代数结构
Chapter 3: Field Fundamentals

Shengli Liu (刘胜利)

liu-sl@cs.sjtu.edu.cn
Lab of Cryptography and Information Security
密码与信息安全实验室
计算机科学与工程系
上海交通大学

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$<a_1,\ldots,a_n>=<d>$，其中$d=\gcd(a_1,\ldots,a_n)$，且$d=\sum_{i=1}^{n}\mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d=\gcd(a_1,\ldots$ 且$d=\sum_{i=1}^{n}\mu_i a_i$。Ex: $(\mathbb{Z},+,\cdot)$，$(\mathbb{F}[x],+,\cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；
  设R是整环且$S=R\setminus\{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n > = < d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$ 且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n > = < d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$
  且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；
  设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1,\ldots,a_n >=< d >$，其中$d=\gcd(a_1,\ldots,a_n)$，且$d=\sum_{i=1}^n \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d=\gcd(a_1,\ldots$ 且$d=\sum_{i=1}^n \mu_i a_i$。Ex: $(\mathbb{Z},+,\cdot)$，$(\mathbb{F}[x],+,\cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；设R是整环且$S=R\setminus\{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n > = < d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$ 且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n > = < d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$ 且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n > = < d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$ 且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

环的回顾

- 我们只考虑有1的环，任意的真理想可以构造R/I商环；
- 有1的交换环：R/P得到整环；R/M得到域；
- 整环：整除，因子，gcd, lcm, irreducible, prime；
- UFD：gcd, lcm的存在性；irreducible=prime；
- PD：(non-zero)prime ideal=maximal ideal；$< a_1, \ldots, a_n >=< d >$，其中$d = \gcd(a_1, \ldots, a_n)$，且$d = \sum_{i=1}^{n} \mu_i a_i$；
- ED：(Extended) Euclid Algorithm 可以计算出d和μ_i使得$d = \gcd(a_1, \ldots$ 且$d = \sum_{i=1}^{n} \mu_i a_i$。Ex: $(\mathbb{Z}, +, \cdot)$，$(\mathbb{F}[x], +, \cdot)$
- 构造域的方法：$ED/(p)$，其中p为素元；
  设R是整环且$S = R \setminus \{0\}$，则R/S是包含R同构环的最小的域，称为R的分式域（商域）；

素域

域至少包括两个元素$0, 1$。最小的域为二元域$(\mathbb{Z}_2, +, \cdot)$。

Theorem 2.1

设R是一个有单位元e的环，则

$$\phi : \mathbb{Z} \to R$$

$$m \to me$$

是一个环同态。

1. 如果R的特征为0，则R中包含一个与$\mathbb{Z}$同构的子环。
2. 如果R的特征为$n(n > 0)$，则R中包含一个与$\mathbb{Z}_n$同构的子环；

域同态总是单同态

Lemma 2.2

Let $f : \mathbb{F} \mapsto \mathbb{E}$ be a homomorphism of fields, i.e., $f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)$ (all $a, b \in F$), and $f(1_{\mathbb{F}}) = 1_E$. Then f is a monomorphism(单同态).

Proof.

- First note that a field $\mathbb{F}$ has no ideals except $\{0\}$ and $\mathbb{F}$. For if a is a nonzero member of the ideal I, then $ab = 1$ for some $b \in \mathbb{F}$, hence $1 \in I$, and therefore $I = \mathbb{F}$.
- Taking I to be the kernel of f, we see that I cannot be all of $\mathbb{F}$ because $f(1) = 0$. Thus I must be $\{0\}$, so that f is injective.

$\square$

域同态总是单同态

Lemma 2.2

Let $f : \mathbb{F} \mapsto \mathbb{E}$ be a homomorphism of fields, i.e., $f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)$ (all $a, b \in F$), and $f(1_{\mathbb{F}}) = 1_E$. Then f is a monomorphism(单同态).

Proof.

- First note that a field $\mathbb{F}$ has no ideals except $\{0\}$ and $\mathbb{F}$. For if a is a nonzero member of the ideal I, then $ab = 1$ for some $b \in \mathbb{F}$, hence $1 \in I$, and therefore $I = \mathbb{F}$.
- Taking I to be the kernel of f, we see that I cannot be all of $\mathbb{F}$ because $f(1) = 0$. Thus I must be $\{0\}$, so that f is injective.

□

域同态总是单同态

Lemma 2.2

Let $f : \mathbb{F} \mapsto \mathbb{E}$ be a homomorphism of fields, i.e., $f(a + b) = f(a) + f(b), f(ab) = f(a)f(b)$ (all $a, b \in F$), and $f(1_{\mathbb{F}}) = 1_E$. Then f is a monomorphism(单同态).

Proof.

- First note that a field $\mathbb{F}$ has no ideals except $\{0\}$ and $\mathbb{F}$. For if a is a nonzero member of the ideal I, then $ab = 1$ for some $b \in \mathbb{F}$, hence $1 \in I$, and therefore $I = \mathbb{F}$.
- Taking I to be the kernel of f, we see that I cannot be all of $\mathbb{F}$ because $f(1) = 0$. Thus I must be $\{0\}$, so that f is injective.

□

域同态总是单同态

Definition 2.3

一个域$\mathbb{F}$如果不包含任何真子域，则$\mathbb{F}$是一个素域。

Theorem 2.4

设$\mathbb{F}$是一个域，则

1. 如果$\mathbb{F}$的特征为0，则$\mathbb{F}$中包含一个与$\mathbb{Q}$同构的(素)子域。
2. 如果$\mathbb{F}$的特征为素数p，则$\mathbb{F}$中包含一个与$(\mathbb{Z}_p,+,\cdot)$同构的(素)域；

Proof.

域同构

$$\phi:\mathbb{Q}\rightarrow\mathbb{F}$$

$$n/m\rightarrow(ne)(me)^{-1}$$

环同构$\phi:\mathbb{Z}\rightarrow\mathbb{F}$，且$n\rightarrow(ne)$。

多项式环$\mathbb{F}[x]$

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a Euclidean domain, PID, and UFD.

- $\forall f(x) \in \mathbb{F}(x)$ can be factored into a product of irreducible polynomials.
- An irreducible polynomial is a prime element in $\mathbb{F}[x]$.
- Every ideal in $\mathbb{F}[x]$ is generated by a polynomial, i.e. $I = (f(x))$.

Example. x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$, but $x^2+1 = (x+i)(x-i)$ can be factored completely in $\mathbb{C}[x]$.

多项式环$\mathbb{F}[x]$

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a Euclidean domain, PID, and UFD.

- $\forall f(x) \in \mathbb{F}(x)$ can be factored into a product of irreducible polynomials.
- An irreducible polynomial is a prime element in $\mathbb{F}[x]$.
- Every ideal in $\mathbb{F}[x]$ is generated by a polynomial, i.e. $I = (f(x))$.

Example. x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$, but $x^2+1 = (x+i)(x-i)$ can be factored completely in $\mathbb{C}[x]$.

多项式环$\mathbb{F}[x]$

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a Euclidean domain, PID, and UFD.

- $\forall f(x) \in \mathbb{F}(x)$ can be factored into a product of irreducible polynomials.
- An irreducible polynomial is a prime element in $\mathbb{F}[x]$.
- Every ideal in $\mathbb{F}[x]$ is generated by a polynomial, i.e. $I = (f(x))$.

Example. x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$, but $x^2+1 = (x+i)(x-i)$ can be factored completely in $\mathbb{C}[x]$.

多项式环$\mathbb{F}[x]$

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a Euclidean domain, PID, and UFD.

- $\forall f(x) \in \mathbb{F}(x)$ can be factored into a product of irreducible polynomials.
- An irreducible polynomial is a prime element in $\mathbb{F}[x]$.
- Every ideal in $\mathbb{F}[x]$ is generated by a polynomial, i.e. $I = (f(x))$.

Example. x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$, but $x^2+1 = (x+i)(x-i)$ can be factored completely in $\mathbb{C}[x]$.

多项式环$\mathbb{F}[x]$

Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a Euclidean domain, PID, and UFD.

- $\forall f(x) \in \mathbb{F}(x)$ can be factored into a product of irreducible polynomials.
- An irreducible polynomial is a prime element in $\mathbb{F}[x]$.
- Every ideal in $\mathbb{F}[x]$ is generated by a polynomial, i.e. $I = (f(x))$.

Example. x^2+1 is an irreducible polynomial in $\mathbb{R}[x]$, but $x^2+1 = (x+i)(x-i)$ can be factored completely in $\mathbb{C}[x]$.

Field Extensions

Definition 3.1 (Field Extensions)

If $\mathbb{F}$ and $\mathbb{E}$ are fields and $\mathbb{F} \subseteq \mathbb{E}$, we say that $\mathbb{E}$ is an extension of $\mathbb{F}$, and we write $\mathbb{F} \leq \mathbb{E}$, or sometimes $\mathbb{E}/\mathbb{F}$.

Fact 3.2

If $\mathbb{F} \leq \mathbb{E}$, then $\mathbb{E}$ is a vector space over $\mathbb{F}$. The dimension of this vector space is called the degree of the extension, written $[\mathbb{E} : \mathbb{F}]$.

- *If $[\mathbb{E} : \mathbb{F}] = n < \infty$, we say that $\mathbb{E}$ is a finite extension of $\mathbb{F}$.*
- *or that the extension $\mathbb{E}/\mathbb{F}$ is finite, $\mathbb{E}$ is of degree n over $\mathbb{F}$.*

Example 3.3

$[\mathbb{C} : \mathbb{R}] = 2$;
$[\mathbb{Q}(x) : \mathbb{Q}] = \infty$。

Field Extensions

Definition 3.1 (Field Extensions)

If $\mathbb{F}$ and $\mathbb{E}$ are fields and $\mathbb{F} \subseteq \mathbb{E}$, we say that $\mathbb{E}$ is an extension of $\mathbb{F}$, and we write $\mathbb{F} \leq \mathbb{E}$, or sometimes $\mathbb{E}/\mathbb{F}$.

