SOLUTIONS TO ALGEBRA2-H

BOWEN LIU

Abstract. This note contain solutions to homework of Algebra2-H (2024Spring), but we will omit proofs which are already shown in the textbook or quite trivial.

Contents

1. Homework-1

1.1. **Solutions to 4.1.**

1. It suffices to note that $(u+1)^{-1} = (u^2-u+1)/3$.
2. Note that $u^8+1=0$, and by Eisenstein criterion it's easy to show that x^8+1 is irreducible.
4. It suffices to note that $[F(u):F(u^2)] \leq 2$.
5. Omit.
6. Omit.
7. Pick any $0 \neq v \in K \setminus F$, then by the explicit construction of $F(u)$, we may write

$$v = \frac{f(u)}{g(u)},$$

where $f, g \in F[x]$ with $g \neq 0$. In other words, one has $f(u) - vg(u) = 0$. On the other hand, $f(x) - vg(x) \not\equiv 0$, otherwise it leads to $v \in F$, since coefficients of f, g lie in F. This shows u satisfies a non-trivial polynomial with coefficients in K, and thus it's algebraic over K.
8. Omit.
9. If β is algebraic over F, then by exercise 7 one has $[F(\alpha):F(\beta)] < \infty$, and thus

$$[F(\alpha):F] = [F(\alpha):F(\beta)][F(\beta):F] < \infty,$$

a contradiction.
10 Since α is algebraic over $F(\beta)$, then there exists a non-trivial polynomial

$$P(x) = x^n + a_{n-1}(\beta)x^{n-1} + \cdots + a_0(\beta) \in F(\beta)[x]$$

such that $P(\alpha) = 0$. On the other hand, it's clear that β is transcendent over F, otherwise

$$[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\beta)][F(\beta):F] < \infty,$$

a contradiction to α is transcendent over F. Thus by the explicit construction of $F(\beta)$, we may write

$$a_i(\beta) = \frac{f_i(\beta)}{g_i(\beta)},$$

where $f_i(x)$ and $g_i(x) \in F[x]$, while $g_i(x) \neq 0$. Now consider the polynomial

$$Q(x,y) = P(x)\prod_{i=1}^{n} g_i(y) \in F[x,y].$$

It's a polynomial satisfying $Q(\alpha,\beta) = 0$, which implies β is algebraic over $F(\alpha)$.

1.2. **Solutions to 4.2.**

2. It's clear $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. On the other hand, note that

$$\sqrt{3}-\sqrt{2} = (\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

This shows $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, and thus $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Remark 1.2.1. In fact, any finite seperable extension is a simple extension, that is, a field extension generated by one element. This is called primitive element theorem.

3. Suppose there exists $a \in E$ such that $g(a) = 0$. Since g is irreducible over F, so it's the minimal polynomial of a over F. Thus

$$[F(a):F] = \deg g = k.$$

On the other hand, $[E:F] = [E:F(a)][F(a):F]$, a contradiction to $k \nmid [E:F]$.

5 Suppose K be a subring of E containing F. For any $0 \neq u \in K$, since E is algebraic over F, there exists a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ such that $f(u) = 0$. Thus

$$u^{-1} = -\frac{1}{a_0}(u^{n-1} + a_{n-1}u^{n-2} + \cdots + a_1) \in K.$$

6. Omit.

7. It's clear $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, since it's algebraic over $\mathbb{R}$, and it's algebraically closed.

(a) An algebraically closed field must contain infinitely many elements, otherwise if an algebraically closed E is a finite field with $|E| = q$, then $x^q - x + 1$ has no roots in E.

(b) An example is $[\mathbb{C}:\mathbb{R}] = 2$.

