

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. Week-1 | 3 |
| 1.1. Solutions to 4.1 | 3 |
| 1.2. Solutions to 4.2 | 3 |
| 1.3. Solutions to 4.3 | 5 |
| 2. Week-2 | 6 |
| 2.1. Solutions to 4.4 | 6 |
| 2.2. Solutions to 4.5 | 7 |
| 3. Week-3 | 8 |
| 3.1. Solutions to 4.6 | 8 |
| 4. Week-4 | 9 |
| 4.1. Solutions to 4.7 | 9 |
| 4.2. Solutions to 4.8 | 9 |
| 5. Week-5 | 11 |
| 5.1. Solutions to 4.9 | 11 |
| 6. Week-6 | 13 |
| 6.1. Solutions to 4.9 | 13 |
| 6.2. Solutions to Chapter 1 of Atiyah-MacDonald | 13 |
| 7. Week-7 | 17 |
| 7.1. Exercise3-7 in Chapter 2 of Atiyah-MacDonald | 17 |
| 7.2. Exercise9-13 in Chapter 2 of Atiyah-MacDonald | 18 |
| 8. Week-8&9 | 20 |
| 8.1. Exercise2-9 in Chapter 3 of Atiyah-MacDonald | 20 |
| 8.2. Exercise12-15 in Chapter 3 of Atiyah-MacDonald | 24 |
| 9. Week-11 | 26 |
| 9.1. Exercise1-9 in Chapter five of Atiyah-MacDonald | 26 |
| 9.2. Exercise12-13 in Chapter five of Atiyah-MacDonald | 29 |
| 9.3. Exercise28-31 in Chapter five of Atiyah-MacDonald | 30 |
| 10. Week-12 | 33 |
| 10.1. Exercise27 in Chapter 5 of Atiyah-MacDonald | 33 |
| 10.2. Exercise1-7 in Chapter 6 of Atiyah-MacDonald | 33 |

| | |
|---|----|
| 10.3. Exercise 1/2/4 in Chapter 7 of Atiyah-MacDonald | 33 |
| References | 34 |

1. WEEK-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, $f(x) - vg(x) \neq 0$, 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 transcendental over F , otherwise

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

a contradiction to α is transcendental 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 separable 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

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

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 hypothesis, 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

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

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 $\overline{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} , and E is algebraic over \mathbb{Q} , so $\overline{\mathbb{Q}}$ 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. WEEK-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 $\varphi: \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{Q}(\sqrt{2})$ 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 hypothesis one has

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

(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 separable, since any element of E fits a irreducible polynomial, and every irreducible polynomial of F is separable; Conversely, if $F \neq F^p$, then there exists $u \in F \setminus F^p$, then $x^p - u$ is irreducible, but not separable over F , a contradiction.

3. WEEK-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, \dots, 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 an automorphism of E which fixes F . As a consequence, one has $\beta \in K$, and thus $N \subseteq K$.

4. WEEK-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 $\text{char}K = 0$ and thus $K = \mathbb{Q}$, but \mathbb{Q}^\times is not cyclic, a contradiction.
4. Omit.
5. If $\text{char}F = 2$, then $F^2 = F$, and thus $F \subseteq F^2 + F^2$. If $\text{char}F = p > 2$ 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

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

6. Omit.
8. Note that $\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{3})$.
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. WEEK-5

5.1. Solutions to 4.9.

2. We divide into two parts:

- (a) It's clear E/K is Galois, with Galois group $\text{Gal}(E/K)$, 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 $\text{Gal}(E/K)$ is a normal subgroup of $\text{Gal}(E/F)$, and it's clear any subgroup of abelian group is normal, thus K/F is Galois. Furthermore it's Galois group is $\text{Gal}(E/F)/\text{Gal}(E/K)$, 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 unity, 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

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

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

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

6. It's isomorphic to $\text{Aut}(\mathbb{Z}_{12})$, 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

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

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

10. Omit.

6. WEEK-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 $\text{Gal}(E/F(\theta))$ is trivial.

6.2. Solutions to Chapter 1 of Atiyah-MacDonald.

6.2.1. Exercise 1/2 in 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. \square

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 $g = \sum_{i=0}^m b_i x^i$ to denote the inverse of f . Since $fg = 1$ and if we use c_k to denote $\sum_{m+n=k} a_m b_n$, then we have

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

But $c_0 = a_0 b_0$, 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 $a_n b_m = c_{n+m} = 0$. If we have already proven this for $k < r$. Then consider c_{m+n-r} , we have

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

and multiply a_n^r we obtain

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

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 $a_n x^n$ is a nilpotent element in $A[x]$. By Exercise 6.2.1, we know that $f - a_n x^n$ 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

$$\varphi: A[x] \rightarrow (A/\mathfrak{m})[x]$$

$$\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n (a_i + \mathfrak{m}) x^i$$

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 $\overline{f} \overline{g} \neq 0 \in (A/\mathfrak{m})[x]$ 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. \square

6.2.2. *Exercise 4-10 in Chapter 1 of Atiyah-MacDonald.*

Exercise 6.2.3. *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. \square

Exercise 6.2.4. *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 .*

¹An alternative proof of (2). Note that

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

- (2) If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. 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 $A/\mathfrak{a} \rightarrow A/\mathfrak{b}$ 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 6.2.5. 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 6.2.6. 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

$x \in \mathfrak{N}$ 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 $x \in \mathfrak{N}$. \square

Exercise 6.2.7. 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 $\text{Spec} A$ denote the set of all prime ideals of A . Clearly it's not empty, since there exists a maximal ideal. We order $\text{Spec} A$ 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 $\text{Spec} A$ has a upper bound in $\text{Spec} A$.

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 loss 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 $\mathfrak{p} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$ 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. \square

Exercise 6.2.8. 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. \square

Exercise 6.2.9. 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 thus A/\mathfrak{N} is a local ring. \square

7. WEEK-7

7.1. Exercise3-7 in Chapter 2 of Atiyah-MacDonald.

Exercise 7.1.1. Let A be a local ring, M and N finitely generated A -modules. Prove that if $M \otimes N = 0$, then $M = 0$ or $N = 0$.

Proof. Let \mathfrak{m} be the maximal ideal, $k = A/\mathfrak{m}$ the residue field. Let $M_k = k \otimes_A M \cong M/\mathfrak{m}M$ by Exercise 2.8.2. By Nakayama's lemma, $M_k = 0 \Rightarrow M = 0$. Note that by definition we have

$$\begin{aligned} (M \otimes_A N)_k &= k \otimes_A (M \otimes_A N) \\ &= (k \otimes_A M) \otimes_A N \\ &= ((k \otimes_A M) \otimes_k k) \otimes_A N \\ &= (k \otimes_A M) \otimes_k (k \otimes_A N) \\ &= M_k \otimes_k N_k \end{aligned}$$

Thus $M \otimes_A N = 0 \Rightarrow (M \otimes_A N)_k = 0 \Rightarrow M_k \otimes_k N_k = 0 \Rightarrow M_k = 0$ or $N_k = 0$, since M_k, N_k are vector spaces over a field. \square

Exercise 7.1.2. Let $M_i, i \in I$ be any family of A -modules and M be their direct sum. Prove that M is flat \Leftrightarrow each M_i is flat.

Proof. It suffices to show tensor commutes with direct sum, that is for any A -module B , we have

$$B \otimes \bigoplus M_i = \bigoplus (B \otimes M_i)$$

And it's clear from Proposition 2.14 of [AM69]. \square

Exercise 7.1.3. Let $A[x]$ be the ring of polynomials in one indeterminate over a ring A . Prove that $A[x]$ is a flat A -algebra.