Fact 3.2

If $\mathbb{F} \leq \mathbb{E}$, then $\mathbb{E}$ is a vector space over $\mathbb{F}$. The dimension of this vector space is called the degree of the extension, written $[\mathbb{E} : \mathbb{F}]$.

- *If $[\mathbb{E} : \mathbb{F}] = n < \infty$, we say that $\mathbb{E}$ is a finite extension of $\mathbb{F}$.*
- *or that the extension $\mathbb{E}/\mathbb{F}$ is finite, $\mathbb{E}$ is of degree n over $\mathbb{F}$.*

Example 3.3

$[\mathbb{C} : \mathbb{R}] = 2$;

$[\mathbb{Q}(x) : \mathbb{Q}] = \infty$。

Field Extensions

Definition 3.1 (Field Extensions)

If $\mathbb{F}$ and $\mathbb{E}$ are fields and $\mathbb{F} \subseteq \mathbb{E}$, we say that $\mathbb{E}$ is an extension of $\mathbb{F}$, and we write $\mathbb{F} \leq \mathbb{E}$, or sometimes $\mathbb{E}/\mathbb{F}$.

Fact 3.2

If $\mathbb{F} \leq \mathbb{E}$, then $\mathbb{E}$ is a vector space over $\mathbb{F}$. The dimension of this vector space is called the degree of the extension, written $[\mathbb{E} : \mathbb{F}]$.

- *If $[\mathbb{E} : \mathbb{F}] = n < \infty$, we say that $\mathbb{E}$ is a finite extension of $\mathbb{F}$.*
- *or that the extension $\mathbb{E}/\mathbb{F}$ is finite, $\mathbb{E}$ is of degree n over $\mathbb{F}$.*

Example 3.3

$[\mathbb{C} : \mathbb{R}] = 2$;

$[\mathbb{Q}(x) : \mathbb{Q}] = \infty$。

Field Extensions

Definition 3.1 (**Field Extensions**)

If $\mathbb{F}$ and $\mathbb{E}$ are fields and $\mathbb{F} \subseteq \mathbb{E}$, we say that $\mathbb{E}$ is an extension of $\mathbb{F}$, and we write $\mathbb{F} \leq \mathbb{E}$, or sometimes $\mathbb{E}/\mathbb{F}$.

Fact 3.2

If $\mathbb{F} \leq \mathbb{E}$, then $\mathbb{E}$ is a vector space over $\mathbb{F}$. The dimension of this vector space is called the degree of the extension, written $[\mathbb{E} : \mathbb{F}]$.

- *If $[\mathbb{E} : \mathbb{F}] = n < \infty$, we say that $\mathbb{E}$ is a finite extension of $\mathbb{F}$.*
- *or that the extension $\mathbb{E}/\mathbb{F}$ is finite, $\mathbb{E}$ is of degree n over $\mathbb{F}$.*

Example 3.3

$[\mathbb{C} : \mathbb{R}] = 2$;
$[\mathbb{Q}(x) : \mathbb{Q}] = \infty$。

Theorem 3.4

Let f be a nonconstant polynomial over the field $\mathbb{F}$, i.e., $f(x) \in \mathbb{F}[x]$ and $deg(f) \geq 1$. Then there is an extension $\mathbb{E}/\mathbb{F}$ and an element $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$.

Proof.

- Since f can be factored into irreducibles, we may assume that f itself is irreducible. The ideal $I =< f(X) >$ in $\mathbb{F}[X]$ is prime, in fact maximal.
- Thus $\mathbb{E} = \mathbb{F}[X]/I$ is a field. We can place an isomorphic copy of $\mathbb{F}$ inside $\mathbb{E}$ via the homomorphism $h : a \mapsto a+I$; h is a monomorphism, we may identify $\mathbb{F} \leq \mathbb{E}$.
- Now let $\alpha = X + I$; if $f(X) = a_0 + a_1 X + \ldots + a_n X^n$, then

$$\begin{aligned} f(\alpha) &= (a_0 + I) + \ldots + a_n(X + I)^n \\ &= (a_0 + \ldots + a_n X^n) + I = f(X) + I \end{aligned}$$

Theorem 3.4

Let f be a nonconstant polynomial over the field $\mathbb{F}$, i.e., $f(x) \in \mathbb{F}[x]$ and $deg(f) \geq 1$. Then there is an extension $\mathbb{E}/\mathbb{F}$ and an element $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$.

Proof.

- Since f can be factored into irreducibles, we may assume that f itself is irreducible. The ideal $I =< f(X) >$ in $\mathbb{F}[X]$ is prime, in fact maximal.
- Thus $\mathbb{E} = \mathbb{F}[X]/I$ is a field. We can place an isomorphic copy of $\mathbb{F}$ inside $\mathbb{E}$ via the homomorphism $h : a \mapsto a+I$; h is a monomorphism, we may identify $\mathbb{F} \leq \mathbb{E}$.
- Now let $\alpha = X + I$; if $f(X) = a_0 + a_1X + \ldots + a_nX^n$, then

$$\begin{aligned} f(\alpha) &= (a_0 + I) + \ldots + a_n(X+I)^n \\ &= (a_0 + \ldots + a_nX^n) + I = f(X) + I \end{aligned}$$

Theorem 3.4

Let f be a nonconstant polynomial over the field $\mathbb{F}$, i.e., $f(x) \in \mathbb{F}[x]$ and $deg(f) \geq 1$. Then there is an extension $\mathbb{E}/\mathbb{F}$ and an element $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$.

Proof.

- Since f can be factored into irreducibles, we may assume that f itself is irreducible. The ideal $I =< f(X) >$ in $\mathbb{F}[X]$ is prime, in fact maximal.
- Thus $\mathbb{E} = \mathbb{F}[X]/I$ is a field. We can place an isomorphic copy of $\mathbb{F}$ inside $\mathbb{E}$ via the homomorphism $h : a \mapsto a+I$; h is a monomorphism, we may identify $\mathbb{F} \leq \mathbb{E}$.
- Now let $\alpha = X + I$; if $f(X) = a_0 + a_1X + \ldots + a_nX^n$, then

$$\begin{aligned} f(\alpha) &= (a_0 + I) + \ldots + a_n(X + I)^n \\ &= (a_0 + \ldots + a_nX^n) + I = f(X) + I \end{aligned}$$

Theorem 3.4

Let f be a nonconstant polynomial over the field $\mathbb{F}$, i.e., $f(x) \in \mathbb{F}[x]$ and $deg(f) \geq 1$. Then there is an extension $\mathbb{E}/\mathbb{F}$ and an element $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$.

Proof.

- Since f can be factored into irreducibles, we may assume that f itself is irreducible. The ideal $I = < f(X) >$ in $\mathbb{F}[X]$ is prime, in fact maximal.
- Thus $\mathbb{E} = \mathbb{F}[X]/I$ is a field. We can place an isomorphic copy of $\mathbb{F}$ inside $\mathbb{E}$ via the homomorphism $h : a \mapsto a + I$; h is a monomorphism, we may identify $\mathbb{F} \leq \mathbb{E}$.
- Now let $\alpha = X + I$; if $f(X) = a_0 + a_1 X + \ldots + a_n X^n$, then

$$\begin{aligned} f(\alpha) &= (a_0 + I) + \ldots + a_n (X + I)^n \\ &= (a_0 + \ldots + a_n X^n) + I = f(X) + I \end{aligned}$$

Theorem 3.5

Let f and g be polynomials over the field F, i.e, $f(x), g(x) \in \mathbb{F}[x]$. Then f and g are relatively prime if and only if f and g have no common root in any extension of $\mathbb{F}$.

Proof.

- If f and g are relatively prime, so there are polynomials $a(X)$ and $b(X)$ over F such that $a(X)f(X) + b(X)g(X) = 1$. If α is a common root of f and g, then the substitution of α for X yields $0 = 1$, a contradiction.
- Conversely, if the $\gcd d(X)$ of $f(X)$ and $g(X)$ is nonconstant, let $\mathbb{E}$ be an extension of $\mathbb{F}$ in which $d(X)$ has a root α. Since $d(X)$ divides both $f(X)$ and $g(X)$, α is a common root of f and g in $\mathbb{E}$.

$\square$

Theorem 3.5

Let f and g be polynomials over the field F, i.e, $f(x), g(x) \in \mathbb{F}[x]$. Then f and g are relatively prime if and only if f and g have no common root in any extension of $\mathbb{F}$.

Proof.

- If f and g are relatively prime, so there are polynomials $a(X)$ and $b(X)$ over F such that $a(X)f(X) + b(X)g(X) = 1$. If α is a common root of f and g, then the substitution of α for X yields $0 = 1$, a contradiction.
- Conversely, if the $\gcd$ $d(X)$ of $f(X)$ and $g(X)$ is nonconstant, let $\mathbb{E}$ be an extension of $\mathbb{F}$ in which $d(X)$ has a root α. Since $d(X)$ divides both $f(X)$ and $g(X)$, α is a common root of f and g in $\mathbb{E}$.

□

Theorem 3.5

Let f and g be polynomials over the field F, i.e, $f(x), g(x) \in \mathbb{F}[x]$. Then f and g are relatively prime if and only if f and g have no common root in any extension of $\mathbb{F}$.

