underGraduate Homework In Mathematics

AlgebraicGeometry 3

白永乐

202011150087

202011150087@mail.bnu.edu.cn

2023 年 10 月 11 日

General fire extinguisher

PROBLEM I Let R be a Abel ring, $\mathfrak{a}$ is an ideal of R, and $\sqrt{\mathfrak{a}} := \{x \in R : \exists n \in \mathbb{N}, x^n \in \mathfrak{a}\}$. Prove that:

1. $\sqrt{\mathfrak{a}}$ is ideal.
2. $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.
3. $\sqrt{\mathfrak{a}}$ is the smallest radical ideal contain $\mathfrak{a}$.
4. If $\mathfrak{p}$ is prime ideal, then $\mathfrak{p}$ is radical.
5. $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}$, where $\mathcal{P}$ is the set of all prime ideal contains $\mathfrak{a}$.

SOLUTION .

1. $\forall a, b \in \sqrt{\mathfrak{a}}, \exists m, n \in \mathbb{N}, a^m, b^n \in \mathfrak{a}$. Consider $a-b$, we have $(a-b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}$. Since $k + m + n - k = m + n$, so $k \geq m$ or $m + n - k \geq n$. So $(a - b)^{m+n} \in \mathfrak{a}$ and thus $a - b \in \sqrt{\mathfrak{a}}$.

   $\forall a \in \sqrt{\mathfrak{a}}, b \in R, (ab)^n = a^n b^n$. So $ab \in \sqrt{\mathfrak{a}}$.
2. Obviously $\sqrt{\mathfrak{a}} \subset \sqrt{\sqrt{\mathfrak{a}}}$, so only need to prove $\sqrt{\sqrt{\mathfrak{a}}} \subset \sqrt{\mathfrak{a}}$. Consider $a \in \sqrt{\sqrt{\mathfrak{a}}}, \exists n \in \mathbb{N}, a^n \in \sqrt{\mathfrak{a}}, \exists m \in \mathbb{N}, (a^n)^m \in \mathfrak{a}$. Thus $a^{mn} \in \mathfrak{a}$, so $a \in \sqrt{\mathfrak{a}}$. So $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$.
3. Let $\mathfrak{b}$ is a radical ideal contains $\mathfrak{a}$, then $\forall a \in \sqrt{\mathfrak{a}}, \exists n \in \mathbb{N}, a^n \in \mathfrak{a} \subset \mathfrak{b}$. Since $\mathfrak{b}$ is radical, we get $a \in \mathfrak{b}$. So $\sqrt{\mathfrak{a}} \subset \mathfrak{b}$. Noting we have proved $\sqrt{\mathfrak{a}}$ is radical in I.2, so it's the smallest.
4. $\forall a \in \sqrt{\mathfrak{p}}, \exists n \in \mathbb{N}, a^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, so $a \in \mathfrak{p}$.
5. From I.3 and I.4 we get $\sqrt{\mathfrak{a}} \subset \mathfrak{p}$, so we only need to prove $\bigcap_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p} \subset \sqrt{\mathfrak{a}}$. If not, then $\exists a \notin \sqrt{\mathfrak{a}}, \forall \mathfrak{p} \in \mathcal{P}, a \in \mathfrak{p}$. Let $\mathcal{I}$ is the set of all ideal contains $\mathfrak{a}$ and not contains any of $a^n, n \in \mathbb{N}$. Since $(\mathcal{I}, \subset)$ is partial order, and obviously every chain has upper bound(use union), and $\mathcal{I} \neq \emptyset (\mathfrak{a} \in \mathcal{I})$. So there is a maximal element in $\mathcal{I}$(by Zorn's lemma). Assume $\mathfrak{q} \in \mathcal{I}$ is maximal element, we will prove $\mathfrak{q}$ is prime ideal. If not, then $\exists x, y \notin \mathfrak{q}, xy \in \mathfrak{q}$. Since $\mathfrak{q}$ is maximal, then $(\mathfrak{q}, x), (\mathfrak{q}, y)$ contians some a^n. Assume $a^n = q_1 + xt_1, a^m = q_2 + yt_2, q_1, q_2 \in \mathfrak{q}, t_1, t_2 \in R$. Then $a^{m+n} = q_1(q_2 + yt_2) + q_2 xt_1 + xyt_1t_2 \in \mathfrak{q}$, contradiction with the definition of $\mathcal{I}$! So $\mathfrak{q} \in \mathcal{P}$. But $a \notin \mathfrak{q}$, contradiction with the assumption that $a \in \mathfrak{p} \forall \mathfrak{p} \in \mathcal{P}$! So $\bigcap_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p} \subset \sqrt{\mathfrak{a}}$.