Proof. Note that $A[x] = \bigoplus_i M_i$, where $M_i = Ax^i$. Clearly $M_i \cong A$ as A -modules, and A is flat as an A -module. Thus by Exercise 2.8.4 we obtain $A[x]$ is flat. \square

Exercise 7.1.4. For any A -module, let $M[x]$ denote the set of all polynomials in x with coefficients in M , that is to say expressions of the form

$$m_0 + m_1x + \cdots + m_r x^r \quad m_i \in M$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$ -module. Show that $M[x] \cong A[x] \otimes_A M$.

Proof. Firstly, let's define the $A[x]$ -module structure on $M[x]$: For $\sum a_i x^i \in A[x], \sum m_j x^j \in M[x]$, define $A[x]$ action as

$$(\sum a_i x^i)(\sum m_j x^j) = \sum c_k x^k, \quad c_k = \sum_{i+j=k} a_i m_j$$

It's a routine to check it do gives an $A[x]$ -module structure, we omit here.

Consider the following map

$$\begin{aligned} \phi: M[x] &\rightarrow A[x] \otimes_A M \\ \sum m_i x^i &\mapsto \sum x^i \otimes m_i \end{aligned}$$

It's an $A[x]$ -module homomorphism. Indeed, for $\sum a_i x^i \in A[x]$, we have

$$\begin{aligned}
 \phi(\sum a_i x^i \sum m_j x^j) &= \phi(\sum_{i+j=k} a_i m_j x^{i+j}) \\
 &= \sum_k \sum_{i+j=k} x^{i+j} \otimes a_i m_j \\
 &= \sum_{i,j} x^i x^j \otimes a_i m_j \\
 &= \sum_j ((\sum_i a_i x^i) x^j \otimes m_j) \\
 &= (\sum_i a_i x^i) (\sum_j x^j \otimes m_j) \\
 &= (\sum_i a_i x^i) \phi(\sum_j m_j x^j)
 \end{aligned}$$

As desired. Conversely, consider $\tilde{\psi}: A[x] \times M \rightarrow M[x]$ defined by $\tilde{\psi}(\sum a_i x^i, m) = \sum a_i m x^i$. It induces a linear map $\psi: A[x] \otimes_A M \rightarrow M[x]$ by sending $(\sum a_i x^i) \otimes m$ to $\sum a_i m x^i$. Clearly ψ and ϕ are inverse. \square

Remark 7.1.1. From this Exercise, hope you can get a feeling of a use of tensor product: a kind of changing domain of coefficients.

Exercise 7.1.5. Let \mathfrak{p} be a prime ideal in A . Show that $\mathfrak{p}[x]$ is a prime ideal in $A[x]$. If \mathfrak{m} is a maximal ideal in A , is $\mathfrak{m}[x]$ a maximal ideal in $A[x]$?

Proof. It suffices to check $A[x]/\mathfrak{p}[x]$ is a domain. Note that $A[x]/\mathfrak{p}[x] \cong (A/\mathfrak{p})[x]$. By Exercise 6.2.2, f is a zero-divisor in $(A/\mathfrak{p})[x]$ if and only if there exists $a \in A/\mathfrak{p}$ such that $af = 0$, but it's impossible since A/\mathfrak{p} is a domain. However, $\mathfrak{m}[x]$ may not be a maximal ideal. For example, let $A = \mathbb{Q}$ and $\mathfrak{m} = (0)$, then clearly (0) is not maximal in $\mathbb{Q}[x]$. \square

7.2. Exercise9-13 in Chapter 2 of Atiyah-MacDonald.

Exercise 7.2.1. Let $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ be an exact sequence of A -modules. If M' and M'' are finitely generated, then so is M .

Proof. There exist sets of generators $\{x_i\}_{i \in I}$ of M' and $\{\overline{y_j}\}_{j \in J}$ of M'' . Consider the preimage of $\{\overline{y_j}\}_{j \in J}$ in M , denoted by $\{y_j\}_{j \in J}$. It's clear $\{f(x_i)\}_{i \in I}$ together with $\{y_j\}_{j \in J}$ generates M by the exactness of sequence. \square

Exercise 7.2.2. Let A be a ring, \mathfrak{a} an ideal contained in the Jacobson radical of A . Let M be an A -module and N a finitely generated A -module, and let $u: M \rightarrow N$ be a homomorphism. If the induced homomorphism $M/\mathfrak{a}M \rightarrow N/\mathfrak{a}N$ is surjective, then u is surjective.

Proof. Consider the following composition

$$M \rightarrow M/\mathfrak{a}M \xrightarrow{u} N/\mathfrak{a}N$$

It's surjective, since it's a composition of two surjective mappings, which implies $u(M) + \mathfrak{a}N = N$. Note that N is finitely generated and $\mathfrak{a} \subseteq \mathfrak{R}$. Then Nakayama's lemma implies $\mu(M) = N$. \square

Exercise 7.2.3. Let A be a ring $\neq 0$. Show that $A^m \cong A^n \Rightarrow m = n$. Furthermore,

(1) If $\phi: A^m \rightarrow A^n$ is surjective, then $m \geq n$.

(2) If $\phi: A^m \rightarrow A^n$ is injective, is it always the case that $m \leq n$?

Proof. (1). Let \mathfrak{m} be a maximal ideal of A and let $\phi: A^m \rightarrow A^n$ be an isomorphism. Then $1 \otimes \phi: (A/\mathfrak{m}) \otimes A^m \rightarrow (A/\mathfrak{m}) \otimes A^n$ is an isomorphism between vector spaces of dimensions m and n over the field $k = A/\mathfrak{m}$. Indeed, there is a surjective map $A^m \rightarrow A^n$ and surjective map $A^n \rightarrow A^m$, so there is a surjective map $(A/\mathfrak{m}) \otimes A^m \rightarrow (A/\mathfrak{m}) \otimes A^n$ and vice versa. Hence $m = n$. So it's natural to see (1) is also true.

(2). This method fails for the case ϕ is injective, since tensor is just a right exact functor, but this statement is still true. \square

Exercise 7.2.4. Let M be a finitely generated A -module and $\phi: M \rightarrow A^n$ a surjective homomorphism. Show that $\ker \phi$ is finitely generated.

Proof. Consider the following exact sequence

$$0 \rightarrow \ker \phi \rightarrow M \xrightarrow{\phi} A^n \rightarrow 0$$

Since A^n is a free A -module, so this exact sequence splits, which is equivalent to $\ker \phi$ is a direct summand of M . Then $\ker \phi$ is finitely generated, since M is. \square

Exercise 7.2.5. Let $f: A \rightarrow B$ be a ring homomorphism, and let N be a B -module. Regarding N as an A -module by restriction of scalars, form the B -module $N_B = B \otimes_A N$. Show that the homomorphism $g: N \rightarrow N_B$ which maps y to $1 \otimes y$ is injective and that $g(N)$ is a direct summand of N_B .

Proof. Consider the following mapping

$$\begin{aligned} p: N_B &\rightarrow N \\ b \otimes y &\mapsto by \end{aligned}$$

Directly check $p \circ g$ as follows: Take $y \in N$, then

$$p \circ g(y) = p(1 \otimes y) = y$$

So we have $p \circ g$ is identity on N , which implies g is injective. Furthermore, this implies the following sequence splits

$$0 \rightarrow N \xrightarrow{g} N_B \rightarrow N_B/\text{im } g \rightarrow 0$$

which is equivalent to $g(N)$ is a direct summand of N_B . \square

8. WEEK-8&9

8.1. Exercise 2-9 in Chapter 3 of Atiyah-MacDonald.

Exercise 8.1.1. Let \mathfrak{a} be an ideal of a ring A , and let $S = 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$.