Proof.

- If f and g are relatively prime, so there are polynomials $a(X)$ and $b(X)$ over F such that $a(X)f(X) + b(X)g(X) = 1$. If α is a common root of f and g, then the substitution of α for X yields $0 = 1$, a contradiction.
- Conversely, if the $\gcd$ $d(X)$ of $f(X)$ and $g(X)$ is nonconstant, let $\mathbb{E}$ be an extension of $\mathbb{F}$ in which $d(X)$ has a root α. Since $d(X)$ divides both $f(X)$ and $g(X)$, α is a common root of f and g in $\mathbb{E}$.

$\square$

Corollary 3.6

If f and g are distinct monic irreducible polynomials over $\mathbb{F}$, then f and g have no common roots in any extension of $\mathbb{F}$.

Proof.

$\mathbb{F}[X]$ is a Euclidean Domain, so f and g are relatively prime. $\square$

Corollary 3.6

If f and g are distinct monic irreducible polynomials over $\mathbb{F}$, then f and g have no common roots in any extension of $\mathbb{F}$.

Proof.

$\mathbb{F}[X]$ is a Euclidean Domain, so f and g are relatively prime. $\square$

代数元及代数扩张

设$\alpha \in \mathbb{E}$。那么在$\mathbb{E}$中包括$\mathbb{F}$和元素α的最小环为

$$\mathbb{F}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m, \mid\ m \in \mathbb{N}, a_i \in \mathbb{F}\}$$

$$\mathbb{F}[\alpha] = \{a(\alpha) \mid\ a(x) \in \mathbb{F}[x]\}.$$

$\mathbb{E}$中包括$\mathbb{F}$和元素α的最小扩域为

$$\begin{aligned} \mathbb{F}(\alpha) &= \left\{ \frac{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m}{b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n} \mid m, n \in \mathbb{N}, a_i, b_j \in \mathbb{F}, \sum_{j=0}^{n} b_j\alpha^j \neq 0 \right\}. \\ &= \left\{ \frac{a(\alpha)}{b(\alpha)} \mid a(x), b(x) \in \mathbb{F}[x], b(\alpha) \neq 0 \right\} \end{aligned}$$

Fact 4.1

$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$;

$\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$.

代数元及代数扩张

Definition 4.2 (Algebraic Extensions)

- If $\mathbb{F} \leq \mathbb{E}$, the element $\alpha \in \mathbb{E}$ is said to be algebraic(代数元) over F if there is a nonconstant polynomial $f \in \mathbb{F}[X]$ such that $f(\alpha) = 0$;
- if α is not algebraic over $\mathbb{F}$, it is said to be transcendental(超越元) over $\mathbb{F}$. If every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$, then $\mathbb{E}$ is said to be an algebraic extension of $\mathbb{F}$.

代数元及代数扩张

Definition 4.2 (Algebraic Extensions)

- If $\mathbb{F} \leq \mathbb{E}$, the element $\alpha \in \mathbb{E}$ is said to be algebraic(代数元) over F if there is a nonconstant polynomial $f \in \mathbb{F}[X]$ such that $f(\alpha) = 0$;
- if α is not algebraic over $\mathbb{F}$, it is said to be transcendental(超越元) over $\mathbb{F}$. If every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$, then $\mathbb{E}$ is said to be an algebraic extension of $\mathbb{F}$.

极小多项式

- Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, and let I be the set of all polynomials g over $\mathbb{F}$ such that $g(\alpha) = 0$.
- I is an ideal of $\mathbb{F}[X]$, and since $\mathbb{F}[X]$ is a PID, I consists of all multiples of some $m(X) \in \mathbb{F}[X]$.
- $m(X)$ is monic and unique, which is called the minimal polynomial of α over $\mathbb{F}$, sometimes written as $min(\alpha, \mathbb{F})$. The polynomial $m(X)$ has the following properties:

1. If $g \in \mathbb{F}[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This follows because $g(\alpha) = 0$ iff $g(X) \in I$, and $I =< m(X) >$, the ideal generated by $m(X)$.
2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$. This follows from **(1)**.
3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. If $m(X) = h(X)k(X)$ with deg h and deg k less than deg m, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that by (1), either $h(X)$ or $k(X)$ is a

- Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, and let I be the set of all polynomials g over $\mathbb{F}$ such that $g(\alpha) = 0$.
- I is an ideal of $\mathbb{F}[X]$, and since $\mathbb{F}[X]$ is a PID, I consists of all multiples of some $m(X) \in \mathbb{F}[X]$.
- $m(X)$ is monic and unique, which is called the minimal polynomial of α over $\mathbb{F}$, sometimes written as $min(\alpha, \mathbb{F})$. The polynomial $m(X)$ has the following properties:

1. If $g \in \mathbb{F}[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This follows because $g(\alpha) = 0$ iff $g(X) \in I$, and $I =< m(X) >$, the ideal generated by $m(X)$.
2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$. This follows from **(1)**.
3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. If $m(X) = h(X)k(X)$ with deg h and deg k less than deg m, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that by (1), either $h(X)$ or $k(X)$ is a

极小多项式

- Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, and let I be the set of all polynomials g over $\mathbb{F}$ such that $g(\alpha) = 0$.
- I is an ideal of $\mathbb{F}[X]$, and since $\mathbb{F}[X]$ is a PID, I consists of all multiples of some $m(X) \in \mathbb{F}[X]$.
- $m(X)$ is monic and unique, which is called the minimal polynomial of α over $\mathbb{F}$, sometimes written as $min(\alpha, \mathbb{F})$. The polynomial $m(X)$ has the following properties:

1. If $g \in \mathbb{F}[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This follows because $g(\alpha) = 0$ iff $g(X) \in I$, and $I =< m(X) >$, the ideal generated by $m(X)$.
2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$. This follows from **(1)**.
3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. If $m(X) = h(X)k(X)$ with deg h and deg k less than deg m, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that by (1), either $h(X)$ or $k(X)$ is a

极小多项式

- Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, and let I be the set of all polynomials g over $\mathbb{F}$ such that $g(\alpha) = 0$.
- I is an ideal of $\mathbb{F}[X]$, and since $\mathbb{F}[X]$ is a PID, I consists of all multiples of some $m(X) \in \mathbb{F}[X]$.
- $m(X)$ is monic and unique, which is called the minimal polynomial of α over $\mathbb{F}$, sometimes written as $min(\alpha, \mathbb{F})$. The polynomial $m(X)$ has the following properties:

1. If $g \in \mathbb{F}[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This follows because $g(\alpha) = 0$ iff $g(X) \in I$, and $I =< m(X) >$, the ideal generated by $m(X)$.
2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$. This follows from **(1)**.
3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. If $m(X) = h(X)k(X)$ with deg h and deg k less than deg m, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that by (1), either $h(X)$ or $k(X)$ is a

极小多项式

- Suppose that $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$, and let I be the set of all polynomials g over $\mathbb{F}$ such that $g(\alpha) = 0$.
- I is an ideal of $\mathbb{F}[X]$, and since $\mathbb{F}[X]$ is a PID, I consists of all multiples of some $m(X) \in \mathbb{F}[X]$.
- $m(X)$ is monic and unique, which is called the minimal polynomial of α over $\mathbb{F}$, sometimes written as $min(\alpha, \mathbb{F})$. The polynomial $m(X)$ has the following properties:

1. If $g \in \mathbb{F}[X]$, then $g(\alpha) = 0$ if and only if $m(X)$ divides $g(X)$. This follows because $g(\alpha) = 0$ iff $g(X) \in I$, and $I =< m(X) >$, the ideal generated by $m(X)$.
2. $m(X)$ is the monic polynomial of least degree such that $m(\alpha) = 0$. This follows from **(1)**.
3. $m(X)$ is the unique monic irreducible polynomial such that $m(\alpha) = 0$. If $m(X) = h(X)k(X)$ with deg h and deg k less than deg m, then either $h(\alpha) = 0$ or $k(\alpha) = 0$, so that by (1), either $h(X)$ or $k(X)$ is a

极小多项式

Theorem 5.1

- *If $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ and the minimal polynomial $m(X)$ of α over $\mathbb{F}$ has degree n, then $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$, the set of polynomials in α with coefficients in $\mathbb{F}$.*
- *In fact, $\mathbb{F}[\alpha]$ is the set $\mathbb{F}_{n-1}[\alpha]$ of all polynomials of degree at most $n-1$ with coefficients in $\mathbb{F}$, and $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for the vector space $\mathbb{F}[\alpha]$ over the field $\mathbb{F}$. Consequently, $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.*

Proof:

- Let $f(X)$ be any nonzero polynomial over F of degree $n-1$ or less. Then since $m(X)$ is irreducible and $\deg f < \deg m$, $f(X)$ and $m(X)$ are relatively prime, and there are polynomials $a(X)$ and $b(X)$ over $\mathbb{F}$ such that $a(X)f(X) + b(X)m(X) = 1$.

极小多项式

Theorem 5.1

- *If $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ and the minimal polynomial $m(X)$ of α over $\mathbb{F}$ has degree n, then $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$, the set of polynomials in α with coefficients in $\mathbb{F}$.*
- *In fact, $\mathbb{F}[\alpha]$ is the set $\mathbb{F}_{n-1}[\alpha]$ of all polynomials of degree at most $n-1$ with coefficients in $\mathbb{F}$, and $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for the vector space $\mathbb{F}[\alpha]$ over the field $\mathbb{F}$. Consequently, $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.*

Proof:

- Let $f(X)$ be any nonzero polynomial over F of degree $n-1$ or less. Then since $m(X)$ is irreducible and deg $f <$ deg m, $f(X)$ and $m(X)$ are relatively prime, and there are polynomials $a(X)$ and $b(X)$ over $\mathbb{F}$ such that $a(X)f(X) + b(X)m(X) = 1$.

