Lecture notes for Abstract Algebra: Lecture 18

1 Integral domains and fields

Let us recall our definitions:

Definition 1. A commutative ring with identity is called an **integral domain** if

$$a.b = 0 \qquad \Rightarrow \qquad a = 0 \quad \text{or} \quad b = 0.$$

Definition 2. A commutative ring with identity where **every non-zero element has a multiplicative inverse** is called a **field**.

A **non-zero element** $a \in R$ such that $a.b = 0$ for some **non-zero** element $b \in R$, is called a **divisor of zero**. An element in a ring R that has a multiplicative inverse is called **a unit** of R.

Remark 3. An **integral domain** is a commutative ring with identity **without zero divisors**. A **field** is a commutative ring where **every non-zero element is a unit**.

Proposition 4. *A field F has no zero divisors. In other words,* ***Any field F is an integral domain****.*

Proof. If a is an element of the field F and $a \neq 0$, we have a multiplicative inverse a^{-1}. If we have an equation $a \cdot b = 0$, we can multiply both sides by a^{-1}:

$$\begin{aligned} a \cdot b &= 0 \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot 0 \\ b &= 0 \end{aligned}$$

Therefore, there is no element $b \neq 0$ such that $a \cdot b = 0$. □

Example 5. The converse of the above proposition is not true, for example $\mathbb{Z}$ is an example of an integral domain, that is not a field.

We have the following chain of inclusions of fields, giving by regular numerical domains:

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Example 6. Consider the ring $R = \mathbb{Z}_n$. Let $x \in R$. The existence of an element $y \in R$ such that

$$x \cdot y \equiv 1 \pmod{n}$$

is equivalent to the existence of $y, z \in \mathbb{Z}$ satisfying the equation

$$xy - 1 = nz \iff xy - nz = 1.$$

This last equation is equivalent to $\gcd(n, x) = 1$ and therefore an element $x \in \mathbb{Z}_n$ **is a unit if and only if the greatest common divisor** $\gcd(x, n) = 1$. In particular, **the ring $\mathbb{Z}_p$, for p a prime number, is a field**.

Example 7. If $i^2 = -1$, then the set $\mathbb{Z}[i] = \{m + ni \,|\, m, n \in \mathbb{Z}\}$ forms a ring known as the Gaussian integers. It is easily seen that the **Gaussian integers** are a subring of the complex numbers since they are closed under addition and multiplication. Let $\alpha = a + bi$ be a unit in $Z[i]$. Then, the conjugate $\bar{\alpha} = a - bi$ is also a unit since, in general, if $\alpha\beta = 1$, the same is true for the conjugates $\bar{\alpha}\bar{\beta} = 1$. If $\beta = c + di$

$$1 = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = (a^2 + b^2)(c^2 + d^2).$$

Therefore, $a^2 + b^2$ must either be 1 or -1; or, equivalently, $a + bi = \pm 1$ or $a + bi = \pm i$ Therefore, units of this ring are $\pm 1, \pm i$; hence, the Gaussian integers are not a field. We will leave it as an exercise to prove that the Gaussian integers are an integral domain.

Example 8. The set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ is a field. We check that the inverse of the element $a + b\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$ is the element $c + d\sqrt{2}$ given by

$$c + d\sqrt{2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Proposition 9. *Every finite integral domain is a field.*

Proof. Let D be a finite integral domain and D^* be the set of nonzero elements of D. We must show that every element in D^* has an inverse. For each $a \in D^*$ we can define a map

$$\lambda_a : D^* \longrightarrow D^*$$

given by $\lambda_a(d) = ad$. This map makes sense, because if $a, d \neq 0$, then $ad \neq 0$. The map λ_a is one-to-one, since for $d_1, d_2 \in D^*$

$$ad_1 = \lambda_a(d_1) = \lambda_a(d_2) = ad_2 \Rightarrow d_1 = d_2$$

by the left cancellation law of the integral domains. Since D^* is a finite set, the map λ_a must also be onto; hence, for some d, $\lambda_a(d) = ad = 1$. Therefore, a has a right inverse. Since D is commutative, d must also be a left inverse for a. Consequently, D is a field. □

For any nonnegative integer n and any element r in a ring R we write $r + r + \cdots + r$ (n times) as nr.

Definition 10. We define **the characteristic** of a ring R to be the least positive integer n such that $nr = 0$ for all $r \in R$. If no such integer exists, then the characteristic of R is defined to be 0. We will denote the characteristic of R by $\mathrm{char}(R)$.

Example 11. For every prime p, the ring $\mathbb{Z}_p$ is a field of characteristic p, every nonzero element in $\mathbb{Z}_p$ has an inverse; hence, $\mathbb{Z}_p$ is a field. If a is any nonzero element in the field, then $pa = 0$, since the order of any nonzero element in the abelian group $\mathbb{Z}_p$ is p.

Example 12. The ring $\mathbb{Z}$ is a ring of characteristic zero. It is not possible to find a natural number n such that $n \cdot m = 0$ for all $m \in \mathbb{Z}$. In the same way the fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields of characteristic zero.

Remark 13. The characteristic of a ring R with identity 1 is just the order of 1. That is, the smallest n such that $n \cdot 1 = 0$.

Proposition 14. *T he characteristic of an integral domain is either a prime number or zero.*

Proof. Let D be an integral domain and suppose that the characteristic of D is $n \neq 0$. If n is not prime, then $n = ab$,where $1 < a, b < n$. The characteristic of D is the order of the identity 1 Therefore $n1 = 0$ and

$$0 = n1 = (ab)1 = (a1)(b1).$$

As there are no zero divisors in D, either $a1 = 0$ or $b1 = 0$. Hence, the characteristic of D must be less than n, which is a contradiction. Therefore, n must be prime. □

Remark 15. A field F has:

characteristic zero $\iff$ there is a subfield of F isomorphic to $\mathbb{Q}$

characteristic p $\iff$ there is a subfield of F isomorphic to $\mathbb{Z}_p$