Proof. It suffices to show for every maximal ideal \mathfrak{m} of $S^{-1}A$, we have $S^{-1}\mathfrak{a} \subseteq \mathfrak{m}$. Note that every ideal of $S^{-1}A$ is an extended ideal, thus there exists an ideal \mathfrak{b} of A such that $S^{-1}\mathfrak{b} = \mathfrak{m}$. Furthermore, $\mathfrak{b} \cap (1 + \mathfrak{a}) = \emptyset$, which implies $(\mathfrak{a} + \mathfrak{b}) \cap (1 + \mathfrak{a}) = \emptyset$. Thus $S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b} \neq (1)$ and it contains $S^{-1}\mathfrak{b}$. By maximality of $S^{-1}\mathfrak{b}$ we have $S^{-1}\mathfrak{a} \subseteq \mathfrak{m}$. This completes the proof. \square

Remark 8.1.1. Now let's show we can derive Corollary ?? from Nakayama's lemma: If M is a finitely generated A -module and \mathfrak{a} is an ideal of A such that $\mathfrak{a}M = M$. Let $S = 1 + \mathfrak{a}$ and note that

$$S^{-1}M = S^{-1}(\mathfrak{a}M) = (S^{-1}\mathfrak{a})(S^{-1}M)$$

Since $S^{-1}\mathfrak{a}$ is contained in Jacobson radical, so Nakayama's lemma implies $S^{-1}M = 0$. By Exercise 3.5.1, there exists $x = 1 + a \in S$ such that $xM = 0$. In this case, $x = 1 + a \equiv 1 \pmod{\mathfrak{a}}$ as desired.

Exercise 8.1.2. Let A be a ring, let S and T be two multiplicative closed subsets of A , and let U be the image of T in $S^{-1}A$. Show that the rings $(ST)^{-1}A$ and $U^{-1}(S^{-1}A)$ are isomorphic.

Proof. It suffices to show $U^{-1}(S^{-1}A)$ is also the localization of A with respect to ST , and use the fact localization is unique. Take $g: A \rightarrow B$ such that $g(st)$ is a unit for all $s \in S, t \in T$. Consider the following commutative diagram

$$\begin{array}{ccccc} A & \xrightarrow{f_S} & S^{-1}A & \xrightarrow{f_U} & U^{-1}(S^{-1}A) \\ g \downarrow & \nearrow h_1 & & \nearrow h_2 & \\ B & & & & \end{array}$$

h_1 is induced by the fact $g(s)$ is unit for all $s \in S$. Furthermore, $h_1(\bar{t})$ is unit in B for all $\bar{t} \in U$, since $\bar{t} = f_S(t)$ for some $t \in T$ and $h_1 \circ f_S = g$, so it induces h_2 . Note that $h_2 \circ f_U \circ f_S = g$, which implies that $U^{-1}(S^{-1}A)$ is the localization of A with respect to ST . \square

Exercise 8.1.3. Let $f: A \rightarrow B$ be a homomorphism of rings and let S be a multiplicative closed subset of A . Let $T = f(S)$. Show that $S^{-1}B$ and $T^{-1}B$ are isomorphic as $S^{-1}A$ -modules.

Proof. It's clearly $S^{-1}B$ is a $S^{-1}A$ -module, and the $S^{-1}A$ -module structure on $T^{-1}B$ is given by $a/s \cdot b := f(a) \cdot b/f(s)$. Consider the following $S^{-1}A$ -module morphism:

$$\begin{aligned} \phi: S^{-1}B &\rightarrow T^{-1}B \\ b/s &\mapsto b/f(s) \end{aligned}$$

It's well-defined, since for $b/s = b'/s'$, there exists $u \in S$ such that $(bs' - b's)u = 0$, thus $f((bs' - b's)u) = (bf(s') - b'f(s))f(u) = 0$, that is $b/f(s) = b'/f(s')$ in $T^{-1}B$.

It's clearly surjective. For injectivity: If $\phi(b/s) = 0$, then there exists $f(s') \in T$ such that $f(s')b = 0$. But if we want to show $b/s = 0$, we need to find $s' \in S$ such that $s' \cdot b = 0$, and that's exactly $f(s')b = 0$. So ϕ is an isomorphism. \square

Exercise 8.1.4. Let A be a ring. Suppose that, for each prime ideal \mathfrak{p} , the local ring $A_{\mathfrak{p}}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_{\mathfrak{p}}$ is an integral domain, is A necessarily an integral domain?

Proof. That's to show nilpotence is a local property: It suffices to show nilradical \mathfrak{N} of A is zero, note that $(\mathfrak{N})_{\mathfrak{p}}$ is the nilradical of $A_{\mathfrak{p}}$. If for all prime ideal \mathfrak{p} we have $A_{\mathfrak{p}}$ contains no nilpotent element, thus $(\mathfrak{N})_{\mathfrak{p}} = 0$ for all prime ideals \mathfrak{p} , which implies $\mathfrak{N} = 0$.

However, integral is not a local property. Consider \mathbb{Z}_6 , it's clearly not a domain. The prime ideals of it are

$$\mathfrak{p} = \mathbb{Z}_3$$

$$\mathfrak{q} = \mathbb{Z}_2$$

Now let's see its localization at \mathfrak{p} : Since it's a local ring, it suffices to consider it's maximal ideal, that's the extension of \mathfrak{p}

$$\begin{aligned} \mathfrak{p}(\mathbb{Z}_6)_{\mathfrak{p}} &= \{r/s \mid r \in \mathfrak{p}, s \notin \mathfrak{p}\} \\ &= \left\{ \frac{0}{1}, \frac{2}{1}, \frac{4}{1}, \frac{0}{3}, \frac{2}{3}, \frac{4}{3}, \frac{0}{5}, \frac{2}{5}, \frac{4}{5} \right\} \end{aligned}$$

However, $r_1/s_1 = r_2/s_2$ if and only if there is $u \notin \mathfrak{p}$ such that $u(r_1s_2 - r_2s_1) = 0$. Thus $2/1 = 0/1$ since $3(2 \times 1 - 0) = 0$. In fact, after simple computations we can see $\mathfrak{p}(\mathbb{Z}_6)_{\mathfrak{p}} = 0$. That's it's a field, definitely a domain. \square

Exercise 8.1.5. Let A be a ring $\neq 0$ and let Σ be the set of all multiplicative closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements, and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal prime ideal of A .

Proof. By Zorn's lemma it's easy to see it has a maximal element. Now let's see S is maximal if and only if $A - S$ is a minimal prime ideal: Note that for a general multiplicative closed subset, the complement of it may not be a prime ideal. However, for a maximal multiplicative closed subset, the complement of it must be a prime ideal: For a multiplicative closed subset S , and $\mathfrak{p} = A - S$.

- (1) To see $a + b \in \mathfrak{p}$ for any $a, b \in \mathfrak{p}$: It suffices to show $a + b \in S$ implies either $a \in S$ or $b \in S$. If $a + b \in S$, consider the multiplicative sets $A = S(a^n)_{n \geq 0}$ and $B = S(b^n)_{n \geq 0}$. If $0 \in A \cap B$, then there exists $s_1, s_2 \in S$ and $n, m \geq 0$ such that

$$s_1 a^n = s_2 b^m = 0$$

Then we have

$$0 = s_1 s_2 (a + b)^{n+m} \in S$$

A contradiction. Therefore, Without lose of generality we may assume $0 \notin S(a^n)_{n \geq 0}$. By maximality of S , this implies $S(a^n)_{n \geq 0} = S$ and so that $a \in S$.