8. Firstly we prove that if $p_1,\dots,p_n$ and p are distinct prime numbers, then $\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ by induction. For $n = 1$, if $\sqrt{p} \in \mathbb{Q}(\sqrt{p_1})$, then there exists $a, b \in \mathbb{Q}$ such that

$$\sqrt{p} = a + \sqrt{p_1},$$

and thus $a^2 + b^2 p_1 + 2ab\sqrt{p_1} = p$. Since $\sqrt{p_1} \notin \mathbb{Q}$, it leads to $ab = 0$. Both $a = 0$ and $b = 0$ will lead to contradictions. Now suppose the statement holds for $n = k-1$ and consider the case $n = k$. By induction hypothsis, one has

$$\sqrt{p}, \sqrt{p_k} \notin \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{k-1}}).$$

If $\sqrt{p} \in \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_k})$, then

$$\sqrt{p} = c + d\sqrt{p_k},$$

where $c, d \in \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{k-1}})$. By the same argument one has $cd = 0$, but $c \neq 0$, otherwise it contradicts to $\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{k-1}})$. This shows $\sqrt{p} = d\sqrt{p_k}$. Repeat above process for $d \in \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{k-1}})$, one has

$$d = d_1\sqrt{p_{k-1}},$$

and thus

$$\sqrt{p} = d_{n-1}\sqrt{p_1 \dots p_k},$$

where $d_{n-1} \in \mathbb{Q}$, a contradiction. This shows $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \dots, \sqrt{p}, \dots)/\mathbb{Q}$ is an algebraic extension of infinite degree. Since $\overline{Q}$ is the algebraic closure of $\mathbb{Q}$, and E is algebraic over $\mathbb{Q}$, so $\overline{Q}$ is also the algebraic closure of E.
9. Omit.
10. Omit.

1.3. **Solutions to 4.3.**

1. Omit.
2. It suffices to show that $\sin 18^\circ$ is constructable. Suppose $\theta = 18^\circ$. Then $\sin 2\theta = \sin(\pi/2 - 3\theta) = \cos 3\theta$, and thus

$$2\sin\theta\cos\theta = 4\cos^3\theta - 3\cos\theta.$$

A simple computation yields

$$\cos\theta(4\sin^2\theta + 2\sin\theta - 1) = 0.$$

As a result, one has $\sin\theta = (\sqrt{5}-1)/4$, which is constructable.

2. Homework-2

2.1. **Solutions to 4.4.**

1. Let ξ_3 be the 3-th unit root. Then

$$\begin{aligned} f(x) &= (x-1)(x+1)(x^4+x^2+1) \\ &= (x-1)(x+1)(x-\xi_3)(x+\xi_3)(x-\xi_3^2)(x+\xi_3^2). \end{aligned}$$

This shows the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\xi_3)$.
2. Let ξ_4 be the 4-th unit root. Then

$$f(x) = (x - \sqrt[4]{2}\xi_4)(x + \sqrt[4]{2})(x - \sqrt[4]{2} \times \sqrt{-1}\xi_4)(x + \sqrt[4]{2} \times \xi_4\sqrt{-1}).$$

This shows the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}\xi_4, \sqrt{-1})$.
3. Let ξ_3 be the 3-th unit root. Then

$$f(x) = (x+\sqrt{2})(x-\sqrt{2})(x-\sqrt[3]{3})(x-\sqrt[3]{3}\xi_3)(x-\sqrt[3]{3}\xi_3^2).$$

This shows the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \xi_3)$.
4. The splitting field of x^3-2 over $\mathbb{R}$ is $\mathbb{C}$.
5. Suppose there is a field isomorphism $\varphi\colon \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})$ and $\varphi(\sqrt{2}) = a + b\sqrt{3}$. Then

$$2 = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

On the other hand, $\{1, \sqrt{3}\}$ gives a basis of $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. This shows $2ab = 0$ and $a^2 + 3b^2 = 0$, a contradiction to $a, b \in \mathbb{Q}$.
6. Suppose $E = F(\alpha)$. Then the minimal polynomial of α is of degree two, which can be written as $x^2 + ax + b$ with $a, b \in F$. On the other hand,

$$x^2 + ax + b = (x-\alpha)(x-\alpha-a).$$

This shows E is exactly the splitting field of x^2+ax+b over F.
7. Note that

$$f(x) = (x-\sqrt{-3})(x+\sqrt{-3})(x-1-\sqrt{-3})(x-1+\sqrt{-3}).$$

This shows the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{-3})$. Suppose there is an automorphism σ such that $\sigma(\sqrt{-3}) = 1 + \sqrt{-3})$. Then

$$-3 = \sigma(\sqrt{-3}^2) = \sigma(\sqrt{-3})^2 = (1+\sqrt{-3})^2 = -2 + 2\sqrt{-3},$$