$\square$

PROBLEM II An algebraically field is not finite field.

SOLUTION . Assume F is a finite, consider $f(x) = \prod_{a\in F}(x - a) + 1 \in F[x]$, easily prove $f(x)$ has no root in F. $\square$

PROBLEM III Let $A = K[x_1, x_2, \cdots x_n]$, and $m_p = (x_1 - a_1, \cdots x_n - a_n), p = (a_1, a_2, \cdots a_n) \in \mathbb{A}_K^n$. Then m is max ideal.

Lemma 1. If $f(x_1, x_2, \cdots x_n) \in K[x_1, x_2, \cdots x_n], f(a_1, a_2, \cdots a_n) = 0$, then $f = \sum_{k=1}^{n}(x_k - a_k) f_k(x_1, x_2, \cdots x_n)$.

证明. Use MI to n. When $n=1$ it's obvious. If for some certain n it's right, when goes to $n+1$: Let $g(x_1,x_2,\cdots x_n) := f(x_1,x_2,\cdots x_n,a_{n+1}) \in K[x_1,x_2,\cdots x_n]$. Then $g(a_1,a_2,\cdots a_n)=0$, so $g(x_1,x_2,\cdots x_n) = \sum_{k=1}^{n}(x_k-a_k)g_i(x_1,x_2,\cdots x_n)$. Let $h(x_{n+1}) := f(x_1,x_2,\cdots x_{n+1}) - g(x_1,x_2,\cdots x_n) \in K[x_1,x_2,\cdots x_n][x_{n+1}]$, then $h(a_{n+1})=0$. So $h(x_{n+1}) = (x_{n+1}-a_{n+1})h_1(x_{n+1})$ for some $h_1(x_{n+1}) \in K[x_1,x_2,\cdots x_n][x_{n+1}]$. Then $f(x_1,x_2,\cdots x_{n+1}) = \sum_{k=1}^{n+1}(x_i-a_i)f_i(x_1,x_2,\cdots x_{n+1})$, where $f_k(x_1,x_2,\cdots x_{n+1}) = g_k(x_1,x_2,\cdots x_n), k=1,2,\cdots n$, and $f_{n+1}(x_1,x_2,\cdots x_{n+1}) = h_1(x_{n+1})$. □

SOLUTION. Obviously m_p is ideal, so we only need to prove it's max. Consider $\phi : K[x_1,x_2,\cdots x_n] \to K, f(x_1,x_2,\cdots x_n) \mapsto f(a_1,a_2,\cdots a_n)$. Obviously it's a homomorphism, consider $\ker\phi$. Obviously $m_p \subset \ker\phi$, now we prove $\ker\phi \subset m_p$. Assume $f \in \ker\phi$, then $f(a_1,a_2,\cdots a_n)=0$. Use Lemma 1 we get $f \in \ker\phi$. So $m_p = \ker\phi$. So $R/m_p \cong K$ is a field, thus m_p is max ideal. □

PROBLEM IV $A \subset B \subset C$ are Abel rings. If B is f.g. $A-$module and C is f.g. $B-$module, then C is f.g. $A-$module, too.