- (2) To see $ra \in \mathfrak{p}$ for any $r \in A, a \in \mathfrak{p}$: Its contrapositive is $ra \in S$ for some $r \in A$ implies $a \in S$. Similarly if $0 \in S(a^n)_{n \geq 0}$ then there exists $s_1 \in S$ and $n \geq 0$ such that $s_1 a^n = 0$. Then

$$0 = s_1 r^n a^n \in S$$

A contradiction. Therefore again by maximality of S we have $a \in S$.

- (3) \mathfrak{p} is prime is clear.

Thus for a maximal multiplicative closed subset S , $\mathfrak{p} = A - S$ must be a prime ideal, and it must be minimal, otherwise for $\mathfrak{p}' \subseteq \mathfrak{p}$, $A - \mathfrak{p}'$ will contain S .

On the other hand: assume $\mathfrak{p} = A - S$ is a minimal prime ideal, and it's not maximal. Then S must be contained in some maximal multiplicative closed subset S' , note that $S' = A - \mathfrak{p}'$ for some minimal prime ideal, but $S \subseteq S'$ implies $\mathfrak{p}' \subseteq \mathfrak{p}$, a contradiction to the minimality of \mathfrak{p} . \square

Exercise 8.1.6. A multiplicative closed subset S of a ring A is said to be saturated if $xy \in S$ if and only if $x \in S$ and $y \in S$. Prove that

- (1) S is saturated if and only if $A - S$ is a union of prime ideals.
- (2) If S is any multiplicative closed subset of A , there is a unique smallest saturated multiplicative closed subset \bar{S} containing S , and that \bar{S} is the complement in A of the union of the prime ideals which do not meet S . (\bar{S} is called the saturation of S .)
- (3) If $S = 1 + \mathfrak{a}$, where \mathfrak{a} is an ideal of A , find \bar{S} .

Proof. For (1). If \mathfrak{p} is a union of prime ideals, then it's clear S is saturated. Conversely, if S is saturated, then if $x \notin S$, then $rx \notin S$ for all $r \in A$, which implies $(x) \cap S = \emptyset$. So $S^{-1}(x) \neq (1)$, and it is contained in some prime ideal \mathfrak{q} . Then

$$(x) \subseteq (S^{-1}(x))^c \subseteq \mathfrak{q}^c$$

Furthermore, $\mathfrak{q}^c \cap S = \emptyset$, thus (x) is contained in a prime $\mathfrak{q}^c \subseteq A - S$. That is every element of $A - S$ lies in some prime ideal, thus $A - S$ is a union of prime ideals.

For (2). If \mathfrak{p} is the union of all prime ideals which do not meet S , then $\bar{S} = A - \mathfrak{p}$ is a saturated multiplicative closed subset containing S . If \bar{S} is not minimal, then the minimal one \bar{S}' must be contained in \bar{S} , then consider $\mathfrak{p}' = A - \bar{S}'$, clear $\mathfrak{p} \subseteq \mathfrak{p}'$. Furthermore, \mathfrak{p}' is the union of prime ideals which do not meet S , thus \mathfrak{p} do not contain all, a contradiction.

For (3). If $S = 1 + \mathfrak{a}$. \square

Exercise 8.1.7. Let S, T be multiplicative closed subsets of A , such that $S \subseteq T$. Let $\phi: S^{-1}A \rightarrow T^{-1}A$ be the homomorphism which maps each $a/x \in S^{-1}A$ to a/x considered as an element of $T^{-1}A$. Show that the following statements are equivalent:

- (1) ϕ is bijective.
- (2) For each $t \in T$, $t/1$ is a unit in $S^{-1}A$.
- (3) For each $t \in T$ there exists $x \in A$ such that $xt \in S$.
- (4) T is contained in the saturation of S .
- (5) Every prime ideal which meets T also meets S .

Proof. For (1) to (2). Since ϕ is surjective, then there exists $a/s \in S^{-1}A$ such that $\phi(a/s) = 1/t$ in $T^{-1}A$. Consider $\phi(a/s \cdot t/1) = 1/1 \in T^{-1}A$, by injectivity of ϕ we have a/s is the inverse of $t/1$.

For (2) to (3). If $t/1$ is a unit in $S^{-1}A$, use a/s to denote its inverse. Then $at/s = 1/1$ in $S^{-1}A$ implies there exists $u \in S$ such that $u(at - s) = 0$. Let $x = au$, we have $xt \in S$.

For (3) to (1). For injectivity: if $a/s = 0$ in $T^{-1}A$, then there exists $t \in T$ such that $at = 0$. But there exists $x \in A$ such that $xt \in S$, thus $axt = 0$ implies $a/s = 0$ in $S^{-1}A$. For surjectivity, for $a/t \in T^{-1}A$, since there exists $x \in A$ such that $xt \in S$. Note that $a/t = ax/xt \in T^{-1}A$, thus $\phi(ax/xt) = a/t$ as desired.

For (3) to (4). For $t \in T$ there exists $x \in A$ such that $xt \in S \subset \bar{S}$, then $t \in \bar{S}$ since \bar{S} is saturated.

For (4) to (5). If there exists a prime ideal which meets T but not meets S , then T can not be contained in \bar{S} , since \bar{S} is the complement of the union of all prime ideals which do not meet S .

For (5) to (3). If there exists a $t \in T$ such that there is no $x \in A$ satisfying $xt \in S$, then $(t) \cap S = \emptyset$. Then consider $S^{-1}(t) \in S^{-1}A$, it must be contained in some prime ideal \mathfrak{p} . Then $(t) \subseteq \mathfrak{p}^e$, that is (t) is contained in a prime ideal which does not meet S , a contradiction. \square

Exercise 8.1.8. The set S_0 of all non-zero-divisors in A is a saturated multiplicative closed subset of A . Hence the set D of zero-divisors in A is a union of prime ideals. Show that every minimal prime ideal of A is contained in D .

The ring $S_0^{-1}A$ is called the total ring of fractions of A . Prove that

- (1) S_0 is the largest multiplicative closed subset of A for which the homomorphism $A \rightarrow S_0^{-1}A$ is injective.
- (2) Every element in $S_0^{-1}A$ is either a zero-divisor or a unit.
- (3) Every ring in which every non-unit is a zero-divisor is equal to its total ring of fractions (i.e., $A \rightarrow S_0^{-1}A$ is bijective).

Proof. For any minimal prime ideal \mathfrak{p} , $S = A - \mathfrak{p}$ is a maximal multiplicative closed subset. If we want to show every minimal prime ideal of A is contained in D , it suffices to show S_0 is contained in every maximal multiplicative closed subset. Indeed, if $S_0 \not\subseteq S$ for some maximal multiplicative closed subset S which does not contain 0, then SS_0 must contain 0, since it strictly contains S . But this implies there exist $s_0 \in S_0, s \in S$ such that $s_0s = 0$, a contradiction to the definition of S_0 .

For (1). It's clear $f: A \rightarrow S_0^{-1}A$ is injective, since by Remark 3.1.5 we know the kernel of f is zero divisor of A . Furthermore, $S_0^{-1}A$ is maximal. Indeed, assume $S_0 \subset S$ for some S , then there exists a zero-divisor a of A in S , then $f: A \rightarrow S^{-1}A$ maps u into zero, not injective.