a contradiction.
8. Note that $f(x)$ is irreducible over $\mathbb{Z}_2[x]$, then $\mathbb{Z}_2[x]/(f(x))$ contains a root u of $f(x)$. Furthermore, note that if $f(u) = 0$, then $f(u+1) = 0$, thus $\mathbb{Z}_2[x]/(f(x))$ contains all roots of $f(x)$, that is it's splitting field of f.
9. The same argument shows $\mathbb{Z}_3[x]/(f(x))$ is splitting field of f.
10. It's clear that we must have f is irreducible over $\mathbb{Q}$ and its splitting field is exactly $\mathbb{Q}[x]/(f(x))$, since $[\mathbb{Q}[x]/(f(x)) : \mathbb{Q}] = 3$. This is equivalent to the discriminant $\sqrt{\Delta}$ of $f(x)$ in $\mathbb{Q}$.
11. In fact, we can prove a stronger result, that is $[E : F] \mid n!$. Let's prove by induction on degree of $f(x)$. It's clear for the case $\deg f(x) = 1$. Now assume $\deg f(x) = n+1$. Let's consider the following cases:

(a) If f is reducible, let $p(x)$ be an irreducible factor of $f(x)$ with degree k, and L the splitting field of $p(x)$ over F. Then E is the splitting field of f/p over L. Note that degree of $p(x)$ and $f(x)/p(x)$ are $\leq n$, then by induction hypothsis one has

$$[E:F]=[E:L][L:F]|k!\times(n+1-k)!|(n+1)!$$

(b) Suppose f is irreducible, then consider $L=F[x]/(f)\cong F(\alpha)$, where α is a root of f. It's clear $[L:F]=n+1$. Now consider polynomial $f/(x-\alpha)$ over L, it's clear that E is the splitting field of it. The same argument yields the result.

2.2. **Solutions to 4.5.**

8. Omit.

9. Omit.

10. If F is a perfect field, then it's clear every finite extension E of F is seperable, since any element of E fits a irreducible polynomial, and every irreducible polynomial of F is seperable; Conversely, if $F\neq F^p$, then there exists $u\in F\backslash F^p$, then x^p-u is irreducible, but not seperable over F, a contradiction.

3. Homework-3

3.1. Solutions to 4.6.

1. If α is a root of $f(x) = x^p - x - c$, then

$$\begin{aligned} f(\alpha + k) &= (\alpha + k)^p - (\alpha + k) - c \\ &= \alpha^p + k^p - \alpha - k - c \\ &= 0 \end{aligned}$$

for all $1 \leq k \leq p - 1$. This shows $F(\alpha)$ is the splitting field of $f(x)$.
2. Suppose $[E : F] = 2$. Then E/F is the splitting field of some polynomial over F, and thus it's a normal extension.
3. $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ are normal extensions, but $\mathbb{Q}(6\sqrt[3]{7})/\mathbb{Q}$ is not normal, since the minimal polynomial of $\sqrt[3]{7}$ over $\mathbb{Q}$ is $x^3 - 7$, which has a root $\sqrt[3]{7}\xi_3$ not lying in $\mathbb{Q}(5\sqrt[3]{7})$.
8. Suppose F is a finite field with characteristic p and E/F is a finite extension. Then E is also a finite field with $|E| = p^m$, and thus E is the splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$. In particular, $E/\mathbb{F}_p$ is a normal extension, so is E/F.
10. Suppose the minimal subfield of L which contains $E_1', \ldots, E_n'$ is K, and the normal closure of E/F is N. On one hand, it's clear that $K \subseteq N$, since $\sigma(N) \subseteq N$. On the other hand, for any $\alpha \in E$, suppose its minimal polynomial over F is $f(x)$ and β is another root of $f(x)$. Then $\alpha \mapsto \beta$ may extend to a automorphism of E which fixes F. As a consequence, one has $\beta \in K$, and thus $N \subseteq K$.