Theorem 5.1

- *If $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{F}$ and the minimal polynomial $m(X)$ of α over $\mathbb{F}$ has degree n, then $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$, the set of polynomials in α with coefficients in $\mathbb{F}$.*
- *In fact, $\mathbb{F}[\alpha]$ is the set $\mathbb{F}_{n-1}[\alpha]$ of all polynomials of degree at most $n-1$ with coefficients in $\mathbb{F}$, and $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for the vector space $\mathbb{F}[\alpha]$ over the field $\mathbb{F}$. Consequently, $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.*

Proof:

- Let $f(X)$ be any nonzero polynomial over F of degree $n-1$ or less. Then since $m(X)$ is irreducible and deg $f <$ deg m, $f(X)$ and $m(X)$ are relatively prime, and there are polynomials $a(X)$ and $b(X)$ over $\mathbb{F}$ such that $a(X)f(X) + b(X)m(X) = 1$.

极小多项式

- But then $a(\alpha)f(\alpha) = 1$, so that any nonzero element of $F_{n-1}[\alpha]$ has a multiplicative inverse. It follows that $F_{n-1}[\alpha]$ is a field.
- Now any field containing $\mathbb{F}$ and α must contain all polynomials in α, in particular all polynomials of degree at most $n-1$. Therefore $\mathbb{F}_{n-1}[\alpha] \subseteq F[\alpha] \subseteq \mathbb{F}(\alpha)$. But $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α, so$\mathbb{F}(\alpha) \subseteq \mathbb{F}_{n-1}[\alpha]$, and we conclude that $\mathbb{F}_{n-1}[\alpha] = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.
- Finally, the elements $1, \alpha, \ldots, \alpha_{n-1}$ certainly span $\mathbb{F}_{n-1}[\alpha]$, and they are linearly independent because if a nontrivial linear combination of these elements were zero, we would have a nonzero polynomial of degree less than that of $m(X)$ with α as a root, a contradiction.

  □

极小多项式

- But then $a(\alpha)f(\alpha) = 1$, so that any nonzero element of $F_{n-1}[\alpha]$ has a multiplicative inverse. It follows that $F_{n-1}[\alpha]$ is a field.
- Now any field containing $\mathbb{F}$ and α must contain all polynomials in α, in particular all polynomials of degree at most $n-1$. Therefore $\mathbb{F}_{n-1}[\alpha] \subseteq F[\alpha] \subseteq \mathbb{F}(\alpha)$. But $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α, so$\mathbb{F}(\alpha) \subseteq \mathbb{F}_{n-1}[\alpha]$, and we conclude that $\mathbb{F}_{n-1}[\alpha] = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.
- Finally, the elements $1, \alpha, \ldots, \alpha_{n-1}$ certainly span $\mathbb{F}_{n-1}[\alpha]$, and they are linearly independent because if a nontrivial linear combination of these elements were zero, we would have a nonzero polynomial of degree less than that of $m(X)$ with α as a root, a contradiction. □

极小多项式

- But then $a(\alpha)f(\alpha) = 1$, so that any nonzero element of $F_{n-1}[\alpha]$ has a multiplicative inverse. It follows that $F_{n-1}[\alpha]$ is a field.
- Now any field containing $\mathbb{F}$ and α must contain all polynomials in α, in particular all polynomials of degree at most $n-1$. Therefore $\mathbb{F}_{n-1}[\alpha] \subseteq F[\alpha] \subseteq \mathbb{F}(\alpha)$. But $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α, so$\mathbb{F}(\alpha) \subseteq \mathbb{F}_{n-1}[\alpha]$, and we conclude that $\mathbb{F}_{n-1}[\alpha] = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.
- Finally, the elements $1, \alpha, \ldots, \alpha_{n-1}$ certainly span $\mathbb{F}_{n-1}[\alpha]$, and they are linearly independent because if a nontrivial linear combination of these elements were zero, we would have a nonzero polynomial of degree less than that of $m(X)$ with α as a root, a contradiction. $\square$

Lemma 5.2

Suppose that $\mathbb{F} \leq K \leq \mathbb{E}$, the elements $\alpha_i, i \in I$, form a basis for $\mathbb{E}$ over K, and the elements $\beta_j, j \in J$, form a basis for K over $\mathbb{F}$. (I and J need not be finite.) Then the products $\alpha_i\beta_j, i \in I, j \in J$, form a basis for $\mathbb{E}$ over $\mathbb{F}$.

Proof:

If $\gamma \in \mathbb{E}$, then γ is a linear combination of the α_i with coefficients $a_i \in K$, and each a_i is a linear combination of the β_j with coefficients $b_{ij} \in \mathbb{F}$. It follows that the $\alpha_i\beta_j$span $\mathbb{E}$ over $\mathbb{F}$. Now if $\sum_{i,j} \gamma_{ij}\alpha_i\beta_j = 0$, then $\sum_i \gamma_{ij}\alpha_i = 0$ for all j, and consequently $\gamma_{ij} = 0$ for all i, j, and the $\alpha_i\beta_j$ are linearly independent.

Lemma 5.2

Suppose that $\mathbb{F} \leq K \leq \mathbb{E}$, the elements $\alpha_i, i \in I$, form a basis for $\mathbb{E}$ over K, and the elements $\beta_j, j \in J$, form a basis for K over $\mathbb{F}$. (I and J need not be finite.) Then the products $\alpha_i\beta_j, i \in I, j \in J$, form a basis for $\mathbb{E}$ over $\mathbb{F}$.

Proof:

If $\gamma \in \mathbb{E}$, then γ is a linear combination of the α_i with coefficients $a_i \in K$, and each a_i is a linear combination of the β_j with coefficients $b_{ij} \in \mathbb{F}$. It follows that the $\alpha_i\beta_j$span $\mathbb{E}$ over $\mathbb{F}$. Now if $\sum_{i,j} \gamma_{ij}\alpha_i\beta_j = 0$, then $\sum_i \gamma_{ij}\alpha_i = 0$ for all j, and consequently $\gamma_{ij} = 0$ for all i, j, and the $\alpha_i\beta_j$ are linearly independent.

Corollary 5.3

If $\mathbb{F} \leq K \leq \mathbb{E}$, *then* $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : K][K : \mathbb{F}]$.

Theorem 5.4

If $\mathbb{E}$ *is a finite extension of* $\mathbb{F}$, *then* $\mathbb{E}$ *is an algebraic extension of* $\mathbb{F}$.

Proof.

Let $\alpha \in \mathbb{E}$, and let $n = [\mathbb{E} : \mathbb{F}]$. Then $1, \alpha, \ldots, \alpha^n$ are $n + 1$ vectors in an n-dimensional vector space, so they must be linearly dependent. Thus α is a root of a nonzero polynomial with coefficients in $\mathbb{F}$, which means that α is algebraic over $\mathbb{F}$. □

Corollary 5.3

If $\mathbb{F} \leq K \leq \mathbb{E}$, *then* $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : K][K : \mathbb{F}]$.

Theorem 5.4

If $\mathbb{E}$ *is a finite extension of* $\mathbb{F}$, *then* $\mathbb{E}$ *is an algebraic extension of* $\mathbb{F}$.

Proof.

Let $\alpha \in \mathbb{E}$, and let $n = [\mathbb{E} : \mathbb{F}]$. Then $1, \alpha, \ldots, \alpha^n$ are $n+1$ vectors in an n-dimensional vector space, so they must be linearly dependent. Thus α is a root of a nonzero polynomial with coefficients in $\mathbb{F}$, which means that α is algebraic over $\mathbb{F}$. □

Corollary 5.3

If $\mathbb{F} \le K \le \mathbb{E}$, *then* $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : K][K : \mathbb{F}]$.

Theorem 5.4

If $\mathbb{E}$ *is a finite extension of* $\mathbb{F}$, *then* $\mathbb{E}$ *is an algebraic extension of* $\mathbb{F}$.

Proof.

Let $\alpha \in \mathbb{E}$, and let $n = [\mathbb{E} : \mathbb{F}]$. Then $1, \alpha, \ldots, \alpha^n$ are $n + 1$ vectors in an n-dimensional vector space, so they must be linearly dependent. Thus α is a root of a nonzero polynomial with coefficients in $\mathbb{F}$, which means that α is algebraic over $\mathbb{F}$. □

$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$

Theorem 6.1

Let $\mathbb{F} \subseteq K$*, and* $\mathbb{F}, K$ *be fields. Let* $S_1 \subseteq K, S_2 \subseteq K$*. Then*

$$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2).$$

Proof.

- Both $\mathbb{F}(S_1 \cup S_2)$ and $\mathbb{F}(S_1)(S_2)$ are extension fields of $\mathbb{F}$ which contain F, S_1, and S_2. Hence $\mathbb{F}(S_1 \cup S_2) \subseteq \mathbb{F}(S_1)(S_2)$.
- $\mathbb{F}(S_1)$ is a subfield of $\mathbb{F}(S_1 \cup S_2)$. Then both $\mathbb{F}(S_1)$ and (S_2) are subsets of $\mathbb{F}(S_1 \cup S_2)$, hence $\mathbb{F}(S_1)(S_2) \subseteq \mathbb{F}(S_1 \cup S_2)$.

So $\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$.

□

$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$

Theorem 6.1

Let $\mathbb{F} \subseteq K$, and $\mathbb{F}, K$ be fields. Let $S_1 \subseteq K, S_2 \subseteq K$. Then

$$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2).$$

Proof.

