

0.1. Prerequisites

- $I \subset R$ is an ideal if $\forall (a, b) \in \mathbb{R}^2, ab \in I \implies a \in I \vee b \in I$.
- I is maximal if $I \neq R$ and there is no ideal $J \subset R$ such that $I \subset J$.
- $p \in \mathbb{Z}$ is prime iff $\langle p \rangle = \langle p \rangle_{\mathbb{Z}}$ is a prime ideal.
- For commutative ring R :
 - $I \subset R$ is prime ideal iff R/I is an integral domain.
 - I is maximal iff R/I is a field.
- Let R be PID and $a \in R$ irreducible. Then $\langle a \rangle = \langle a \rangle_R$ is maximal.
- **Theorem:** let F be field, $f(x) \in F[x]$ irreducible. Then $F[x]/\langle f(x) \rangle$ is a field and a vector space over F with basis $B = \{1, \bar{x}, \dots, \bar{x}^{n-1}\}$ where $n = \deg(f)$. That is, every element in $F[x]/\langle f(x) \rangle$ can be uniquely written as a linear combination

$$a_0 + a_1 \bar{x} + \dots + a_{n-1} \bar{x}^{n-1}$$

1. Divisibility in rings

1.1. Every ED is a PID

- **Definition:** let R integral domain. $\varphi : R - \{0\} \rightarrow \mathbb{N}_0$ is **Euclidean function (norm)** on R if:
 - $\forall x, y \in R - \{0\}, \varphi(x) \leq \varphi(xy)$.
 - $\forall x \in R, y \in R - \{0\}, \exists q, r \in R : x = qy + r$ with either $r = 0$ or $\varphi(r) < \varphi(y)$.
- R is **Euclidean domain (ED)** if a Euclidean function is defined on it.
- Examples of EDs:
 - \mathbb{Z} with $\varphi(n) = |n|$.
 - $F[x]$ for field F with $\varphi(f) = \deg(f)$.
- **Lemma:** $\mathbb{Z}[\sqrt{-2}]$ is an ED with Euclidean function with

$$\varphi(a + b\sqrt{-2}) = N(a + b\sqrt{-2}) =: a^2 + 2b^2.$$

- **Proposition:** every ED is a PID.

1.2. Every PID is a UFD

- **Definition:** Integral domain R is **unique factorisation domain (UFD)** if every non-zero non-unit in R can be written uniquely (up to order of factors and multiplication by units) as product of irreducible elements in R .
- **Example:** let $R = \{f(x) \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$. Its units are ± 1 . Any factorisation of $x \in R$ must be of the form $f(x)g(x)$ where $\deg f = 1, \deg g = 0$, so $x = (ax + b)c$, $a \in \mathbb{Q}, b, c \in \mathbb{Z}$. We have $bc = 0$ and $ac = 1$ hence $x = \frac{x}{c} \cdot c$. So x irreducible if $c \neq \pm 1$. Also, any factorisation of $\frac{x}{c}$ in R is of the form $\frac{x}{c} = \frac{x}{cd} \cdot d$, $d \in \mathbb{Z}, d \neq 0$. Again, neither factor is a unit when $d \neq \pm 1$. So $x = \frac{x}{c} \cdot c = \frac{x}{cd} \cdot c \cdot c = \dots$ can never be decomposed into irreducibles (the first factor is never irreducible).
- **Lemma:** let R be PID. Then every irreducible element is prime in R .
- **Theorem:** every PID is a UFD.
- **Example:** $\mathbb{Z}[\sqrt{-2}]$ so by the above theorem it is a UFD. Let $x, y \in \mathbb{Z}$ such that $y^2 + 2 = x^3$.

- y must be odd, since if $y = 2a, a \in \mathbb{Z}$ then $x = 2b, b \in \mathbb{Z}$ but then $2a^2 + 1 = 4b^3$.
- $y \pm \sqrt{-2}$ are relatively prime: if $a + b\sqrt{-2}$ divides both, then it divides their difference $2\sqrt{-2}$, so $\text{norm } a^2 + 2b^2 \mid N(2\sqrt{-2}) = 8$. Only possible case is $a = \pm 1, b = 0$ so $a + b\sqrt{-2}$ is unit. Other cases $a = 0, b = \pm 1, a = \pm 2, b = 0$ and $a = 0, b = \pm 2$ are impossible since y not even.
- If $a + b\sqrt{-2}$ is unit, $\exists x, y \in \mathbb{Z} : (a + b\sqrt{-2})(x + y\sqrt{-2}) = 1$. If $b \neq 0$ then $(-a^2 - 2b^2)y = 1 \implies b = 0$: contradiction. If $b = 0, a = \pm 1$.

2. Finite field extensions

- **Definition:** let F, L fields. If $F \subseteq L$ and F and L share the same operations then F is a **subfield** of L and L is **field extension** of F (denoted L/F), and L is vector space over F with
 - $0 \in L$ (zero vector).
 - $u, v \in L \implies u + v \in L$ (additivity).
 - $a \in F, u \in L \implies au \in L$ (scalar multiplication).
- **Definition:** let L/F field extension. **Degree** of L over F is dimension of L as vector space over F :

$$[L : F] := \dim_F(L)$$

If $[L : F]$ finite, L/F is **finite field extension**.