4. Homework-4

4.1. **Solutions to 4.7.**

1. Note that $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$, and it's the splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$, so $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is a Galois extension with the Klein four group K_4 as its Galois group. By the Galois correspondence, the subfields of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ are $\mathbb{Q},\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{6})$ and itself.
2. The splitting field of x^4+1 over $\mathbb{Q}$ is $\mathbb{Q}(e^{\sqrt{-1}\pi/4})$, which is also the splitting field of x^8-1. Then the Galois group is isomorphic to the automorphism group of C_8, which is the Klein four group K_4.
3. $\mathbb{Z}/4\mathbb{Z}$.
4. $\mathbb{Z}/5\mathbb{Z}$.
5. Note that over $\mathbb{Z}_3$ one has the following decomposition

$$x^4+2=(x^2+1)(x+1)(x-2),$$

which implies the splitting field of x^4+2 is the same as the one of x^2+1. In other words, the splitting field of x^4+2 over $\mathbb{Z}_3$ is $\mathbb{Z}_3(\sqrt{-1})$, and the Galois group is $\mathbb{Z}_2$.
6. By the assumption on a we know that $f(x)=x^p-x-a$ is irreducible over F, and if α is a root of $f(x)$, then $\{\alpha+k \mid k=0,1\dots,p-1\}$ are all roots of $f(x)$. In particular, the Galois group is $\mathbb{Z}_p$.
7. Omit.

4.2. **Solutions to 4.8.**

1. Since the Frobenius map $x\mapsto x^p$ is injective, then it's also surjective by the finiteness.
2. Note that $E=F[x]/(f(x))$ is a finite field with $|E|=q^n$. In particular, every non-zero element is a root of $x^{q^n-1}-1$, and thus $f(x)\mid x^{q^n-1}-1$.
3. Suppose F is a infinite field such that $F^\times$ is an infinite cyclic group. Let K be the prime subfield of F. Then $K^\times\subseteq F^\times$ is also an infinite cyclic subgroup. This shows $\mathrm{char}K=0$ and thus $K=\mathbb{Q}$, but $\mathbb{Q}^\times$ is not cyclic, a contradiction.
4. Omit.
5. If $\mathrm{char}F=2$, then $F^2=F$, and thus $F\subseteq F^2+F^2$. If $\mathrm{char}F=p>2$ and suppose $F=\{0,a,a^2,\dots,a^{q-1}\}$, where $q=p^n$, then

$$F^2=\{0,a^2,a^4,\dots,a^{q-1}\}.$$

In particular, $|F^2|=(q+1)/2$. For any $c\in F$, similarly one has $|c-F^2|=(q+1)/2$, and thus

$$c-F^2\cap F^2\neq\varnothing.$$

6. Omit.
8. Note that $\mathbb{Q}(\sqrt{2})\ncong\mathbb{Q}(\sqrt{3})$.
9. In exercise 2 we have already shown that every irreducible polynomial of degree p is a divisor of $x^{q^p}-x$. On the other hand, $\mathbb{F}_{q^p}/\mathbb{F}_q$ is the splitting field of $x^{q^p}-x$, and since p is prime, so there is no intermediate field. In

other words, every irreducible polynomial that divides $x^{q^p} - x$ must be of degree p or 1. Since there are q irreducible polynomial of degree 1, so the number of irreducible polynomial of degree p over $\mathbb{F}_q$ is exactly $(q^p - q)/p$.
10. Omit.

5. Homework-5

5.1. **Solutions to 4.9.**

2. We divide into two parts:
(a) It's clear E/K is Galois, with Galois group $\mathrm{Gal}(E/K)$, which is abelian, since any subgroup of abelian group is still abelian. So E/K is an abelian extension;
(b) Note that K/F is Galois if and only if $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$, and it's clear any subgroup of abelian group is normal, thus K/F is Galois. Furthermore it's Galois group is $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$, which implies K/F is abelian extension, since any quotient group of abelian group is still abelian.
3. By the same argument as above.
4. It suffices to show if z is a n-th primitive root of unity, then $-z$ is a $2n$-th primitive root of unit, since cyclotomic polynomial is the product of these roots. Let $z = \cos(2k\pi/n) + \sqrt{-1}\sin(2k\pi/n)$ is n-th primitive root of unity, thus $(k,n) = 1$. Note that

$$
\begin{aligned}
-z &= \cos(\frac{2k\pi}{n} + \pi) + \sqrt{-1}\sin(\frac{2k\pi}{n} + \pi) \\
&= \cos\frac{2(2k+n)\pi}{2n} + \sqrt{-1}\sin\frac{2(2k+n)\pi}{2n}.
\end{aligned}
$$