- Both $\mathbb{F}(S_1 \cup S_2)$ and $\mathbb{F}(S_1)(S_2)$ are extension fields of $\mathbb{F}$ which contain F, S_1, and S_2. Hence $\mathbb{F}(S_1 \cup S_2) \subseteq \mathbb{F}(S_1)(S_2)$.
- $\mathbb{F}(S_1)$ is a subfield of $\mathbb{F}(S_1 \cup S_2)$. Then both $\mathbb{F}(S_1)$ and (S_2) are subsets of $\mathbb{F}(S_1 \cup S_2)$, hence $\mathbb{F}(S_1)(S_2) \subseteq \mathbb{F}(S_1 \cup S_2)$.

So $\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$. $\square$

Theorem 6.1

Let $\mathbb{F} \subseteq K$*, and* $\mathbb{F}, K$ *be fields. Let* $S_1 \subseteq K, S_2 \subseteq K$*. Then*

$$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2).$$

Proof.

- Both $\mathbb{F}(S_1 \cup S_2)$ and $\mathbb{F}(S_1)(S_2)$ are extension fields of $\mathbb{F}$ which contain F, S_1, and S_2. Hence $\mathbb{F}(S_1 \cup S_2) \subseteq \mathbb{F}(S_1)(S_2)$.
- $\mathbb{F}(S_1)$ is a subfield of $\mathbb{F}(S_1 \cup S_2)$. Then both $\mathbb{F}(S_1)$ and (S_2) are subsets of $\mathbb{F}(S_1 \cup S_2)$, hence $\mathbb{F}(S_1)(S_2) \subseteq \mathbb{F}(S_1 \cup S_2)$.

So $\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$. □

$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$

Theorem 6.1

Let $\mathbb{F} \subseteq K$, and $\mathbb{F}, K$ be fields. Let $S_1 \subseteq K, S_2 \subseteq K$. Then

$$\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2).$$

Proof.

- Both $\mathbb{F}(S_1 \cup S_2)$ and $\mathbb{F}(S_1)(S_2)$ are extension fields of $\mathbb{F}$ which contain F, S_1, and S_2. Hence $\mathbb{F}(S_1 \cup S_2) \subseteq \mathbb{F}(S_1)(S_2)$.
- $\mathbb{F}(S_1)$ is a subfield of $\mathbb{F}(S_1 \cup S_2)$. Then both $\mathbb{F}(S_1)$ and (S_2) are subsets of $\mathbb{F}(S_1 \cup S_2)$, hence $\mathbb{F}(S_1)(S_2) \subseteq \mathbb{F}(S_1 \cup S_2)$.

So $\mathbb{F}(S_1 \cup S_2) = \mathbb{F}(S_1)(S_2)$.

□

Splitting Fields

If $\mathbb{F} \leq \mathbb{E}$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$, we will use the notation $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ for the subfield of $\mathbb{E}$ generated by $\mathbb{F}$ and the α_i. Thus $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ is the smallest subfield of $\mathbb{E}$ containing all elements of $\mathbb{F}$ along with the α_i.

Definition 6.2

- If $\mathbb{F} \leq \mathbb{E}$ and $f \in \mathbb{F}[X]$, we say that f splits over $\mathbb{E}$ if f can be written as $\lambda(X - \alpha_1) \ldots (X - \alpha_k)$ for some $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$ and $\lambda \in \mathbb{F}$.
- If $\mathbb{F} \leq K$ and $f \in \mathbb{F}[X]$, we say that K is a splitting field for f over F if f splits over K but not over any proper subfield of K containing $\mathbb{F}$.

If $\mathbb{F} \leq \mathbb{E}$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$, we will use the notation $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ for the subfield of $\mathbb{E}$ generated by $\mathbb{F}$ and the α_i. Thus $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ is the smallest subfield of $\mathbb{E}$ containing all elements of $\mathbb{F}$ along with the α_i.

Definition 6.2

- If $\mathbb{F} \leq \mathbb{E}$ and $f \in \mathbb{F}[X]$, we say that f splits over $\mathbb{E}$ if f can be written as $\lambda(X - \alpha_1) \ldots (X - \alpha_k)$ for some $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$ and $\lambda \in \mathbb{F}$.
- If $\mathbb{F} \leq K$ and $f \in \mathbb{F}[X]$, we say that K is a splitting field for f over F if f splits over K but not over any proper subfield of K containing $\mathbb{F}$.

Splitting Fields

If $\mathbb{F} \leq \mathbb{E}$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$, we will use the notation $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ for the subfield of $\mathbb{E}$ generated by $\mathbb{F}$ and the α_i. Thus $\mathbb{F}(\alpha_1, \ldots, \alpha_k)$ is the smallest subfield of $\mathbb{E}$ containing all elements of $\mathbb{F}$ along with the α_i.

Definition 6.2

- If $\mathbb{F} \leq \mathbb{E}$ and $f \in \mathbb{F}[X]$, we say that f splits over $\mathbb{E}$ if f can be written as $\lambda(X - \alpha_1) \ldots (X - \alpha_k)$ for some $\alpha_1, \ldots, \alpha_k \in \mathbb{E}$ and $\lambda \in \mathbb{F}$.
- If $\mathbb{F} \leq K$ and $f \in \mathbb{F}[X]$, we say that K is a splitting field for f over F if f splits over K but not over any proper subfield of K containing $\mathbb{F}$.

Splitting Fields

Theorem 6.3

If $f \in \mathbb{F}[X]$ and deg $f = n$, then f has a splitting field K over $\mathbb{F}$ with $[K : \mathbb{F}] \leq n!$.

Proof.

- $\mathbb{F}$ has an extension $\mathbb{E}_1$ containing a root α_1 of f, and the extension $\mathbb{F}(\alpha_1)/\mathbb{F}$ has degree at most n.
- We may then write $f(X) = \lambda(X - \alpha_1)^{r_1} g(X)$, where α_1 is not a root of g and deg $g \leq n-1$. If g is nonconstant, we can find an extension of $\mathbb{F}(\alpha_1)$ containing a root α_2 of g, and the extension $\mathbb{F}(\alpha_1, \alpha_2)$ will have degree at most $n-1$ over $\mathbb{F}(\alpha_1)$.
- Continue inductively and we can reach an extension of degree at most $n!$ containing all the roots of f.

□

Splitting Fields

Theorem 6.3

If $f \in \mathbb{F}[X]$ and deg $f = n$, then f has a splitting field K over $\mathbb{F}$ with $[K : \mathbb{F}] \leq n!$.

Proof.

- $\mathbb{F}$ has an extension $\mathbb{E}_1$ containing a root α_1 of f, and the extension $\mathbb{F}(\alpha_1)/\mathbb{F}$ has degree at most n.
- We may then write $f(X) = \lambda(X - \alpha_1)^{r_1} g(X)$, where α_1 is not a root of g and deg $g \leq n - 1$. If g is nonconstant, we can find an extension of $\mathbb{F}(\alpha_1)$ containing a root α_2 of g, and the extension $\mathbb{F}(\alpha_1, \alpha_2)$ will have degree at most $n - 1$ over $\mathbb{F}(\alpha_1)$.
- Continue inductively and we can reach an extension of degree at most $n!$ containing all the roots of f.

□

Splitting Fields

Theorem 6.4

Let $f(x) \in \mathbb{F}[x]$. Suppose that $f(x)$ splits over $\mathbb{E}$, i.e.,

$$f(x) = b(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $b \neq 0$. $\mathbb{E}$ is the splitting field of $f(x)$ iff $\mathbb{E} = \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.

Proof.

Let $\mathbb{E}$ be the splitting field of $f(x)$.

- $f(x)$ splits over $\mathbb{F}(\alpha_1, \cdots, \alpha_n)$, so $\mathbb{E} \subseteq \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.
- The splitting field $\mathbb{E}$ contains $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. $\mathbb{F}(\alpha_1, \cdots, \alpha_m)$ is the smallest field containing $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. So $\mathbb{F}(\alpha_1, \cdots, \alpha_m) \subseteq \mathbb{E}$.

$\square$

Splitting Fields

Theorem 6.4

Let $f(x) \in \mathbb{F}[x]$. Suppose that $f(x)$ splits over $\mathbb{E}$, i.e.,

$$f(x) = b(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $b \neq 0$. $\mathbb{E}$ is the splitting field of $f(x)$ iff $\mathbb{E} = \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.

Proof.

Let $\mathbb{E}$ be the splitting field of $f(x)$.

- $f(x)$ splits over $\mathbb{F}(\alpha_1, \cdots, \alpha_n)$, so $\mathbb{E} \subseteq \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.
- The splitting field $\mathbb{E}$ contains $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. $\mathbb{F}(\alpha_1, \cdots, \alpha_m)$ is the smallest field containing $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. So $\mathbb{F}(\alpha_1, \cdots, \alpha_m) \subseteq \mathbb{E}$.

□

Splitting Fields

Theorem 6.4

Let $f(x) \in \mathbb{F}[x]$. Suppose that $f(x)$ splits over $\mathbb{E}$, i.e.,

$$f(x) = b(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $b \neq 0$. $\mathbb{E}$ is the splitting field of $f(x)$ iff $\mathbb{E} = \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.

Proof.

Let $\mathbb{E}$ be the splitting field of $f(x)$.