SOLUTION. Let $\{b_i : i=1,2,\cdots n\}$ is a basis of B over A, and $\{c_i : i=1,2,\cdots m\}$ is a basis of C over B. Then for $c \in C, \exists x_i \in B$ such that $c=\sum_{i=1}^{m} x_ic_i$. And $\exists y_{ij} \in A$ such that $x_i = \sum_{j=1}^{n} y_{ij}b_j$. So $c = \sum_{i=1}^{m}\sum_{j=1}^{n} y_{ij}b_jc_i$. That means $\{b_jc_i : j=1,2,\cdots n, i=1,2,\cdots m\}$ is a basis of C over A. □

PROBLEM V If x is integral over A then $A[x]$ is f.g. $A-$module.

SOLUTION. Assume $x^n + \sum_{k=0}^{n-1} -a_kx^k = 0, a_k \in A$. Then we prove $\{x^k : k=0,1,\cdots n-1\}$ is a basis of $A[x]$. Only need to prove $x^m, m \in \mathbb{N}$ can be reperesented. Use MI to m. When $m \leq n-1$ it's obvious. Assume for certain $m \geq n, \forall k < m, x^k$ can be reperesented, then for m, we have $x^m = x^{m-n}x^n = x^{m-n}\sum_{t=0}^{n-1} a_tx^t = \sum_{t=0}^{n-1} a_tx^{t+m-n}$. Since $t+m-n \leq n-1+m-n = m-1 < m$, we get x^k can be reperesented, so $\sum_{t=0}^{n-1} a_tx^{t+m-n}$ can be reperesented. i.e., x^m can be reperesented. So $\{x^k : k=0,1,\cdots n-1\}$ is basis. □

PROBLEM VI Let R be an integral domain, finitely generated over a field k. If R has transcendence degree n over k, then there exist elements $x_1,\ldots,x_n \in R$, algebraically independent over k, such that R is integrally dependent on the subring $k[x_1,\ldots,x_n]$ generated by the x 's.

SOLUTION. Since R is f.g. over k, we can assume $R := k[x_1,\cdots x_m]/I$. We use induction on m. If $m=0$, there is nothing to do. If $I=(0)$, then we can set $c_i = x_i + I$ for $i=1,\cdots,m$, and again there is nothing to show. If $I \neq (0)$, then choose $f \in I \setminus \{0\}$. If $f \in k$ then $I = k[x_1,\cdots,x_m]$. Then $R=\{0\}$. Else, $\deg f > 0$. Write f as

$$f = \sum_{i=(i_1,i_2,\cdots i_m)\in S} \alpha_i \prod_{t=1}^{m} x_t^{i_t} \tag{1}$$

Where $\emptyset \neq S \subset \mathbb{N}^m$ is a finite set and $\alpha_i \in k^*$. Choose d greater than all x_i-degrees of f, then the function $\phi : S \to \mathbb{N}, i \mapsto \sum_{j=1}^{m} i_jd^{j-1}$ is injective. For $i=2,\cdots,m$, let $y_i = x_i - x_1^{d^{i-1}}$, then:

$$f = f\left(x_1, y_2 + x_1^d, \cdots y_m + x_1^{d^{m-1}}\right) = \sum_{i\in S} \alpha_i \left(x_1^{\phi(i)} + g_i(x_1,y_2,\cdots,y_m)\right) \tag{2}$$

where g_i's are polynomials satisfying $\deg_{x_1} g_i < \phi(i)$. Since ϕ is injective, we have exactly one $i \in S$ such that $\phi(i)$ is maximum, assume the maximum value is $u = \phi(i)$. Since f is not constant, $u > 0$. Thus we obtain:

$$f = \alpha_i x_1^u + h(x_1, y_2, \cdots, y_m) \tag{3}$$

with $\deg_{x_1} h < u$. Therefore

$$x_1^u + \alpha_i^{-1} h(x_1, y_2, \cdots, y_m) \in I \tag{4}$$

Let $B := k[y_2 + I, \cdots y_m + I] \subset R$, then $R = B[x_1 + I]$, and above equation shows R is integral over B. By induction, there exists algebraically independent $c_1, \cdots, c_n \in B$ such that B is integral over $k[c_1, \cdots, c_n]$. Thus R is integral over $k[c_1, \cdots c_n]$, too. $\square$