- **Example:** $\mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} : a, b \in \mathbb{Q}\}$ is isomorphic as a vector space to \mathbb{Q}^2 so is 2-dimensional vector space over \mathbb{Q} . Isomorphism is $a + b\sqrt{-2} \leftrightarrow (a, b)$. Standard basis $\{e_1, e_2\}$ in \mathbb{Q}^2 corresponds to the basis $\{1, \sqrt{-2}\}$ in $\mathbb{Q}(\sqrt{-2})$. $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$.
- **Example:** $[\mathbb{C} : \mathbb{R}] = 2$ (a basis is $\{1, i\}$). $[\mathbb{R} : \mathbb{Q}]$ is not finite, due to the existence of transcendental numbers (if α transcendental, then $\{1, \alpha, \alpha^2, \dots\}$ is linearly independent).
- **Definition:** let L/F field extension. $\alpha \in L$ is **algebraic** over F if

$$\exists f(x) \in F[x] : f(\alpha) = 0$$

If all elements in L are algebraic, then L/F is **algebraic field extension**.

- **Example:** $i \in \mathbb{C}$ is algebraic over \mathbb{R} since i is root of $x^2 + 1$. \mathbb{C}/\mathbb{R} is algebraic since $z = a + bi$ is root of $(x - z)(x - \bar{z})$.
- **Proposition:** if L/F is finite field extension then it is algebraic.
- **Definition:** let L/F field extension, $\alpha \in L$ algebraic. **Minimal polynomial** $p_\alpha(x) = p_{\alpha, F}(x)$ of α over F is the monic polynomial f of smallest degree such that $f(\alpha) = 0$.
- **Proposition:** $p_\alpha(x)$ is unique and irreducible. Also, if $f(x) \in F[x]$ is monic, irreducible and $f(\alpha) = 0$, then $f = p_\alpha$.
- **Example:**
 - $p_{i, \mathbb{R}}(x) = p_{i, \mathbb{Q}}(x) = x^2 + 1, p_{i, \mathbb{Q}(i)}(x) = x - i$.
 - Let $\alpha = \sqrt[7]{5}$. $f(x) = x^7 - 5$ is minimal polynomial of α over \mathbb{Q} , as it is irreducible by Eisenstein's criterion with $p = 5$ and the above proposition.

- Let $\alpha = e^{2\pi i/p}$, p prime. α is algebraic as root of $x^p - 1$ which isn't irreducible as $x^p - 1 = (x - 1)\Phi(x)$ where $\Phi(x) = (x^{p-1} + \dots + 1)$. $\Phi(\alpha) = 0$ since $\alpha \neq 1$, $\Phi(x)$ is monic and $\Phi(x + 1) = ((x + 1)^p - 1)/x$ irreducible by Eisenstein's criterion with $p = p$, hence $\Phi(x)$ irreducible. So $p_\alpha(x) = \Phi(x)$.

2.1. Fields generated by elements

- **Definition:** let L/F field extension, $\alpha \in L$. The **field generated by α over F** is the smallest subfield of L containing F and α :

$$F(\alpha) = \bigcap_{\substack{K \text{ field,} \\ F \subseteq K \subseteq L, \\ \alpha \in K}} K$$

Generally, $F(\alpha_1, \dots, \alpha_n)$ is smallest field extension of F containing $\alpha_1, \dots, \alpha_n$

- We have $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1) \dots (\alpha_n)$ (show $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$ and $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$ by minimality and use induction).
- **Definition:** $F[\alpha] = \{\sum_{i=0}^n a_i \alpha^i : a_i \in F, n \in \mathbb{N}\} = \{f(\alpha) : f(x) \in F[x]\}$.
- **Lemma:** let L/F field extension, $\alpha \in L$ algebraic over F . Then $F[\alpha]$ is field, hence $F(\alpha) = F[\alpha]$.
- **Lemma:** let α algebraic over F . Then $[F(\alpha) : F] = \deg(p_\alpha)$.
- **Definition:** let K/F and L/K field extensions, then $F \subseteq K \subseteq L$ are **tower of fields**.
- **Tower theorem:** let $F \subseteq K \subseteq L$ tower of fields. Then

$$[L : F] = [L : K] \cdot [K : F]$$

- **Example:** let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Show $[L : \mathbb{Q}] = 4$.
 - Let $K = \mathbb{Q}(\sqrt{2})$. Let $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ so $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. So $0 \in \{a, b\}$, otherwise $\sqrt{2} \in \mathbb{Q}$. But if $a = 0$, then $\sqrt{6} = 2b \in \mathbb{Q}$, if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$: contradiction. So $x^2 - 3$ has no roots in K so is irreducible over K so $p_{\sqrt{3}, K}(x) = x^2 - 3$.
 - So $[L : K] = 2$ so by the tower theorem, $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 4$.