- $f(x)$ splits over $\mathbb{F}(\alpha_1, \cdots, \alpha_n)$, so $\mathbb{E} \subseteq \mathbb{F}(\alpha_1, \cdots, \alpha_m)$.
- The splitting field $\mathbb{E}$ contains $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. $\mathbb{F}(\alpha_1, \cdots, \alpha_m)$ is the smallest field containing $\mathbb{F}, \alpha_1, \cdots, \alpha_n$. So $\mathbb{F}(\alpha_1, \cdots, \alpha_m) \subseteq \mathbb{E}$.

□

Splitting Fields

Theorem 6.5

If α and β are roots of the irreducible polynomial $f \in \mathbb{F}[X]$ in an extension $\mathbb{E}$ of $\mathbb{F}$, then $\mathbb{F}(\alpha)$ is isomorphic to $\mathbb{F}(\beta)$ via an isomorphism that carries α into β and is the identity on $\mathbb{F}$.

Proof.

- Without loss of generality we may assume f monic (if not, divide f by its leading coefficient). f is the minimal polynomial of both α and β. The elements of $\mathbb{F}(\alpha)$ can be expressed uniquely as $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, where the a_i belong to $\mathbb{F}$ and n is the degree of f. The desired isomorphism is given by:

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}.$$

□

Splitting Fields

Theorem 6.5

If α and β are roots of the irreducible polynomial $f \in \mathbb{F}[X]$ in an extension $\mathbb{E}$ of $\mathbb{F}$, then $\mathbb{F}(\alpha)$ is isomorphic to $\mathbb{F}(\beta)$ via an isomorphism that carries α into β and is the identity on $\mathbb{F}$.

Proof.

- Without loss of generality we may assume f monic (if not, divide f by its leading coefficient). f is the minimal polynomial of both α and β. The elements of $\mathbb{F}(\alpha)$ can be expressed uniquely as $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, where the a_i belong to $\mathbb{F}$ and n is the degree of f. The desired isomorphism is given by:

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}.$$

□

Splitting Fields

Lemma 6.6

Let $p(x) \in \mathbb{F}[x]$ be an irreducible polynomial. Let α be a root over an extended field $\mathbb{E}$. Let $\phi : \mathbb{F} \to \mathbb{F}'$ be a field isomorphism. Let α' be $\phi(p(x))$ a root over some extended field E'. Then there exists an isomorphism $i : \mathbb{F}(\alpha) \to \mathbb{F}'(\alpha')$, which, when restricted on $\mathbb{F}$, results in ϕ.

Proof.

$\phi(p(x)) \in \mathbb{F}'[x]$ is irreducible since $p(x) \in \mathbb{F}[x]$ is irreducible.

- $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(p(x))$;
- $\mathbb{F}'(\alpha') \cong \mathbb{F}'[x]/(\phi(p(x)))$;
- $\mathbb{F}[x]/(p(x)) \cong \mathbb{F}'[x]/(\phi(p(x)))$.
- $\mathbb{F}(\alpha) \xrightarrow{\rho} \mathbb{F}[x]/(p(x)) \xrightarrow{\phi} \mathbb{F}'[x]/(\phi(p(x))) \xrightarrow{\sigma} \mathbb{F}'(\alpha')$. So the isomorphism function is $\sigma\phi\rho$.

□

Splitting Fields

Definition 6.7

If $\mathbb{E}$ and $\mathbb{E}'$ are extensions of $\mathbb{F}$ and i is an isomorphism of $\mathbb{E}$ and $\mathbb{E}'$, we say that i is an $\mathbb{F}$-isomorphism if i fixes $\mathbb{F}$, that is, $i(a) = a$ for every $a \in \mathbb{F}$. $\mathbb{F}$-homomorphisms, $\mathbb{F}$-monomorphisms, etc., are defined similarly.

Theorem 6.8

Isomorphism Extension Theorem: *Suppose that $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic, and the isomorphism i carries the polynomial $f \in \mathbb{F}[X]$ to $f' \in \mathbb{F}'[X]$.*

- *If K is a splitting field for f over $\mathbb{F}$ and K' is a splitting field for f' over $\mathbb{F}'$, then i can be extended to an isomorphism of K and K'.*
- *In particular, if $\mathbb{F} = \mathbb{F}'$ and i is the identity function, we conclude that any two splitting fields of f are $\mathbb{F}$-isomorphic.*

Splitting Fields

Definition 6.7

If $\mathbb{E}$ and $\mathbb{E}'$ are extensions of $\mathbb{F}$ and i is an isomorphism of $\mathbb{E}$ and $\mathbb{E}'$, we say that i is an $\mathbb{F}$-isomorphism if i fixes $\mathbb{F}$, that is, $i(a) = a$ for every $a \in \mathbb{F}$. $\mathbb{F}$-homomorphisms, $\mathbb{F}$-monomorphisms, etc., are defined similarly.

Theorem 6.8

Isomorphism Extension Theorem: *Suppose that $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic, and the isomorphism i carries the polynomial $f \in \mathbb{F}[X]$ to $f' \in \mathbb{F}'[X]$.*

- *If K is a splitting field for f over $\mathbb{F}$ and K' is a splitting field for f' over $\mathbb{F}'$, then i can be extended to an isomorphism of K and K'.*
- *In particular, if $\mathbb{F} = \mathbb{F}'$ and i is the identity function, we conclude that any two splitting fields of f are $\mathbb{F}$-isomorphic.*

Splitting Fields

Definition 6.7

If $\mathbb{E}$ and $\mathbb{E}'$ are extensions of $\mathbb{F}$ and i is an isomorphism of $\mathbb{E}$ and $\mathbb{E}'$, we say that i is an $\mathbb{F}$-isomorphism if i fixes $\mathbb{F}$, that is, $i(a) = a$ for every $a \in \mathbb{F}$. $\mathbb{F}$-homomorphisms, $\mathbb{F}$-monomorphisms, etc., are defined similarly.

Theorem 6.8

Isomorphism Extension Theorem: *Suppose that $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic, and the isomorphism i carries the polynomial $f \in \mathbb{F}[X]$ to $f' \in \mathbb{F}'[X]$.*

- *If K is a splitting field for f over $\mathbb{F}$ and K' is a splitting field for f' over $\mathbb{F}'$, then i can be extended to an isomorphism of K and K'.*
- *In particular, if $\mathbb{F} = \mathbb{F}'$ and i is the identity function, we conclude that any two splitting fields of f are $\mathbb{F}$-isomorphic.*

Splitting Fields

Definition 6.7

If $\mathbb{E}$ and $\mathbb{E}'$ are extensions of $\mathbb{F}$ and i is an isomorphism of $\mathbb{E}$ and $\mathbb{E}'$, we say that i is an $\mathbb{F}$-isomorphism if i fixes $\mathbb{F}$, that is, $i(a) = a$ for every $a \in \mathbb{F}$. $\mathbb{F}$-homomorphisms, $\mathbb{F}$-monomorphisms, etc., are defined similarly.

Theorem 6.8

Isomorphism Extension Theorem: *Suppose that $\mathbb{F}$ and $\mathbb{F}'$ are isomorphic, and the isomorphism i carries the polynomial $f \in \mathbb{F}[X]$ to $f' \in \mathbb{F}'[X]$.*

- *If K is a splitting field for f over $\mathbb{F}$ and K' is a splitting field for f' over $\mathbb{F}'$, then i can be extended to an isomorphism of K and K'.*
- *In particular, if $\mathbb{F} = \mathbb{F}'$ and i is the identity function, we conclude that any two splitting fields of f are $\mathbb{F}$-isomorphic.*

Splitting Fields

Proof.

- Carry out the construction of a splitting field for f over F, and perform exactly the same steps to construct a splitting field for f' over $\mathbb{F}'$.
- At every stage, there is only a notational difference between the fields obtained.
- Furthermore, we can do the first construction inside K and the second inside K'. It shows that the splitting fields that we have constructed coincide with K and K'.

□

Splitting Fields

Proof.

- Carry out the construction of a splitting field for f over F, and perform exactly the same steps to construct a splitting field for f' over $\mathbb{F}'$.
- At every stage, there is only a notational difference between the fields obtained.
- Furthermore, we can do the first construction inside K and the second inside K'. It shows that the splitting fields that we have constructed coincide with K and K'.

$\square$

Splitting Fields

Proof.

- Carry out the construction of a splitting field for f over F, and perform exactly the same steps to construct a splitting field for f' over $\mathbb{F}'$.
- At every stage, there is only a notational difference between the fields obtained.
- Furthermore, we can do the first construction inside K and the second inside K'. It shows that the splitting fields that we have constructed coincide with K and K'.

$\square$

Splitting Fields

多项式$f(x) \in \mathbb{F}[x]$的分裂域是惟一的：$f(x)$的任意两个分裂域必是$\mathbb{F}$–同构的。

Splitting Fields

Example 6.9

Find a splitting field for $f(X) = X^3 - 2$ over the rationals $\mathbb{Q}$.

Solution:

- If α is the positive cube root of 2, then the roots of f are $\alpha, \alpha(-1/2 + i\frac{1}{2}\sqrt{3})$ and $\alpha(-1/2 - i\frac{1}{2}\sqrt{3})$.
- The polynomial f is irreducible, either by Eisenstein' s criterion or by the observation that if f were factorable, it would have a linear factor, and there is no rational number whose cube is 2. Thus f is the minimal polynomial of α, so $[Q(\alpha) : Q] = 3$.

Splitting Fields

Example 6.9

Find a splitting field for $f(X) = X^3 - 2$ over the rationals $\mathbb{Q}$.

