the inverse has $b = (u)^{-1}0 = 0$, a contradiction. A symmetric case follows for the other part of the definition. □

Definition A. commutative ring R is an integral domain is the only zero-divisor is 0.

Recall integral domains have cancellation.

Definition L. et R be a ring. A *formal polynomial* over $\mathbb{R}$ is an expression of the form $\sum_{n=0}^{\infty} a_n x^n$ such that each a_n is in R, such that only finitely many a_n are nonzero. The largest n for which $a_n \neq 0$ is called the degree of F.

Definition W. e define addition of polynomials coefficient-wise. Multiplication is defined in the binomial context.