For (2). Note that if $a/s = 0 \in S_0^{-1}A$ is a zero-divisor, then there exists $u \in S_0$ such that $au = 0$, but u is a non-zero-divisor, then $a = 0$. So $a/s = 0 \in S_0^{-1}A$ if and only if $a = 0$, thus $a/s \in S_0^{-1}A$ is a zero-divisor if and only if a is. So if a/s is not a zero-divisor, thus a is not a zero-divisor, that is $a \in S_0$, thus a/s is a unit.

For (3). Note that if in ring A every non-unit is a zero-divisor, then S_0 , the set of all non-zero-divisors is exactly the set of all units. Thus $A \rightarrow S_0^{-1}A$ clearly a bijective, since localization is the most economic operation to make all elements in S_0 to be unit. \square

8.2. Exercise 12-15 in Chapter 3 of Atiyah-MacDonald.

Exercise 8.2.1. Let A be an integral domain and M an A -module. An element $x \in M$ is a torsion element of M if $\text{Ann}(x) \neq 0$, that is if x is killed by some non-zero element of A . Show that the torsion elements of M form a submodule of M . This submodule is called the torsion submodule of M and is denoted by $T(M)$. If $T(M) = 0$, the module M is said to be torsion-free. Show that

- (1) If M is any A -module, then $M/T(M)$ is torsion-free.
- (2) If $f: M \rightarrow N$ is a module homomorphism, then $f(T(M)) \subseteq T(N)$.
- (3) If $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ is an exact sequence, then the sequence $0 \rightarrow T(M') \xrightarrow{f} T(M) \xrightarrow{g} T(M'')$ is exact.
- (4) If M is any A -module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A M$, where K is the field of fractions of A .

Proof. It's clear that all torsion elements form a submodule module of M . For (1). We need to show $T(M/T(M)) = 0$: If $x + T(M) \in M/T(M)$ is a torsion element, so there exists $a_1 \in A$ such that $a_1x \in T(M)$, so there exists a_2 such that $a_2a_1x = 0$, that is $x \in T(M)$.

For (2). Take $x \in T(M)$, then there exists $a \in A$ such that $ax = 0$, it's clear to see $f(a)f(x) = 0$, so $f(x) \in T(N)$, which implies $f(T(M)) \subseteq T(N)$.

For (3). It's clear $f: T(M') \rightarrow T(M)$ is still injective, since for $x \in T(M')$ we can regard it as an element in M' and $f(x) = 0$ implies $x = 0$. By the same method, we can see $\text{im } f \subseteq \ker g$. Now it suffices to show $\ker g \subseteq \text{im } f$. Take $x \in T(M)$ such that $g(x) = 0$, then there exists $y \in M'$ such that $f(y) = x$, then it suffices to show $y \in T(M')$. Indeed, note that there exists $a \in A$ such that $ax = 0$, so $f(ay) = 0$, then $ay = 0$ since f is injective.

For (4). It's clear $T(M)$ lies in the kernel of this mapping. Conversely, note that $K \otimes_A M \cong (A \setminus \{0\})^{-1}M$, this isomorphism is defined by $a/s \otimes m \mapsto am/s$. So the kernel of $M \rightarrow K \otimes_A M$ is the same as the kernel of $M \rightarrow K \otimes_A M \rightarrow (A \setminus \{0\})^{-1}M$. The latter mapping is given by $m \mapsto m/1$. So $m/1 = 0$ implies there exists $a \in A \setminus \{0\}$ such that $am = 0$, that is $m \in T(M)$. \square

Exercise 8.2.2. Let S be a multiplicative closed subset of an integral domain A . In the notation of Exercise 3.5.12, show that $T(S^{-1}M) = S^{-1}(T(M))$. Deduce that the following statements are equivalent.

- (1) M is torsion-free.
- (2) $M_{\mathfrak{p}}$ is torsion-free for all prime ideal \mathfrak{p} .
- (3) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals \mathfrak{m} .

Proof. For $x \in T(M)$, there exists $a \in A$ such that $ax = 0$, so $x/s \in T(S^{-1}M)$ since $a/1 \cdot x/s = 0$, that is $S^{-1}(T(M)) \subseteq T(S^{-1}M)$. Conversely, if $x/s \in T(S^{-1}M)$, there

exists a/s' such that $a/s' \cdot x/s = 0$, that is there exists $u \in S$ such that $uax = 0$, that is $x \in T(M)$. Thus $T(S^{-1}M) = S^{-1}(T(M))$.

For (1) to (2). It's clear since $T(M_p) = T(M)_p = 0$. For (2) to (3). Trivial.

For (3) to (1). It suffices to show $T(M)_m$ for all maximal ideal m , and that's clear. \square

Exercise 8.2.3. Let M be an A -module and \mathfrak{a} an ideal of A . Suppose that $M_m = 0$ for all maximal ideals $m \supseteq \mathfrak{a}$. Prove that $M = \mathfrak{a}M$.

Proof. It suffices to show A/\mathfrak{a} -module $M/\mathfrak{a}M = 0$. But

$$(M/\mathfrak{a})_m \cong M_m/(\mathfrak{a}M)_m = 0$$

This completes the proof. \square

Exercise 8.2.4. Let A be a ring, and let F be the A -module A^n . Show that every set of n generators of F is a basis of F . Deduce that every set of generators of F has at least n elements.

Proof. Let x_1, \dots, x_n be a set of generators and e_1, \dots, e_n the canonical basis of F . Define $\phi: F \rightarrow F$ by $\phi(e_i) = x_i$. Then ϕ is surjective and we have to prove that it is an isomorphism. Since injectivity is a local property we may assume that A is a local ring. Let N be the kernel of ϕ and let $k = A/\mathfrak{m}$ be the residue field of A . Since field is always flat, the exact sequence $0 \rightarrow N \rightarrow F \xrightarrow{\phi} F \rightarrow 0$ gives an exact sequence

$$0 \rightarrow k \otimes N \rightarrow k \otimes F \xrightarrow{1 \otimes \phi} k \otimes F \rightarrow 0$$

Now $k \otimes F = k^n$ is an n -dimensional vector space over k . $1 \otimes \phi$ is surjective, hence bijective, hence $k \otimes N = N/\mathfrak{m}N = 0$. Also N is finitely generated, by Chapter 2, Exercise 2.8.12, hence $N = 0$ by Nakayama's lemma, since $N = \mathfrak{m}N$ and for a local ring $\mathfrak{m} = \mathfrak{R}$. Hence ϕ is an isomorphism.

Assume $\{x_1, \dots, x_k\}, k < n$ is a set of generators of F , then add $\{e_{k+1}, \dots, e_n\}$ into them we still obtain a set of generators, with n elements. Then we know that

$$\begin{cases} \phi(e_i) = x_i, & 1 \leq i \leq k \\ \phi(e_i) = e_i, & k < i \leq n \end{cases}$$

is an isomorphism. Claim $\{x_1, \dots, x_k\}$ can not generate e_{k+1} . Indeed, if $\sum_{i=1}^k a_i x_i = e_{k+1}$, then

$$\phi\left(\sum_{i=1}^k a_i e_i\right) = \sum_{i=1}^k a_i x_i = e_{k+1} = \phi(e_{k+1})$$

But ϕ is injective, thus $\sum_{i=1}^k a_i e_i = e_{k+1}$, a contradiction. \square

9. WEEK-11

9.1. Exercise 1-9 in Chapter five of Atiyah-MacDonald.

Exercise 9.1.1. Let $f: A \rightarrow B$ be an integral homomorphism of rings. Show that $f^*: \text{Spec} B \rightarrow \text{Spec} A$ is a closed mapping.