Solution:

- If α is the positive cube root of 2, then the roots of f are $\alpha, \alpha(-1/2 + i\frac{1}{2}\sqrt{3})$ and $\alpha(-1/2 - i\frac{1}{2}\sqrt{3})$.
- The polynomial f is irreducible, either by Eisenstein's criterion or by the observation that if f were factorable, it would have a linear factor, and there is no rational number whose cube is 2. Thus f is the minimal polynomial of α, so $[Q(\alpha) : Q] = 3$.

Splitting Fields

Example 6.9

Find a splitting field for $f(X) = X^3 - 2$ over the rationals $\mathbb{Q}$.

Solution:

- If α is the positive cube root of 2, then the roots of f are $\alpha, \alpha(-1/2 + i\frac{1}{2}\sqrt{3})$ and $\alpha(-1/2 - i\frac{1}{2}\sqrt{3})$.
- The polynomial f is irreducible, either by Eisenstein's criterion or by the observation that if f were factorable, it would have a linear factor, and there is no rational number whose cube is 2. Thus f is the minimal polynomial of α, so $[Q(\alpha) : Q] = 3$.

- Now since α and $i\sqrt{3}$generate all the roots of f, the splitting field is $K = Q(\alpha, i\sqrt{3})$. Since $i\sqrt{3} \notin Q(\alpha)$, $[Q(\alpha, i\sqrt{3}) : Q(\alpha)]$ is at least 2. But $i\sqrt{3}$ is a root of $X^2 + 3 \in Q(\alpha)[X]$, so the degree of $Q(\alpha, i\sqrt{3})$ over $Q(\alpha)$ is a most 2, and therefore is exactly 2.
- Thus

$$\begin{aligned}[K : Q] &= [Q(\alpha, i\sqrt{3}) : Q] \\ &= [Q(\alpha, i\sqrt{3}) : Q(\alpha)][Q(\alpha) : Q] \\ &= 2 \times 3 = 6 \quad \heartsuit\end{aligned}$$

- Now since α and $i\sqrt{3}$generate all the roots of f, the splitting field is $K = Q(\alpha, i\sqrt{3})$. Since $i\sqrt{3} \notin Q(\alpha)$, $[Q(\alpha, i\sqrt{3}) : Q(\alpha)]$ is at least 2. But $i\sqrt{3}$ is a root of $X^2 + 3 \in Q(\alpha)[X]$, so the degree of $Q(\alpha, i\sqrt{3})$ over $Q(\alpha)$ is a most 2, and therefore is exactly 2.
- Thus

$$\begin{aligned}
[K : Q] &= [Q(\alpha, i\sqrt{3}) : Q] \\
&= [Q(\alpha, i\sqrt{3}) : Q(\alpha)][Q(\alpha) : Q] \\
&= 2 \times 3 = 6 \quad \heartsuit
\end{aligned}$$

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。
- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a\in\mathbb{Z}$的线段；
- 给定三个线段a,b,c，可以做出线段x，使得$a:b=c:x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q\in\mathbb{Q}$的线段；
- 给定两个线段a,b，可以做出线段x，使得$x^2=ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q\in\mathbb{Q}(\sqrt{b})$的线段，其中$b\in\mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a\in\mathbb{Z}$的线段；
- 给定三个线段a,b,c，可以做出线段x，使得$a:b=c:x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q\in\mathbb{Q}$的线段；
- 给定两个线段a,b，可以做出线段x，使得$x^2=ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q\in\mathbb{Q}(\sqrt{b})$的线段，其中$b\in\mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图不能问题

尺规做图问题：给定平面上的一些点，要求用尺规作出另一些点。

- 给定两个点，可以得到过两点的一条直线；
- 给定两个点，可以得到两点间的中点；
- 给定一个线段，和线段外的一个点，可以做出过该点并与已知线段垂直(平行)的一条直线。

- 给定一个单位长度为1的线段，可以做出长度为$\forall a \in \mathbb{Z}$的线段；
- 给定三个线段a, b, c，可以做出线段x，使得$a : b = c : x$；
- 给定一个单位长度为1的线段，可以做出长度为$\forall q \in \mathbb{Q}$的线段；
- 给定两个线段a, b，可以做出线段x，使得$x^2 = ab$；
- 给定一个单位长度为1的线段，可以做出任意长度为$q \in \mathbb{Q}(\sqrt{b})$的线段，其中$b \in \mathbb{Q}$。

分裂域的应用一：尺规做图问题

- 已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意实数。
- 对于任意$b \in \mathbb{Q}(a_1, \cdots, a_n)$，可用尺规做出$\mathbb{Q}(a_1, \cdots, a_n)(\sqrt{b})$中的任意实数，其中$b > 0$。

Definition 6.10

设$F \subseteq K$，而F, K是$\mathbb{R}$的子域。如果$K = F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_m})$，其中$b_i > 0, b_1 \in F, b_i \in F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_{i-1}})$，其中$i \geq 2$，则称$K$为$F$的Pythagoras扩域，称为毕氏扩域。

总结：已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意毕氏扩域中的数。

分裂域的应用一：尺规做图问题

- 已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意实数。
- 对于任意$b \in \mathbb{Q}(a_1, \cdots, a_n)$，可用尺规做出$\mathbb{Q}(a_1, \cdots, a_n)(\sqrt{b})$中的任意实数，其中$b > 0$。

Definition 6.10

设$F \subseteq K$，而F, K是$\mathbb{R}$的子域。如果$K = F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_m})$，其中$b_i > 0, b_1 \in F, b_i \in F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_{i-1}})$，其中$i \geq 2$，则称$K$为$F$的Pythagoras扩域，称为毕氏扩域。

总结：已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意毕氏扩域中的数。

分裂域的应用一：尺规做图问题

- 已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意实数。
- 对于任意$b \in \mathbb{Q}(a_1, \cdots, a_n)$，可用尺规做出$\mathbb{Q}(a_1, \cdots, a_n)(\sqrt{b})$中的任意实数，其中$b > 0$。

Definition 6.10

设$F \subseteq K$，而F, K是$\mathbb{R}$的子域。如果$K = F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_m})$，其中$b_i > 0, b_1 \in F, b_i \in F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_{i-1}})$，其中$i \geq 2$，则称$K$为$F$的Pythagoras扩域，称为毕氏扩域。

总结：已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意毕氏扩域中的数。

分裂域的应用一：尺规做图问题

- 已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意实数。
- 对于任意$b \in \mathbb{Q}(a_1, \cdots, a_n)$，可用尺规做出$\mathbb{Q}(a_1, \cdots, a_n)(\sqrt{b})$中的任意实数，其中$b > 0$。

Definition 6.10

设$F \subseteq K$，而F, K是$\mathbb{R}$的子域。如果$K = F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_m})$，其中$b_i > 0, b_1 \in F, b_i \in F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_{i-1}})$，其中$i \geq 2$，则称$K$为$F$的Pythagoras扩域，称为毕氏扩域。

总结：已知实数$1, a_1, a_2, \cdots, a_n$，利用尺规可以做出$\mathbb{Q}(a_1, \cdots, a_n)$中的任意毕氏扩域中的数。

尺规做图：能行的及不能的

Theorem 6.11

初等几何尺规作图的数学模型：由已知数$1, a_1, a_2, \cdots, a_n$出发，利用尺规可以做出数是且仅是$\mathbb{Q}(a_1, \cdots, a_n)$的毕氏扩域中的数。

Theorem 6.12

F的毕氏扩域E的次数$[E:F] = 2^n$，n是非负整数。

如果一个域F的扩域E的次数$[E:F]$是奇数，则E不是毕氏扩域。

尺规做图：能行的及不能的

Theorem 6.11

初等几何尺规作图的数学模型：由已知数$1, a_1, a_2, \cdots, a_n$出发，利用尺规可以做出数是且仅是$\mathbb{Q}(a_1, \cdots, a_n)$的毕氏扩域中的数。

Theorem 6.12

F的毕氏扩域E的次数$[E:F] = 2^n$，n是非负整数。

如果一个域F的扩域E的次数$[E:F]$是奇数，则E不是毕氏扩域。

尺规做图：能行的及不能的

Theorem 6.11

初等几何尺规作图的数学模型：由已知数$1, a_1, a_2, \cdots, a_n$出发，利用尺规可以做出数是且仅是$\mathbb{Q}(a_1, \cdots, a_n)$的毕氏扩域中的数。

Theorem 6.12

F的毕氏扩域E的次数$[E : F] = 2^n$，n是非负整数。

如果一个域F的扩域E的次数$[E : F]$是奇数，则E不是毕氏扩域。

尺规做图不能问题：三等分角

Example 6.13

三等分角问题：给定任意已知角α，试三等分之。即求$\theta = \alpha/3$。

由于$\cos\alpha = \cos 3\theta = 4\cos^3\theta - 3\cos\theta$，故$\cos\theta$是三次多项式$4x^3 - 3x - \cos\alpha = 0$的根。
上述多项式如果是域$F = \mathbb{Q}(\cos\alpha)$上的既约多项式，则$F(\cos\theta)$是$F$的一个三次扩域，所以不是毕氏扩域，故$\cos\theta$不能用尺规做出。

尺规做图不能问题：三等分角

Example 6.13

三等分角问题：给定任意已知角α，试三等分之。即求$\theta = \alpha/3$。

由于$\cos\alpha = \cos 3\theta = 4\cos^3\theta - 3\cos\theta$，故$\cos\theta$是三次多项式$4x^3 - 3x - \cos\alpha = 0$的根。

上述多项式如果是域$F = \mathbb{Q}(\cos\alpha)$上的既约多项式，则$F(\cos\theta)$是$F$的一个三次扩域，所以不是毕氏扩域，故$\cos\theta$不能用尺规做出。

