LECTURE 1

Author
Tom Jeong

January 8, 2025

Contents

1 D-integral domains

Q(D)-fields of faction, smalliest field containing Define

universa, property theta: D -¿ Q theta injective, k- field (draw down i: D to Q(D)) sending a to (a,1)

and draw phi D(D) to K and say theta = phi composite i

$$\begin{tikzcd}
D \arrow[r, dashed, "\theta"] \arrow[d, "i"'] & K \\
Q(D) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

- $i : D \to Q(D)$ sends $a \mapsto (a, 1)$
- θ is injective
- K is a field
- $\theta = \phi \circ i$

2 Characteristic of a Ring

Let R be a unital commutative ring. The characteristic of R, denoted $\text{char}(R)$, is defined as follows:

Definition 2.1. The characteristic of a ring R is the smallest positive integer n such that

$$n \cdot 1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = 0_R$$

If no such positive integer exists, we say $\text{char}(R) = 0$.

Proposition 2.1. For a unital commutative ring R, exactly one of the following holds:

1. $\text{char}(R) = 0$: In this case, the additive subgroup generated by 1_R is infinite.
2. $\text{char}(R) = n > 0$: In this case, n is the smallest positive integer such that $n \cdot 1_R = 0_R$.

If $k \cdot 1_R = m \cdot 1_R$ for some integers k, m, then:

$$(k - m) \cdot 1_R = 0_R$$

This means that if $\text{char}(R) = n > 0$, then n divides $k - m$.

example:

1. $\text{char}(\mathbb{Z}) = 0$
2. $\text{char}(\mathbb{Q}) = 0$

3. char($\mathbb{F}_p$) $= p$ for any prime field

4. For any field K, char(K) is either 0 or a prime number

Proposition 2.2. If R is a domain (i.e., has no zero divisors), then char(R) is either 0 or prime.

Proof.
s = char(k) and $s = ab$ where $a, b < s$
$(a \cdot 1)(b \cdot 1) = (a \cdot b) \cdot 1 = 0 \to a \cdot 1 = 0$ or $b \cdot 1 = 0$ but $a, b < s$ $\square$

k-field:: $char(K) = 0 \to \mathbb{Q} \subseteq K$
$char(K) = p \to \mathbb{Z}_p$ or $\mathbb{F}_| \subseteq K$
$\mathbb{Q}$ or $\mathbb{Z}_p$ are called prime subfields of K.

---

3 vector Space

Proposition 3.1. Lets say a field is inside another field, $F \subseteq K$ then K is an F-vector space

So vector space over F (F field) if

1. $s_1 s_2 \in S \to s_1 + s_2 \in S$

2. $c \cdot s_1 \in S, c \in F$

3. $c(s_1 + s_2) = cs_1 + cs_2$

$\mathbb{R} \subseteq \mathbb{C}$

$a + bi$
1, i is a basis of $\mathbb{C}$ over $\mathbb{R}$
$\mathbb{C} \cong \mathbb{R}^2$ but then
$\mathbb{Q} \subseteq \mathbb{R}$ .. $\mathbb{R}$ is an infinite-dimensional vector space over $\mathbb{Q}$

K is a field extension of F

Proposition 3.2 (freshmans dream).
if $char(K) = p, K$ field then, $(x + y)^p = x^p + y^p$

Proof. binomial expansion of

$$
\begin{aligned}
(x+y)^p &= x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p \\
&= x^p + \cancelto{0}{\binom{p}{1}}x^{p-1}y + \cancelto{0}{\binom{p}{2}}x^{p-2}y^2 + \cdots + \cancelto{0}{\binom{p}{p-1}}xy^{p-1} + y^p \\
&= x^p + y^p
\end{aligned}
$$

In characteristic p, all binomial coefficients $\binom{p}{k}$ for $1 \leq k \leq p-1$ are divisible by p, hence equal to zero in the field. ☐

Let K be a field of characteristic $p > 0$. The Frobenius homomorphism $\phi : K \to K$ is defined as:

$$
\begin{aligned}
\phi : K &\to K \\
x &\mapsto x^p
\end{aligned}
$$

Proposition 3.3 (Properties of Frobenius)**.** The map ϕ is a ring homomorphism:

1. $\phi(x+y) = (x+y)^p = x^p + y^p = \phi(x) + \phi(y)$ (using the binomial expansion in char p)
2. $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$
3. $\phi(1) = 1^p = 1$

Example 3.4. In $\mathbb{F}_p$, the Frobenius map is the identity map since:

$$a^p = a \text{ for all } a \in \mathbb{F}_p$$

This is known as Fermat's Little Theorem.

Goal Theorem:

Theorem 3.5.
K-field, K(x) - polynomial rings.

1. For any polynomials $f, g \in K[x]$, there exists a greatest common divisor $d \in K[x]$ such that:
$$d = af + bg \quad \text{for some } a, b \in K[x]$$
This is known as Bézout's identity in $K[x]$.

2. $K[x]$ is a Principal Ideal Domain (PID).

3. $K[x]$ is a Unique Factorization Domain (UFD).

4. For any polynomial $f(x) \in K[x]$, the following are equivalent:
   (a) $f(x)$ is irreducible in $K[x]$
   (b) The quotient ring $K[x]/\langle f(x)\rangle$ is a field

Proof. $K \subseteq K[x]/\langle f(x)\rangle$ □

4 Euclidian Domain

A integral domain D is a Euclidian Domain (ED) if there exists a function

$$\delta : R \to \mathbb{Z}_{\geq 0} \text{ st}$$
$$\delta(0) = 0$$

and for all $a \in D, b \in D^* = D\backslash\{0\}$,
there exists $g, r \in D$ such that $a = qb = r$
AND $\delta(r) \leq \delta(b)$

This allows us t define division with remainder.
$\delta^{-1}(0) = 0$
$\delta(b) = 0, b \neq 0$
$a = qb + r \to \delta(r) < \delta(b) \to\leftarrow$
example: $\mathbb{Z}, \delta(r) = |r|$

Definition 4.1 (PID)**.** D-integral domain is a PID, if all ideals in D are principal, generated by one element

Proposition 4.1. every euclidian domain is a PID

Proof.
$\{0\}$ principal $\langle 0\rangle$
$D = \langle 1\rangle$

I - proper ideal of D: wts a single element that generates all of I. let $b \in I$ be the element with the smallest positive δ
then we would like to claim that $I = \langle b \rangle$

suppose that $a \in I$. Then $a = qb + r$ wgere $\delta(r) < \delta(b)$
$r = a - qb$ a, qb in Ideal, thus r is in ideal.
$\delta(r)$ must be 0 ($r = 0$) since b is the smallest element.
$\therefore a \in \langle b \rangle$ □

In PID there is a well-defined $gcd(a, b)$ where $a, b \in D$.
And: $d = gcd(a, b) \to d = af + bg$ where $f, g \in D$

Proof.

$$a, b \in D$$
$$\langle a, b \rangle = \langle d \rangle$$
$$d = gcd(a, b)$$
$gcd(a, b)$ is only depende oup to units. since d in ideal of a b

□

example: $\mathbb{Z}$ and 8, 12