Proof. Firstly, consider $A \xrightarrow{f} f(A) \xrightarrow{i} B$, where i is an inclusion. Then one has $\text{Spec} f(A)$ is homeomorphic to a closed subset of $\text{Spec} A$, thus it suffices to show $i^*: \text{Spec} B \rightarrow \text{Spec} f(A)$ is a closed mapping, that is we may assume $A \subseteq B$, as a subring.

For an closed sets $V(\mathfrak{b})$ of $\text{Spec} B$, we claim

$$f^*(V(\mathfrak{b})) = V(f^{-1}(\mathfrak{b}))$$

thus it's closed mapping. Indeed, note that $V(\mathfrak{b}) = \{\mathfrak{q} \supseteq \mathfrak{b} \mid \mathfrak{q} \text{ is prime}\}$, then it's clear $f^*(\mathfrak{q}) = f^{-1}(\mathfrak{q}) \supseteq f^{-1}(\mathfrak{b})$ and it's prime, thus $f^*(V(\mathfrak{b})) \subseteq V(f^{-1}(\mathfrak{b}))$. Conversely, for any prime \mathfrak{p} containing $f^{-1}(\mathfrak{b})$, by going-up theorem, there exists $\mathfrak{q} \supseteq \mathfrak{b}$ such that $\mathfrak{q}^c = \mathfrak{p}$, this implies reverse inclusion. \square

Exercise 9.1.2. Let A be a subring of a ring B such that B is integral over A , and let $f: A \rightarrow \Omega$ be a homomorphism of A into an algebraically closed field Ω . Show that f can be extended to a homomorphism of B into Ω .

Proof. Since Ω is a field, thus $\ker f$ is a prime ideal, denoted by \mathfrak{p} . By going-up theorem, there exists a prime ideal \mathfrak{q} of B such that its contraction is \mathfrak{p} since B is integral over A . Furthermore, Proposition 9.1.1 implies B/\mathfrak{q} is integral over A/\mathfrak{p} . So if we extend $\tilde{f}: A/\mathfrak{p} \rightarrow \Omega$ to $\tilde{f}': B/\mathfrak{q} \rightarrow \Omega$, we can also extend $f: A \rightarrow \Omega$ to $f': B \rightarrow \Omega$, that is we reduce our case to A, B are integral domains and f is injective.

Let $S = A \setminus \{0\}$, then consider the localization $S^{-1}B$, by (2) of Proposition 9.1.1 one has $S^{-1}B$ is also integral over $\text{Frac} A$. By Proposition 9.1.2 one has $S^{-1}B$ is a field, and it equals to $\text{Frac} B$ since it's contained in $\text{Frac} B$. That's $\text{Frac} B$ is integral over $\text{Frac} A$, which implies $\text{Frac} B$ is an algebraic extension of $\text{Frac} A$. Thus we can firstly extend $f: A \rightarrow \Omega$ to $\tilde{f}: \text{Frac} A \rightarrow \Omega$, namely by $a_1/a_2 \mapsto f(a_1)/f(a_2)$, and the following lemma completes the proof.

Lemma 9.1.1. Let $f: k \rightarrow \Omega$ be a homomorphism of fields, where Ω is an algebraically closed field. For any algebraic extension k' , there is a homomorphism $f': k' \rightarrow \Omega$ which extends f .

Proposition 9.1.1. Let $A \subseteq B$ be rings, B integral over A .

- (1) If \mathfrak{b} is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$, then B/\mathfrak{b} is integral over A/\mathfrak{a} .
- (2) If S is a multiplicative closed subset of A , then $S^{-1}B$ is integral over $S^{-1}A$.

Proposition 9.1.2. Let $A \subseteq B$ be integral domains, B integral over A . Then B is a field if and only if A is a field.

\square

Exercise 9.1.3. Let $f: B \rightarrow B'$ be a homomorphism of A -algebras, and let C be an A -algebra. If f is integral, prove that $f \otimes 1: B \otimes_A C \rightarrow B' \otimes_A C$ is integral.

Proof. For any element $\sum_{i=1}^n b'_i \otimes c_i \in B' \otimes_A C$, it suffices to check $b'_i \otimes c_i$ is integral over $f(B) \otimes_A C$ for any i , since integral closure is a subring of $B' \otimes_A C$. For $b' \in B'$, there exists a polynomial

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

such that b' is a root of it, where $a_i \in f(B)$. So for $b' \otimes c \in B' \otimes_A C$, consider the following polynomial

$$x^n + (a_1 \otimes c)x^{n-1} + (a_2 \otimes c^2)x^{n-2} + \cdots + a_n \otimes c^n$$

Then

$$\begin{aligned} (b' \otimes c)^n + (a_1 \otimes c)(b' \otimes c)^{n-1} + \cdots + a_n \otimes c^n &= (b')^n \otimes c^n + a_1 b' \otimes c^n + \cdots + a_n \otimes c^n \\ &= ((b')^n + a_1(b')^{n-1} + \cdots + a_n) \otimes c^n \\ &= 0 \otimes c^n \\ &= 0 \end{aligned}$$

Thus $b' \otimes c$ is integral over $f(B) \otimes C$, since for each i , we have $a_i \otimes c \in f(B) \otimes C$. In particular, localization preserves integral, since $S^{-1}B$ can be seen as $S^{-1}A \otimes_A B$. \square

Exercise 9.1.4. Let A be a subring of a ring B such that B is integral over A . Let \mathfrak{n} be a maximal ideal of B and let $\mathfrak{m} = \mathfrak{n} \cap A$ be the corresponding maximal ideal of A . Is $B_{\mathfrak{n}}$ necessarily integral over $A_{\mathfrak{m}}$?

Proof. No. Consider the case $A = k[x^2 - 1]$ and $B = k[x]$, where k is a field, and consider the maximal ideal $\mathfrak{n} = (x - 1)$ of B . It's clear $\mathfrak{m} = (x - 1) \cap k[x^2 - 1] = (x^2 - 1)$ since $(x^2 - 1) \subseteq (x - 1)$ in B , and the localization of A with respect to \mathfrak{m} is itself, since the complement of \mathfrak{m} is just k . But $1/(x + 1) \in B_{\mathfrak{n}}$ will not satisfy any monic polynomials with coefficients in A , since $1/(x + 1)$ never kills $x^2 - 1$. \square

Exercise 9.1.5. Let $A \subseteq B$ be rings, B integral over A .

(1) If $x \in A$ is a unit in B , then it is a unit in A .

(2) The Jacobson radical of A is the contraction of the Jacobson radical of B .

Proof. For (1). For $x \in A$, if x is a unit in B , that is there exists $y \in B$ such that $xy = 1$. But B is integral over A , which implies there exists $a_0, \dots, a_{n-1} \in A$ such that

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1y + a_0 = 0$$

So multiply x^n on each side we obtain

$$1 + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n = 0$$

so we have

$$-x(a_{n-1} + \cdots + a_0x^{n-1}) = 1$$

that is x is a unit in A .

For (2). Note that if B is integral over A , then for every maximal ideal \mathfrak{m} of B , we have $\mathfrak{m} \cap A$ is an maximal ideal of A . Furthermore, every prime ideal of A is contracted, so in particular, every maximal ideal of A can be written as $\mathfrak{m} \cap A$ where \mathfrak{m} is a maximal ideal of B . So it's clear to see

$$\mathfrak{R}_B \cap A = \bigcap (\mathfrak{m} \cap A) = \mathfrak{R}_A$$

where intersection runs over all maximal ideals of B . \square

Exercise 9.1.6. Let B_1, \dots, B_n be integral A -algebras. Show that $\prod_{i=1}^n B_i$ is an integral A -algebra.