尺规做图不能问题：三等分角

Example 6.13

三等分角问题：给定任意已知角α，试三等分之。即求$\theta = \alpha/3$。

由于$\cos\alpha = \cos 3\theta = 4\cos^3\theta - 3\cos\theta$，故$\cos\theta$是三次多项式$4x^3 - 3x - \cos\alpha = 0$的根。

上述多项式如果是域$F = \mathbb{Q}(\cos\alpha)$上的既约多项式，则$F(\cos\theta)$是$F$的一个三次扩域，所以不是毕氏扩域，故$\cos\theta$不能用尺规做出。

尺规做图不能问题：立方倍积问题

Example 6.14

将已知一边长为a的立方体，求做另一个立方体，使新的立方体是原来的体积的两倍。

设新的立方体的边长为b，则$b^3 = 2a^3$，即b是方程$x^3 - 2a^3 = 0$的解。如果多项式$x^3 - 2a^3$在$F = \mathbb{Q}(a)$上既约，则$F(b)$是F的一个三次扩域，所以不是毕氏扩域，故b不能用尺规做出。

尺规做图不能问题：立方倍积问题

Example 6.14

将已知一边长为a的立方体，求做另一个立方体，使新的立方体是原来的体积的两倍。

设新的立方体的边长为b，则$b^3 = 2a^3$，即b是方程$x^3 - 2a^3 = 0$的解。如果多项式$x^3 - 2a^3$在$F = \mathbb{Q}(a)$上既约，则$F(b)$是F的一个三次扩域，所以不是毕氏扩域，故b不能用尺规做出。

Example 6.15

将已知半径为a的圆化成一个等面积的正方形。

设正方形的边长为b，则$b^2 = \pi a^2$。故b是二次多项式$x^2 - \pi a^2 = 0$的根。为得到$b = a\sqrt{\pi}$，必须得到π，而π是超越数。令$F = \mathbb{Q}(a)$，则$F(\pi)$是F的∞
扩域，所以不是毕氏扩域，故b不能用尺规做出。

Example 6.15

将已知半径为a的圆化成一个等面积的正方形。

设正方形的边长为b，则$b^2 = \pi a^2$。故b是二次多项式$x^2 - \pi a^2 = 0$的根。
为得到$b = a\sqrt{\pi}$，必须得到π，而π是超越数。令$F = \mathbb{Q}(a)$，则$F(\pi)$是F的∞
扩域，所以不是毕氏扩域，故b不能用尺规做出。

尺规做图不能问题：化圆为方问题

Example 6.15

将已知半径为a的圆化成一个等面积的正方形。

设正方形的边长为b，则$b^2 = \pi a^2$。故b是二次多项式$x^2 - \pi a^2 = 0$的根。为得到$b = a\sqrt{\pi}$，必须得到π，而π是超越数。令$F = \mathbb{Q}(a)$，则$F(\pi)$是F的∞次扩域，所以不是毕氏扩域，故b不能用尺规做出。

Jacobi symbol

Let $P \in \mathbb{Z}$ be a prime. For $x \in \mathbb{Z}_P^*$, define

$$\mathbb{QR}_P = \{x^2 \mid x \in \mathbb{Z}_P^*\},$$

$$\mathbb{QNR}_P = \mathbb{Z}_P^* \setminus \mathbb{QR}_P.$$

For $x \in \mathbb{Z}_P^*$, define $\mathcal{J}_P(x)$, the Jacobi symbol of x modulo P, as

$$\mathcal{J}_P(x) = x^{(P-1)/2} = \begin{cases} +1 & \text{if } x \in \mathbb{QR}_P \\ -1 & \text{if } x \in \mathbb{QNR}_P \end{cases}$$

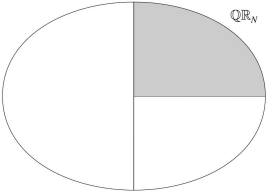
For $x \in \mathbb{Z}_N^*$, where $N = PQ$, define $\mathcal{J}_N(x)$, the Jacobi symbol of x modulo N, as

$$\mathcal{J}_N(x) = \mathcal{J}_P(x)\mathcal{J}_Q(x)$$

For an integer N, consider subsets of $\mathbb{Z}_N^*$:

let $\mathbb{QR}_N = \{x^2 \bmod N \mid x \in \mathbb{Z}_N^*\}$ be the set of quadratic residues modulo N,
let $\mathbb{QNR}_N = \mathbb{Z}_N^* \setminus \mathbb{QR}_N$,
let $\mathbb{Z}_N^*(+1) = \{x \mid \mathcal{J}_N(x) = 1, x \in \mathbb{Z}_N^*\}$,
let $\mathbb{Z}_N^*(-1) = \{x \mid \mathcal{J}_N(x) = -1, x \in \mathbb{Z}_N^*\}$.

Then $\mathbb{Z}_N^* = \mathbb{QR}_N \dot\cup \mathbb{QNR}_N = \mathbb{Z}_N^*(+1) \dot\cup \mathbb{Z}_N^*(-1)$, $\mathbb{QR}_N \subseteq \mathbb{Z}_N^*(+1)$, $\mathbb{Z}_N^*(-1) \subseteq \mathbb{QNR}_N$.



If $\underline{N = P \cdot Q \text{ for distinct odd primes } P, Q}$, then $\frac{|\mathbb{Z}_N^*(+1)|}{|\mathbb{Z}_N^*|} = \frac{|\mathbb{QR}_N|}{|\mathbb{Z}_N^*(+1)|} = \frac{1}{2}$.

The Factoring Assumption: for $\forall$ PPTA $\mathcal{D}$, given N, it is hard to reconstruct P, Q.

The Quadratic Residuosity (QR) Assumption: for $\forall$ PPTA $\mathcal{D}$, $z \xleftarrow{\$} \mathbb{Z}_N^*(+1)$, given (N, z), it is hard to decide whether $z \in \mathbb{QR}_N$ or $z \in \mathbb{QNR}_N$.

The Goldwasser-Micali Scheme

1. Key Generation: $(pk, sk) \leftarrow \mathsf{Gen}(1^k)$.
   Pick an integer $N = P \cdot Q$ randomly. Pick $z \leftarrow \mathbb{QNR}_N \cap \mathbb{Z}_N^*(+1)$.
   It outputs $pk = (N, z)$, $sk = (P, Q)$.
2. Encryption: $c \leftarrow \mathsf{Enc}(pk, m)$.
   To encrypt $m \in \{0, 1\}$, Choose $x \leftarrow \mathbb{Z}_N^*$ and compute
   $$c = z^m \cdot x^2 \mod N.$$
3. Decryption: $m \leftarrow \mathsf{Dec}(sk, c)$.
   To decrypt a ciphertext $c \in \mathbb{Z}_N$, compute
   $$\mathcal{J}_P(x),\ \mathcal{J}_Q(x).$$
   If both of $\mathcal{J}_P(x)$ and $\mathcal{J}_Q(x)$ are 1, output 1, otherwise output 0.

Security Proof of The Goldwasser-Micali Scheme

Let $\mathcal{D}$ be a distinguisher, which is given (N, z) (with $z \in \mathbb{Z}_N^*(+1)$) and going to tell $z \in \mathbb{QR}_N$ or $z \in \mathbb{QNR}_N \cap \mathbb{Z}_N^*(+1)$.

1. $\mathcal{D}$ gives (N, z) to $\mathcal{A}$ as the public key.
2. $\mathcal{D}$ chooses $m \leftarrow \{0, 1\}$ and computes $c = z^m \cdot x^2 \mod N$. Then it sends c to $\mathcal{A}$.
3. $\mathcal{A}$ guesses b'. If $b = b'$, $\mathcal{A}$ wins.
4. If $b = b'$, $\mathcal{D}$ recognizes $z \in \mathbb{QNR}_N$, otherwise $z \in \mathbb{QR}_N$.

- If $z \in \mathbb{QNR}_N$, this is exactly IND-CPA game.

$$\Pr[\mathcal{A}\ wins] = 1/2 + \epsilon.$$

- If $z \in \mathbb{QR}_N$,

$$\Pr[\mathcal{A}\ wins] = 1/2.$$

- $\mathcal{D}$ succeeds with $1/2 + \epsilon/2$.

Security Proof of The Goldwasser-Micali Scheme

Let $\mathcal{D}$ be a distinguisher, which is given (N, z) (with $z \in \mathbb{Z}_N^*(+1)$) and going to tell $z \in \mathbb{QR}_N$ or $z \in \mathbb{QNR}_N \cap \mathbb{Z}_N^*(+1)$.

1. $\mathcal{D}$ gives (N, z) to $\mathcal{A}$ as the public key.
2. $\mathcal{D}$ chooses $m \leftarrow \{0, 1\}$ and computes $c = z^m \cdot x^2 \mod N$. Then it sends c to $\mathcal{A}$.
3. $\mathcal{A}$ guesses b'. If $b = b'$, $\mathcal{A}$ wins.
4. If $b = b'$, $\mathcal{D}$ recognizes $z \in \mathbb{QNR}_N$, otherwise $z \in \mathbb{QR}_N$.

- If $z \in \mathbb{QNR}_N$, this is exactly IND-CPA game.

$$\texttt{Pr}[\mathcal{A}\ wins] = 1/2 + \epsilon.$$

- If $z \in \mathbb{QR}_N$,

$$\texttt{Pr}[\mathcal{A}\ wins] = 1/2.$$

- $\mathcal{D}$ succeeds with $1/2 + \epsilon/2$.

作业

1. Find a splitting field for $f(x) = x^2 + 1$ over Z_3 and the corresponding extension degree.
2. Construct a finite field with 64 elements.(hint: find a splitting field over Z_p.)