Since $(k,n) = 1$ and $n > 1$ is odd, we have $(2k+n, 2n) = 1$, and thus $-z$ is a $2n$-th primitive root.
5. Since

$$
x^{p^n} - 1 = \prod_{m|n} \varphi_m(x) = \prod_{0\leq k\leq n} \varphi_{p^k}(x),
$$

we have

$$
\varphi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}.
$$

6. It's isomorphic to $\mathrm{Aut}(\mathbb{Z}_{12})$, which is the Klein four group.
7. Otherwise, suppose $n = pm$. Then $x^n - 1 = (x^m - 1)^p$, which implies the number of different roots of $x^n - 1$ is at most m, a contradiction.
8. If $x^m - a$ is reducible, then it's clear $(x^n)^m - a$ is also reducible. This shows if $x^{mn} - a$ is irreducible, then both $x^n - a$ and $x^m - a$ are irreducible. Conversely, suppose both $x^m - a$ and $x^n - a$ are irreducible, and α is a root of $x^{mn} - a$. Then α^m is a root of $x^n - a$. This shows $[F(\alpha^m) : F] = n$, and similarly we have $[F(\alpha^n) : F] = m$. Since $(m,n) = 1$, we have $[F(\alpha) : F] = mn$, and thus $x^{mn} - a$ is irreducible.
9. If $a \in F^p$, it's clear that $x^p - a$ is reducible. Conversely, suppose $a \notin F^p$ and $f(x)$ is an irreducible factor of $x^p - a$ with degree k, and the constant term of $f(x)$ is c. Let α be a root of $x^p - a$ in the splitting field. Then any root of $x^p - a$ is of the form $\alpha\omega$, where ω is some primitive p-th root. By Vieta's theorem we have $c = \pm\omega^\ell\alpha^k$. Since $(k,p) = 1$, there exist s, t such

that $sk + pt = 1$, and thus

$$\alpha = \alpha^{sk}\alpha^{pt} = \pm(c\omega^{-\ell})^s a^t,$$

which implies $\alpha\omega^{s\ell} = \pm c^s a^t \in F$. Then we have $a = \alpha^p = (\alpha\omega^{s\ell})^p \in F^p$, a contradiction.

10. Omit.

6. Homework-6

6.1. Solutions to 4.9.

1. Prove the Galois groups of these polynomials are all S_5.
2. Consider $-x^7+10x^5-15x+5$, which only has 5 real roots.
3. Consider Cayley's theorem.
4. Omit.
5. Let $F=\mathbb{Q}(t_1,\dots,t_n)$. Then prove $\mathrm{Gal}(E/F(\theta))$ is trivial.

6.2. Solutions to chapter 1 of Atiyah-MacDonald.

Exercise 6.2.1. Let x be a nilpotent element of a ring A. Show that $1+x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. If x is a nilpotent element, then $x\in\mathfrak{N}\subseteq\mathfrak{R}$. By property of Jacobson ideal, we have $1-xy$ is unit for any $y\in A$. Take $y=-1$ we obtain $1+x$ is a unit. If y is unit, then we have $x+y=y^{-1}(y^{-1}x+1)$. Since $y^{-1}x$ is also nilpotent, we have $y^{-1}x+1$ is unit, thus $x+y$ is unit. □

Exercise 6.2.2. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f=a_0+a_1x+\dots+a_nx^n\in A[x]$. Prove that

(1) f is a unit in $A[x]\Leftrightarrow a_0$ is a unit in A and $a_1,\dots,a_n$ are nilpotent.
(2) f is nilpotent $\Leftrightarrow a_0,a_1,\dots,a_n$ are nilpotent.
(3) f is a zero-divisor $\Leftrightarrow$ there exists $a\neq 0$ in A such that $af=0$.
(4) f is said to be primitive if $(a_0,a_1,\dots,a_n)=(1)$. Prove that if $f,g\in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

