TW 314 Lecture 21 (Fr 24 Mar. 2017)

Definition $(R, +, \cdot)$ is a commutative ring with unity if

1. $(R, +)$ is an abelian group.
2. R is closed under multiplication $\cdot$.
3. Multiplication $\cdot$ is associative.
4. The distributive law holds.
5. Multiplication $\cdot$ is commutative
6. R contains the multiplicative identity element 1.

Verify that, for any integer $m > 1$, $(\mathbb{Z}_m, +, \cdot)$ is a commutative ring with unity.

Theorem 2.3 $(\mathbb{Z}_m, +, \cdot)$ is a field if and only if m is a prime number.

Proof: If m is not a prime number, then $m = ab$ with $a, b < m$. Therefore a and b are two non-zero elements of $\mathbb{Z}_m$ with product zero in $\mathbb{Z}_m$. It follows that $(\mathbb{Z}_m, +, \cdot)$ is not a field.

For the converse, suppose m is a prime number. We have seen that $(\mathbb{Z}_m, +, \cdot)$ is a commutative ring with unity, and therefore we only have to show that every non-zero element of $\mathbb{Z}_m$ has a multiplicative inverse:

Let a be any non-zero element of $\mathbb{Z}_m$, and let $S = \{1a, 2a, \ldots, (m-1)a\}$. Then $S \subseteq \mathbb{Z}_m - \{0\}$. But the $m-1$ elements of S are distinct, for if $ia = ja$, then m is a divisor of $(i-j)a$ and therefore of $i-j$ (since m is prime), hence $i=j$. It follows that $S = \mathbb{Z}_m - \{0\}$, that is

$$\{1a, 2a, \ldots, (m-1)a\} = \{1, 2, \ldots, (m-1)\}$$

and therefore $ia = 1$ for some $i \in \{1, 2, \ldots, (m-1)\}$, and so a has i as multiplicative inverse. ∎

It can be shown that, for any integer q that is a prime power (that is, $q = p^n$ for some prime number p), there exists a unique field (up to isomorphism) of order q. This field is called the Galois field of order q and is denoted by $GF(q)$.