2.2. Norm and trace

- Let L/F finite field extension, $n = [L : F]$. For any $\alpha \in L$, there is F -linear map

$$\hat{\alpha} : L \rightarrow L, \quad x \rightarrow \alpha x$$

- With basis $\{\alpha_1, \dots, \alpha_n\}$ of L over F , then let $T_\alpha = T_{\alpha, L/F} \in M_n(F)$ be the corresponding matrix of the linear map α with respect to the basis $\{\alpha_i\}$:

$$\begin{aligned} \hat{\alpha}(\alpha_1) &= \alpha\alpha_1 = a_{1,1}\alpha_1 + \dots + a_{1,n}\alpha_n, \\ &\vdots \\ \hat{\alpha}(\alpha_n) &= \alpha\alpha_n = a_{n,1}\alpha_1 + \dots + a_{n,n}\alpha_n \end{aligned}$$

with $a_{i,j} \in F$, $T_\alpha = (a_{i,j})$, i.e.

$$\alpha \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = T_\alpha \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

- **Definition: norm** of α is

$$N_{L/F}(\alpha) := \det(T_\alpha)$$

- **Definition: trace** of α is

$$\text{tr}_{L/F}(\alpha) := \text{tr}(T_\alpha)$$

- **Remark:** norm and trace are independent of choice of basis so are well-defined (uniquely determined by α).
- **Example:** let $L = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ non-square, let $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$. Fix basis $\{1, \sqrt{m}\}$. Now

$$\begin{aligned} \hat{\alpha}(1) &= \alpha \cdot 1 = a + b\sqrt{m}, \\ \hat{\alpha}(\sqrt{m}) &= \alpha\sqrt{m} = bm + a\sqrt{m}, \\ T_\alpha &= \begin{bmatrix} a & b \\ bm & a \end{bmatrix} \end{aligned}$$

So $N_{L/F}(\alpha) = a^2 - b^2m$, $\text{tr}_{L/F}(\alpha) = 2a$.

- **Lemma:** the map $L \rightarrow M_{n(F)}$ given by $\alpha \rightarrow T_\alpha$ is injective ring homomorphism. So if $f(x) \in F[x]$, $T_{f(\alpha)} = f(T_\alpha)$ ($f(T_\alpha)$ is a polynomial in T_α , not f applied to each entry).
- **Proposition:** let L/F finite field extension. $\forall \alpha, \beta \in L$,
 - $N_{L/F}(\alpha) = 0 \iff \alpha = 0$.
 - $N_{L/F}(\alpha\beta) = N_{L/F}(\alpha)N_{L/F}(\beta)$.
 - $\forall a \in F$, $N_{L/F}(a) = a^{[L:F]}$ and $\text{tr}_{L/F}(a) = [L:F]\alpha$.
 - $\forall a, b \in F$, $\text{tr}_{L/F}(a\alpha + b\beta) = a \text{tr}_{L/F}(\alpha) + b \text{tr}_{L/F}(\beta)$ (hence $\text{tr}_{L/F}$ is F -linear map).

2.3. Characteristic polynomials

- Let $A \in M_n(F)$, then characteristic polynomial is $\chi_A(x) = \det(xI - A) \in F[x]$ and is monic, $\deg(\chi_A) = n$. If $\chi_A(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ then $\det(A) = (-1)^n \det(0 - A) = (-1)^n \chi_A(0) = (-1)^n c_0$ and $\text{tr}(A) = -c_{n-1}$, since if $\alpha_1, \dots, \alpha_n$ are eigenvalues of A (in some field extension of F), then $\text{tr}(A) = \alpha_1 + \dots + \alpha_n$, $\chi_A(x) = (x - \alpha_1) \cdots (x - \alpha_n) = x^n - (\alpha_1 + \dots + \alpha_n)x^{n-1} + \dots$.
- For finite field extension L/F , $n = [L:F]$, $\alpha \in L$, **characteristic polynomial** $\chi_\alpha(x) = \chi_{\alpha, L/F}(x)$ is characteristic polynomial of T_α . So $N_{L/F}(\alpha) = (-1)^n c_0$, $\text{tr}_{L/F}(\alpha) = -c_{n-1}$. By the Cayley-Hamilton theorem, $\chi_\alpha(T_\alpha) = 0$ so $T_{\chi_\alpha(\alpha)} = \chi_\alpha(T_\alpha) = 0$. Since $\alpha \rightarrow T_\alpha$ is injective, $\chi_\alpha(\alpha) = 0$.
- **Lemma:** let L/F finite field extension, $\alpha \in L$ with $L = F(\alpha)$. Then $\chi_\alpha(x) = p_\alpha(x)$.
- **Proposition:** consider tower $F \subseteq F(\alpha) \subseteq L$, let $m = [L:F(\alpha)]$. Then $\chi_\alpha(x) = p_\alpha(x)^m$.

- **Corollary:** let L/F , $\alpha \in L$ as above, $p_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, $a_i \in F$.
Then

$$N_{L/F}(\alpha) = (-1)^n a_0^m, \quad \text{tr}_{L/F}(\alpha) = -ma_{d-1}$$