Proof. For (1). Use $g=\sum_{i=0}^m b_ix^i$ to denote the inverse of f. Since $fg=1$ and if we use c_k to denote $\sum_{m+n=k}a_mb_n$, then we have

$$\begin{cases} c_0=1\\ c_k=0, & k>0\end{cases}$$

But $c_0=a_0b_0$, thus a_0 is unit. Now let's prove $a_n^{r+1}b_{m-r}=0$ by induction on r: $r=0$ is trivial, since $a_nb_m=c_{n+m}=0$. If we have already proven this for $k<r$. Then consider c_{m+n-r}, we have

$$0=c_{m+n-r}=a_nb_{m-r}+a_{n-1}b_{m-r+1}+\dots$$

and multiply a_n^r we obtain

$$0=a_n^{r+1}b_{m-r}+a_{n-1}\underbrace{a_n^rb_{m-r+1}}_{\text{by induction this term is }0}+a_{n-2}a_n\underbrace{a_n^{r-1}b_{m-r+2}}_{\text{by induction this term is }0}+\dots$$

which completes the proof of claim. Take $r=m$, we obtain $a_n^{m+1}b_0=0$. But b_0 is unit, thus a_n is nilpotent and a_nx^n is a nilpotent element in $A[x]$. By Exercise 6.2.1, we know that $f-a_nx^n$ is unit, then we can prove a_{n-1},a_{n-2} is also nilpotent by induction on degree of f. Conversely, if a_0 is unit and

$a_1, \dots, a_n$ is nilpotent. We can imagine that if you power f enough times, then we will obtain unit. Or you can see $\sum_{i=1}^n a_i x^i$ is nilpotent, then unit plus nilpotent is also unit.

For (2)[1]. If $a_0, \dots, a_n$ are nilpotent, then clearly f is. Conversely, if f is nilpotent, then clearly a_n is nilpotent, and we have $f - a_n x^n$ is nilpotent, then by induction on degree of f to conclude.

For (3). $af = 0$ for $a \neq 0$ implies f is a zero-divisor is clear. Conversely choose a $g = \sum_{i=0}^m b_i x^i$ of least degree m such that $fg = 0$, then we have $a_n b_m = 0$, hence $a_n g = 0$, since $a_n g f = 0$ and has degree less than m. Then consider

$$0 = fg - a_n x^n g = (f - a_n x^n) g$$

Then $f - a_n x^n$ is a zero-divisor with degree $n-1$, so we can conclude by induction on degree of f.

For (4). Note that $(a_0, \dots, a_n) = 1$ is equivalent to there is no maximal ideal $\mathfrak{m}$ contains $a_0, \dots, a_n$, it's an equivalent description for primitive polynomials. For $f \in A[x]$, f is primitive if and only if for all maximal ideal $\mathfrak{m}$, we have $f \notin \mathfrak{m}[x]$. Note that we have the following isomorphism

$$A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$$

Indeed, consider the following homomorphism

$$\begin{aligned} \varphi\colon A[x] &\to (A/\mathfrak{m})[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n (a_i + \mathfrak{m}) x^i \end{aligned}$$

Clearly $\ker \varphi = \mathfrak{m}[x]$ and use the first isomorphism theorem. So in other words, $f \in A[x]$ is primitive if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x]$ for any maximal ideal $\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, then $(A/\mathfrak{m})[x]$ is an integral domain by (3), so $\overline{fg} \neq 0 \in (A/\mathfrak{m})[x]$ if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x], \overline{g} \neq 0 \in (A/\mathfrak{m})[x]$. This completes the proof. □

Exercise 6.2.3. Generalize the results of Exercise 6.2.2 to a polynomial ring $A[x_1, \dots, x_r]$ in several indeterminate.

Proof. It suffices to consider the case of $A[x, y]$, since we can do induction on r to conclude general case. Consider $A[x, y] = A[x][y] = B[y]$, where $B = A[x]$. For $f \in B[y]$, we write it as

$$f = \sum_{ij} a_{ij} x^i y^j = \sum_k b_k y^k, \quad b_k = \sum_i a_{ik} x^i \in B$$

For (1). f is a unit in $B[y]$ if and only if b_0 is a unit in B and b_k is nilpotent for $k > 0$, if and only if a_{00} is a unit, and a_{ij} is nilpotent for otherwise.

[1]An alternative proof of (2). Note that

$$\mathfrak{N}(A[x]) = \bigcap \mathfrak{p}[x] = (\bigcap \mathfrak{p})[x] = \mathfrak{N}(A)[x]$$

For (2). f is a nilpotent in $B[y]$ if and only if b_k is nilpotent for all k, if and only if a_{ij} is nilpotent for all i, j.