Proof. Firstly, let $\varphi_i: A \rightarrow B_i$ be the homomorphism making B_i into A -algebra, thus consider $\prod_{i=1}^n \varphi_i: A \rightarrow \prod_{i=1}^n B_i$, which makes $\prod_{i=1}^n B_i$ into an A -algebra. Now it suffices to show B is an integral A -algebra. Choose an element $b = (b_1, \dots, b_n) \in \prod_{i=1}^n B_i$, then for each b_i we have a polynomial with coefficients in $f_i(A)$, denoted by f_i , then consider

$$f(x_1, \dots, x_n) := \left(\prod_{i=1}^n f_i(x_1), \dots, \prod_{i=1}^n f_i(x_n) \right)$$

it's clear $f(b) = 0$, this completes the proof. \square

Exercise 9.1.7. Let A be a subring of a ring B , such that the set $B \setminus A$ is closed under multiplication. Show that A is integrally closed in B .

Proof. Let $b \in B$ which is integral over A , then it satisfies a monic polynomial, that is

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

where $a_i \in A$. Note that $b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) \in A$, thus if $b \notin A$, then we have $b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1 \in A$, since $B \setminus A$ is multiplicative closed. Repeat above process one has $b + a_1 \in A$, which implies $b \in A$, a contradiction. \square

Exercise 9.1.8. Show the following statements:

- (1) Let A be a subring of an integral domain B , and let C be the integral closure of A in B . Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Then f, g are in $C[x]$.
- (2) Prove the same result without assuming that B or A is an integral domain.

Proof. For (1). Take a field containing B in which the polynomials f, g split into linear factors: say $f = \prod (x - \xi_i), g = \prod (x - \eta_j)$. Each ξ_i and each η_j is a root of fg , and $fg \in C[x]$, one has ξ_i and η_j is integral over C . By Vieta's formula one has coefficients of f and g are still integral over C , since C is a ring. Furthermore, $f, g \in C[x]$, since C is integrally closed in B . \square

Exercise 9.1.9. Let A be a subring of a ring B and let C be the integral closure of A in B . Prove that $C[x]$ is the integral closure of $A[x]$ in $B[x]$.

Proof. If $f \in B[x]$ is integral over $A[x]$, then there exists some $g_i \in A[x]$ such that

$$f^m + g_1 f^{m-1} + \cdots + g_m = 0$$

Consider integer r satisfies the following conditions

- (1) r is larger than m and the degrees of g_1, \dots, g_m .
- (2) If we set $f_1 = f - x^r$, then

Note that in other words (2) is to say

$$f_1^m + h_1 f_1^{m-1} + \cdots + h_m = 0$$

where $h_m = (x^r)^m + g_1(x^r)^{m-1} + \cdots + g_m \in A[x]$. Now apply Exercise 5.5.8 to the polynomials f_1 and $f_1^{m-1} + h_1 f_1^{m-2} + \cdots + h_{m-1}$ to conclude $f_1 \in C[x]$, so is f . \square

9.2. Exercise12-13 in Chapter five of Atiyah-MacDonald.

Exercise 9.2.1. Let G be a finite group of automorphisms of a ring A , and let A^G denote the subring of G -invariants, that is of all $x \in A$ such that $\sigma(x) = x$ for all $\sigma \in G$. Prove that A is integral over A^G .

Let S be a multiplicative closed subset of A such that $\sigma(S) \subseteq S$ for all $\sigma \in G$, and let $S^G = S \cap A^G$. Show that the action of G on A extends to an action on $S^{-1}A$, and that $(S^G)^{-1}A^G \cong (S^{-1}A)^G$.

Proof. It's easy to see A^G is a subring of A . To see A is integral over A^G , we pick any $a \in A$ and consider the polynomials $f(x) = \prod_{\sigma \in G} (x - \sigma(a))$. Then a is a root of $f(x)$ and $f(x) \in A^G[x]$.

For any $a/b \in S^{-1}A$ and $\sigma \in G$, we define $\sigma(a/s) := \sigma(a)/\sigma(s)$. Now we need to check the following things to show G acts on $S^{-1}A$.

- (1) If $a/s = b/t \in S^{-1}A$, then there exists $u \in S$ such that $uta = usb \in A$, then

$$\sigma(u)\sigma(t)\sigma(a) = \sigma(u)\sigma(s)\sigma(b).$$

This means $\sigma(a)/\sigma(s) = \sigma(b)/\sigma(t) \in S^{-1}A$.

- (2) It's additive, that is,

$$\sigma\left(\frac{a}{s} + \frac{b}{t}\right) = \sigma\left(\frac{at + bs}{st}\right) = \frac{\sigma(a)\sigma(t) + \sigma(b)\sigma(s)}{\sigma(s)\sigma(t)} = \sigma\left(\frac{a}{s}\right) + \sigma\left(\frac{b}{t}\right).$$

- (3) For $\sigma_1, \sigma_2 \in G$, we have

$$\sigma_1\left(\sigma_2\left(\frac{s}{t}\right)\right) = \sigma_1\sigma_2\left(\frac{s}{t}\right).$$

Now let's prove $(S^G)^{-1}A^G \cong (S^{-1}A)^G$. For $a \in A^G$ and any $\sigma \in G$, we have $\sigma(a/1) = \sigma(a)/1 = a/1$. Then the natural inclusion $A^G \hookrightarrow A \rightarrow S^{-1}A$ factors through $A^G \rightarrow (S^{-1}A)^G \hookrightarrow S^{-1}A$. Moreover, for any element $s \in S^G$, one has s is sent to unit in $(S^{-1}A)^G$. Then by the universal property of localization, there is a unique morphism from $(S^G)^{-1}A^G \rightarrow (S^{-1}A)^G$, which is given by $a/s \mapsto a/s$. Now it suffices to show this morphism is bijective.

- (1) If $a/s = 0 \in (S^{-1}A)^G$, then there exists some $t \in S$ such that $ta = 0$. Then take $t' = \prod_{\sigma \in G} \sigma(t)$, we have $t' \in S^G$ and $t'a = 0$. This shows $a/s = 0 \in (S^G)^{-1}A^G$.

(2) If $a/s \in (S^{-1}A)^G$,

□

Exercise 9.2.2. In the setting of Exercise 9.2.1, let \mathfrak{p} be a prime ideal of A^G , and let P be the set of prime ideals of A whose contraction is \mathfrak{p} . Show that G acts transitively on P . In particular, P is finite.

Proof. Firstly, an easy observation is that G acts on P . Let $\mathfrak{p}_1, \mathfrak{p}_2$ be prime ideals in P . For any $x \in \mathfrak{p}_1$, note that $\prod_{\sigma \in G} \sigma(x) \in \mathfrak{p}_1$. Then we have

$$\prod_{\sigma \in G} \sigma(x) \in \mathfrak{p}_1 \cap A^G = \mathfrak{p} = \mathfrak{p}_2 \cap A^G \subseteq \mathfrak{p}_2.$$

This shows for some $\sigma \in G$, one has $\sigma(x) \in \mathfrak{p}_2$. Since x is arbitrary, one has $\mathfrak{p}_1 \subseteq \prod_{\sigma \in G} \sigma(\mathfrak{p}_2)$, but since all these $\sigma(\mathfrak{p}_2)$ are prime ideals, there exists some $\sigma \in G$ such that $\mathfrak{p}_1 \subseteq \sigma(\mathfrak{p}_2)$. By Exercise 9.2.1 we have A is integral over A^G , and thus $\mathfrak{p}_1 = \sigma(\mathfrak{p}_2)$. This shows G acts on P transitively. □

9.3. Exercise 28-31 in Chapter five of Atiyah-MacDonald.

Exercise 9.3.1. Let A be an integral domain, K its field of fractions. Show that the followir equivalent:

- (1) A is a valuation ring of K ;
- (2) If $\mathfrak{a}, \mathfrak{b}$ are any two ideals of A , then either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$.

