Abstract Algebra
: Lecture 7

Leo

2024.10.10

Definition 1. *Let R be a ring. If each non-zero element of R has inverse, then R is a division ring. Further, a commutative division ring is a field.*

Example 2. *Let $R = \{\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} | \alpha, \beta \in \mathbb{C}\}$, where $\bar{\alpha} = \overline{a+bi} = a - bi$. Then R is a division ring, which is not commutative.*

Check: 1. R is a ring. 2. Each non-zero element of R has inverse $\frac{1}{\alpha^2+\beta^2}\begin{bmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{bmatrix}$. 3. R is not commutative.

This ring is called quaternion ring $\mathbb{H}$.

Definition 3. *Let E be a field, and let $F \subset E$ be a subfield. Then E is an extension of F.*

Example 4. *$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and there is no proper subfield of $\mathbb{Q}$.*

Example 5. *Consider $\mathbb{Q} \subset S \subset \mathbb{R}$.*

1. $S_1 = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. It's easy to check that S_1 is a field.

2. $S_2 = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$. It's easy to check that S_2 is also a field.

Are S_1 and S_2 the same field? No. Suppose $\phi : S_1 \to S_2$ then it must fix 1 so $\phi(2) = 2$, $2 = \phi(2) = (\phi(\sqrt{2}))^2 = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$, so $a^2 + 3b^2 = 2$ and $2ab = 0$. Since $a, b \in \mathbb{Q}$, $a = 0$ or $b = 0$. If $a = 0$ then $3b^2 = 2$, which is impossible. If $b = 0$ then $a^2 = 2$, which is also impossible. So ϕ is not well-defined.

3. $S_3 = \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} | a, b \in \mathbb{Q}\}$ where n is not a square integer. Then S_3 is a field.

4. $S = \mathbb{Q}(2^{\frac{1}{3}})$, the samllest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and $2^{\frac{1}{3}}$. Then $S = \{a + b2^{\frac{1}{3}} + c2^{\frac{2}{3}} | a, b, c \in \mathbb{Q}\}$.

Theorem 6. *Let $F = \mathbb{Q}$ or $\mathbb{F}_p$. Let $R = F[x]$. Take $p(x) \in R$ s.t. $p(x)$ is irreducible i.e. $p(x)$ is not a product of two non-constant polynomials in R. And let $I = (p(x))$. Then $S = R/I$ is a field. (Recall: I is a maximal ideal in R, this is because R is a principal ideal domain and $p(x)$ is irreducible if and only if $(p(x))$ is maximal.)*

证明. Suppose $f(x) + I$ has inverse, i.e. $(f(x) + I)(g(x) + I) = 1 + I \Rightarrow f(x)g(x) = 1 + I \Rightarrow f(x)g(x) = 1 + p(x)q(x)$ for some $q(x) \in R$. Then $fg - pq = 1$. By Euclid Algorithm, $\gcd(f, p) = 1$. But p is irreducible, so this is always ture. □

Now we look back to S, let $p(x) = x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$. Then $S' = \mathbb{Q}[x]/(x^3-2)$ is a field. And $\phi : S \to S'$ s.t. $2^{\frac{1}{3}} \mapsto x$ is a field isomorphism. Then S is a field.

Exercise 7. *Let $F = \mathbb{F}_3 = \{0, 1, 2\}$ be a field. Let $p(x) = x^2 + 1$, check that $p(x)$ is irreducible over F. This means that $F[x]/(x^2+1)$ is a field. Find a basis for $F[x]/(x^2+1)$ as a vector space over F.*

Theorem 8. *If F is a finite field. Then $|F| = p^d$, where p is a prime number and d is a positive integer.*

Example 9. *Question: Find an irreducible polynomial of degree 2 over $\mathbb{F}_2$.*

$x^2 + 1 = x^2 - 1 = (x+1)(x-1) = (x+1)^2$ is not irreducible.

$p(x) = x^2 + x + 1$ is irreducible. Thus $\mathbb{F}_2[x]/(p(x))$ is a field of order 2^2.

Question: Is there a field of order 6?

No, since 6 is not a p's power. So why we need a p's power?

finite field always has a characteristic.

Definition 10. *Let F be a field. Let n be the smallest non-negtive integer s.t. $n \cdot 1 = 0$. Then n is called the characteristic of F. If n is not a positive integer, then F is said to have characteristic 0.*

Lemma 11. *The char of a field is either 0 or a prime number.*

证明. If $n = pq$, then $(p \cdot 1)(q \cdot 1) = 0 \Rightarrow p$ *or* $q = 0$. (least. → $p\cdot 1=0$ or $q\cdot 1=0$) □

Example 12. $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$, $\mathrm{char}(\mathbb{F}_{p^d}) = p$.

Theorem 13. *Any field contains a subfield which is isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p.*

证明. Let E be the smallest subfield of F. Then $0, 1 \in E$, and hence $n \cdot 1 \in E$ and $\frac{m}{n} \cdot \in E$. If $\mathrm{char}(F) = 0$, then $E \simeq \mathbb{Q}$, if $\mathrm{char}(F) = p$, then $E \simeq \mathbb{F}_p$. □

Definition 14. *$\mathbb{Q}$ and $\mathbb{F}_p$ are called the prime fields.*

$\mathbb{F}_p = GF(p) = \mathbb{Z}/p\mathbb{Z}$.