For (3). f is a zero divisor in $B[y]$ if and only if there exists $a \in A$ such that $af = 0$. Indeed, if f is a zero divisor in $B[y]$, then there exists $b \in B$ such that $bf = 0$, then $bb_k = 0$ for all k, then for each k there exists a_k such that $a_k b_k = 0$, then consider $a = \prod_k a_k$, then $af = 0$.

For (4). fg is primitive if and only if f and g are primitive. Indeed, proof in Exercise 6.2.2 still holds in this case. □

Exercise 6.2.4. In the ring $A[x]$, the Jacobson radical is equal to the nilradical

Proof. Since we already have $\mathfrak{N} \subseteq \mathfrak{R}$, it suffices to show for any $f \in \mathfrak{R}$, it's nilpotent. Note that by property of Jacobson ideal, we have $1 - fg$ is unit for any $g \in A[x]$. Choose g to be x, then by (1) of Exercise 1.8.1 we know that all coefficients of f is nilpotent in A, and by (2) of Exercise 6.2.1, f is nilpotent. This completes the proof. □

Exercise 6.2.5. Let A be a ring and let $A[[x]]$ be the ring of formal power series $f = \sum_{n=0}^{\infty} a_n x^n$ with coefficients in A. Show that

(1) f is a unit in $A[[x]] \Leftrightarrow a_0$ is a unit in A.
(2) If f is nilpotent, then a_n is nilpotent for all $n \geqslant 0$. Is the converse true?
(3) f belongs to the Jacobson radical of $A[[x]] \Leftrightarrow a_0$ belongs to the Jacobson radical of A.
(4) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[x]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x.
(5) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Proof. For (1). Let $g = \sum_{j=1}^{\infty} b_j x^j$ be the inverse of f. Since $fg = 1$, then clearly we have $a_0 b_0 = 1$, thus a_0 is a unit. Conversely, if a_0 is a unit, then consider the Taylor expansion of $1/f$ at $x = 0$ to conclude.

For (2). If $f = \sum_{i=0}^{\infty} a_i x^i$ is nilpotent, then a_0 must be nilpotent, so $f - a_0$ is also nilpotent. Consider $(f - a_0)/x$ which is also nilpotent, we will obtain a_1 is nilpotent. Repeat what we have done to conclude $a_0, a_1, a_2, \dots$ are nilpotent. The converse holds when A is a Noetherian ring.

For (3). $f \in \mathfrak{R}(A[[x]])$ if and only if $1 - fg$ is unit for all $g \in A[[x]]$. Note that the zero term of $1 - fg$ is $1 - a_0 b_0$, so by (1) we obtain $1 - fg$ is unit if and only if $1 - a_0 b_0$ is unit for all $b_0 \in A$, and that's equivalent to $a_0 \in \mathfrak{R}(A)$.

For (4). For maximal ideal $\mathfrak{m} \in A[[x]]$, we have $(x) \subseteq \mathfrak{m}$, since by (3) we have $x \in \mathfrak{R}(A[[x]])$. Then $\mathfrak{m}^c = \mathfrak{m} - (x)$, that is $\mathfrak{m} = \mathfrak{m}^c + (x)$. Furthermore, note that

$$A[[x]]/\mathfrak{m} = A[[x]]/(\mathfrak{m}^c + (x)) \cong A/\mathfrak{m}^c$$

implies $\mathfrak{m}^c$ is maximal. The last isomorphism holds since for a ring A and two ideals $\mathfrak{b} \subseteq \mathfrak{a}$, we have

$$A/\mathfrak{a} \cong (A/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$$

just by considering $A/\mathfrak{a} \to A/\mathfrak{b}$ and use first isomorphism theorem.

For (5). Let $\mathfrak{p}$ be a prime ideal in A. Consider the ideal $\mathfrak{q}$ which is generated by $\mathfrak{p}$ and x. Clearly $\mathfrak{q}^c = \mathfrak{p}$ and $\mathfrak{q}$ is prime since

$$A[[x]]/\mathfrak{q} \cong A/\mathfrak{p}$$

□

Exercise 6.2.6. A ring A is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element e such that $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of A are equal.