Deduce that if A is a valuation ring and \mathfrak{p} is a prime ideal of A , then $A_{\mathfrak{p}}$ and A/\mathfrak{p} are valuation rings of their fields of fractions.

Proof. (1) to (2). Suppose there exist two ideals $\mathfrak{a}, \mathfrak{b}$ such that $\mathfrak{a} \not\subseteq \mathfrak{b}$ and $\mathfrak{b} \not\subseteq \mathfrak{a}$. Then we pick $0 \neq a \in \mathfrak{a}$ and $0 \neq b \in \mathfrak{b}$ such that $a \notin \mathfrak{b}$ and $b \notin \mathfrak{a}$. For $0 \neq a/b \in K$, the definition of valuation ring, we may assume $a/b \in A$, but it will imply $(a/b) \cdot b = a \in \mathfrak{b}$, a contradiction.

(2) to (1). Let $0 \neq a/b \in K$, consider ideals $(a), (b) \in \mathfrak{A}$. Then by assumption we may assume $(a) \subseteq (b)$. In particular, we have $a/b \in A$, and thus A is a valuation ring of K .

In particular, if A is a valuation ring and \mathfrak{p} is a prime ideal of A , then both $A_{\mathfrak{p}}$ and A/\mathfrak{p} is a valuation ring of their fraction fields, since the inclusion order on $A_{\mathfrak{p}}$ and A/\mathfrak{p} is inherited from A . □

Exercise 9.3.2. Let A be a valuation ring of a field K . Show that every subring of K which contains A is a local ring of A , that is, a localization of A with respect to some prime ideal.

Proof. Suppose $B \subseteq K$ is a subring which contains A . Since A is a valuation ring, one has B is also a valuation ring, and thus a local ring. Suppose \mathfrak{n} is the maximal ideal of B and $\mathfrak{p} = \mathfrak{n} \cap A$. Now we're going to show $B = A_{\mathfrak{p}}$. For any $a/b \in A_{\mathfrak{p}}$, we have $b \in A \setminus \mathfrak{p}$ and thus $b \notin \mathfrak{n}$, which implies b is a unit in B . In particular, $a/b \in B$.

Conversely, since $A_{\mathfrak{p}} \subseteq K$ is a valuation ring, we have it's a maximal element under inclusion order of local rings of K . As a consequence, we should have $B \subseteq A_{\mathfrak{p}}$, and thus $B = A_{\mathfrak{p}}$. □

Exercise 9.3.3. Let A be a valuation ring of a field K . The group U of units of A is a subgroup of the multiplicative group K^* of K . Let $\Gamma = K^*/U$. If $\xi, \eta \in \Gamma$ are represented by $x, y \in K$, define $\xi \geq \eta$ to mean $xy^{-1} \in A$.

Show that this defines a total ordering on Γ which is compatible with the group structure (i.e., $\xi \geq \eta \Rightarrow \xi\omega \geq \eta\omega$ for all $\omega \in \Gamma$). In other words, Γ is a totally ordered abelian group. It is called the value group of A .

Let $v: K^* \rightarrow \Gamma$ be the canonical homomorphism. Show that $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K^*$.

Proof. Firstly, we need to show that relation \leq is well-defined on Γ . If $\xi \in \Gamma$ is represented by x, x' and $\eta \in \Gamma$ is represented by y, y' , then we need to prove $\xi \geq \eta$ does not depend on the choice of representatives. Since both x, x' present ξ , so we have $x'x^{-1} \in U$, and by the same reason we have $y'y^{-1} \in U$. If $xy^{-1} \in U$, then

$$x'(y')^{-1} = x'x^{-1}xy^{-1}y(y')^{-1} \in UAU = A.$$

This shows the well-defineness. Now let's prove \leq gives a totally ordered on Γ .

- (1) For $\xi \in \Gamma$ which is represented by $x \in K^*$, one has $xx^{-1} = 1 \in A$, which implies $\xi \geq \xi$.
- (2) For $\xi, \eta \in \Gamma$ which are represented by $x, y \in K^*$ such that $\xi \geq \eta$ and $\eta \geq \xi$, one has $xy^{-1} \in A$ and $y^{-1}x \in A$. This shows xy^{-1} is invertible and thus $xy^{-1} \in U$, which implies $\xi = \eta$.
- (3) For $\xi, \eta, \gamma \in \Gamma$ which are represented by $x, y, z \in K^*$, if $\xi \geq \eta$ and $\eta \geq \gamma$, then $xy^{-1} \in A$ and $yz^{-1} \in A$, and thus $xz^{-1} \in A$, which implies $\xi \geq \gamma$.

Finally we're going to show this total order is compatible with the group structure on Γ . For $\xi, \eta, \gamma \in \Gamma$ which are represented by $x, y, z \in K^*$. If $\xi \geq \eta$, then $xy^{-1} \in A$, and thus

$$xy^{-1} = xww^{-1}y^{-1} = (xw)(yw)^{-1} \in A,$$

which implies $\xi\gamma \geq \eta\gamma$.

Let $v: K^* \rightarrow \Gamma$ be the canonical morphism. For $x, y \in K^*$ with $v(x) \geq v(y)$, then $xy^{-1} \in A$, and thus

$$(x+y)y^{-1} = xy^{-1} + 1 \in A.$$

This shows $v(x+y) \geq v(y)$. □

Exercise 9.3.4. Conversely, let Γ be a totally ordered abelian group (written additively), and let K be a field. A valuation of K with values in Γ is a mapping $v: K^* \rightarrow \Gamma$ such that

- (1) $v(xy) = v(x) + v(y)$,
- (2) $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K^*$.

Show that the set of elements $x \in K^*$ such that $v(x) \geq 0$ together with 0 is a valuation ring of K . This ring is called the valuation ring of v , and the subgroup $v(K^*)$ of Γ is the value group of v . Thus the concepts of valuation ring and valuation are essentially equivalent.

Proof. For convenient, we denote

$$A = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}.$$

A routine check shows that A is a subring of K . Note that $v(1) = v(1) + v(1)$ implies $v(1) = 0$. Then for any $x \in K^*$, we must have either $v(x) \geq 0$ or $v(x) \leq 0$, since $v(x) + v(x^{-1}) = 0$. Thus for any $x \in K^*$, we have $x \in A$ or $x^{-1} \in A$. This shows A is a valuation ring of K . \square

10. WEEK-12

- 10.1. **Exercise27 in Chapter 5 of Atiyah-MacDonald.**
- 10.2. **Exercise1-7 in Chapter 6 of Atiyah-MacDonald.**
- 10.3. **Exercise1/2/4 in Chapter 7 of Atiyah-MacDonald.**

REFERENCES

- [AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley-Longman, 1969.

YAU MATHEMATICAL SCIENCES CENTER, TSINGHUA UNIVERSITY, BEIJING, 100084, P.R. CHINA,

Email address: liubw22@mails.tsinghua.edu.cn