Proof. Take $x \in \mathfrak{R}$ which is not in $\mathfrak{N}$. Then (x) is an ideal not contained in $\mathfrak{N}$. Thus there exists a nonzero idempotent $e = xy \in (x)$. Note that an important property of idempotent is that an idempotent is a zero-divisor, since $e(1-e) = 0$. Thus $1 - e = 1 - xy$ is not a unit. So by property of Jacobson ideal, we have $x \notin \mathfrak{R}$, a contradiction. □

Exercise 6.2.7. Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.

Proof. The proof is quite similar to above Exercise: Note that every prime ideal is maximal if and only if nilradical and Jacobson radical are equal. If not, take $x \in \mathfrak{R}$ which is not in $\mathfrak{N}$, then from $x^n = x$ we know that $1 - x^{n-1}$ is not a unit, a contradiction to $x \in \mathfrak{R}$. □

Exercise 6.2.8. Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Proof. Let $\operatorname{Spec} A$ denote the set of all prime ideals of A. Clearly it's not empty, since there exists a maximal ideal. We order $\operatorname{Spec} A$ by reverse inclusion, that is $\mathfrak{p}_a \leq \mathfrak{p}_b$ if $\mathfrak{p}_b \subseteq \mathfrak{p}_a$. By Zorn lemma, it suffices to show every chain in $\operatorname{Spec} A$ has a upper bound in $\operatorname{Spec} A$.

For a chain $\{\mathfrak{p}_i\}_{i \in I}$, it's natural to consider the intersection of all $\mathfrak{p}_i$, denote by $\mathfrak{p}$. It's an ideal clearly. Now it suffices to show it's prime. Suppose $xy \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then there exists $\mathfrak{p}_i, \mathfrak{p}_j$ such that $x \notin \mathfrak{p}_i, y \notin \mathfrak{p}_j$. Without lose of generality we may assume $\mathfrak{p}_i \subset \mathfrak{p}_j$. Then $x, y \notin \mathfrak{p}_i$. But $xy \in \mathfrak{p}$ implies $xy \in \mathfrak{p}_i$, a contradiction to the fact $\mathfrak{p}_i$ is prime. This completes the proof.

Remark 6.2.1. At first I want to check the nilradical is a prime ideal to complete the proof. However, this statement fails in general. And it's easy to explain why: If there exists at least two minimal prime ideals, then nilradical can not be prime. Indeed, the intersections of distinct minimal prime ideal can not be prime, since if $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ is minimal and if $\mathfrak{p} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ is prime, then we must have $\mathfrak{p} = \mathfrak{p}_i$ for some i, which implies $\mathfrak{p}_i$ is contained in other $\mathfrak{p}_j, i \neq j$, a contradiction to minimality. Furthermore, as you can see, nilradical of a ring A is prime if and only if A only has one minimal prime ideal.

□

Exercise 6.2.9. Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \Leftrightarrow \mathfrak{a}$ is an intersection of prime ideals.

Proof. One direction is clear, since $r(\mathfrak{a})$ is the intersection of all prime ideal containing $\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is an intersection of prime ideals, denoted by $\mathfrak{a} = \bigcap_i \mathfrak{p}_i$. If $x^n \in \mathfrak{a}$, then $x^n \in \mathfrak{p}_i$ for each i, then by property of prime ideal we obtain $x \in \mathfrak{p}_i$ for each i, which implies $x \in \mathfrak{a}$. This completes the proof. □

Exercise 6.2.10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following statements are equivalent.

(1) A has exactly one prime ideal.
(2) every element of A is either a unit or nilpotent.
(3) $A/\mathfrak{N}$ is a field.

Proof. (1) to (3): Since A has exactly one prime ideal, it must be a maximal ideal, in this case A is a local ring and clearly $A/\mathfrak{N}$ is a field.

(3) to (2): If $A/\mathfrak{N}$ is a field, thus if an element in A is not a nilpotent, then it must be a unit.

(2) to (1): Consider the set of all nilpotent elements in A, it's clear it's an ideal, and thusd $A/\mathfrak{N}$ is a local ring. □

References

Yau Mathematical Sciences Center, Tsinghua University, Beijing, 100084, P.R. China,
Email address: liubw22@mails.tsinghua.edu.cn