1 Rings and Ideals

Exercise 1.12. $(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$

i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$

ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$

iii) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$

iv) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$

v) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$

Solution. Trivial. □

Exercise 1.13. $r(\mathfrak{a}) = \{x \in A : \exists n, x^n \in \mathfrak{a}\}$

i) $r(\mathfrak{a}) \supseteq \mathfrak{a}$

ii) $r(r(\mathfrak{a})) = r(\mathfrak{a})$

iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

iv) $r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$

v) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

vi) if $\mathfrak{p}$ is a prime, $r(\mathfrak{p}^n) = \mathfrak{p}$ forall $n > 0$.

Solution. i) ii) Trivial.

iii) Suppose $x^n \in \mathfrak{a}, x^m \in \mathfrak{b}$, then $x^{n+m} \in \mathfrak{a}\mathfrak{b}$, so $r(\mathfrak{a}) \cap r(\mathfrak{b}) \subseteq r(\mathfrak{a}\mathfrak{b})$. Obviously $r(\mathfrak{a}\mathfrak{b}) \subseteq r(\mathfrak{a} \cap \mathfrak{b}) \subseteq r(\mathfrak{a}) \cap r(\mathfrak{b})$.

iv) $1 = 1^n \in \mathfrak{a}$, hence $\mathfrak{a} = (1)$.

v) If $x^n = u + v, u^m \in \mathfrak{a}, v^l \in \mathfrak{b}$, then by binomal theorem $x^{n(m+l-1)}$ can be written in sums of $u^a v^b$ where $a \geq m$ or $b \geq l$, hence $u^a v^b \in \mathfrak{a} + \mathfrak{b}$, and $x^{n(m+l-1)} \in \mathfrak{a} + \mathfrak{b}$.

vi) By iii), we have $r(\mathfrak{a}^n) = r(\mathfrak{a})$ for any $n > 0$; so by $r(\mathfrak{p}) = \mathfrak{p}$ we have $r(\mathfrak{p}^n) = \mathfrak{p}$. □

Exercises 1.1. Sum of a nilpotent and a unit is a unit.

Solution. If $x^n = 0$ then $(1 + x)(1 - x + x^2 - x^3 + ... + (-1)^{n-1}x^{n-1}) = 1$, so $1 + x$ is a unit. If a is a unit and x is a nilpotent, then $a^{-1}x$ is a nilpotent, hence $a + x = a(1 + a^{-1}x)$ is a unit. □

Exercises 1.2. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove:

i) f is a unit in $A[x] \iff a_0$ is a unit in $A[x]$, and $a_1, \ldots, a_n$ are nilpotent.

ii) f is nilpotent $\iff a_0, \ldots, a_n$ are nilpotent.

iii) f is a zero-divisior $\iff$ there exists $a \neq 0 \in A$ such that $af = 0$.

iv) f is said *primitive* if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that fg is primitive $\iff$ f and g are both primitive.

Solution.

i) $\Longrightarrow$: Suppose $g = b_0 + b_1x + \cdots + b_mx^m$ such that $fg = 1$, then $a_0b_0 = 1$ hence a_0, b_0 are both units. We Prove $a_n^{r+1}b_{m-r} = 0$ for all $0 \le r \le m$ by induction on r.

If this is true for all $r' < r$, consider the $(n + m - r)$-th coefficient of fg, we have $0 = \sum_{i=0}^{r} a_{n-r+i}b_{m-i}$, so $a_nb_{m-r} = \sum_{i=0}^{r-1} a_{n-r+i}b_{m-i}$. Multiply a_n^r to both side, then by induction hypothesis we get $a_n^{r+1}b_{m-r} = 0$.

In partial, $a_n^{m+1}b_0 = 0$, hence a_n is nilpotent, and so is a_nx^n. By Ex.1.1, $f - a_nx^n$ is a unit, so repeat the proof above we have $a_1, \ldots, a_n$ are nilpotent.

$\Longleftarrow$: Repeat Ex.1.1 for n times.

ii) $\Longrightarrow$ If $f^k = 0$, then consider nk-th coefficient of f^k we have $a_n^k = 0$. Then $f - a_nx^n$ is also nilpotent, hence $a_0, a_1, \ldots, a_n$ are all nilpotent.

$\Longleftarrow$: f is sums of n nilpotents, also a nilpotent.

iii) $\Longrightarrow$: Choose $g = b_0 + b_1x + \cdots + b_mx^m$ of least degree m such that $fg = 0$, then $a_nb_m = 0$, so a_ng is of at most degree $m - 1$. But $a_ngf = 0$, by the choice of g we have $a_ng = 0$. Then we prove $a_{n-r}g = 0$ by induction on r. For $r = 1$ it's proved above, and if it is true for $0, 1, \ldots, r - 1$, then we have $a_{n-r}b_m = 0$, so similarly $a_{n-r}g = 0$. So we have $b_mf = 0$.

$\Longleftarrow$: Trivial.

iv) $\Longrightarrow$: if all coefficients of f are in an ideal $\mathfrak{a} \neq (1)$, then obviously all coefficients of fg are also in $\mathfrak{a}$, so fg is not primitive.

$\Longleftarrow$ Left $f = a_0+a_1x+\cdots+a_nx^n$ and $g = b_0+b_1x+\cdots+b_mx^m$ both primitive. Suppose $fg = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ is not primitive, that is, $(c_0, c_1, \ldots, c_{n+m}) = \mathfrak{c} \neq (1)$. Let $\mathfrak{p}$ be a prime ideal contains $\mathfrak{c}$, and let i, j be the least number that $a_i \notin \mathfrak{p}, b_j \notin \mathfrak{p}$ (cause f, g are primitive, these number exist), then $a_ib_j = c_{i+j} - \sum_{k=0}^{i-1} a_ib_{i+j-k} - \sum_{k=0}^{j-1} a_{i+j-k}b_k \in \mathfrak{p}$, contradiction.

□

Exercises 1.3. Generate results in Ex.1.2 to a ring $A[x_1, x_2, \ldots, x_n]$ with several indeterminates.

Solution. Just consider $A[x_1, x_2, \ldots, x_n]$ as a polynomial ring over $A[x_1, x_2, \ldots, x_{n-1}]$. Repeat the proof above, we have: if $f, g \in A[x_1, x_2, \ldots, x_n]$, then

i) f is a unit $\iff$ the constant term of f is a unit, all other coefficients are nilpotent.

ii) f is nilpotent $\iff$ all coefficients of f are nilpotent.

iii) f is a zero-divisior $\iff$ there exists $a \neq 0 \in A$ such that $af = 0$

iv) fg is primitive $\iff$ f, g are both primitive.

□

Exercises 1.4. In the ring $A[x]$, the Jacobson radical is equal to nilradical.

Solution. Let $f \in A[x]$ belong to Jacobson radical, then for all $g \in A[x]$, $1 - fg$ is a unit. In particular, $1 - xf$ is a unit, hence any coefficient of f is nilpotent, and f is nilpotent, i.e. f belongs to nilradical of $A[x]$. □

Exercises 1.5. Let $A[[x]]$ be the ring former power series over A, and let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$. Show that

i) f is a unit of $A[[x]]$ $\iff$ a_0 is a unit of A.

ii) If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. *Is the converse true? (See Chapter 7,Exercise 2.)*

iii) f belongs to Jacabson radical of $A[[x]]$ $\iff$ a_0 belongs to Jacabson radical of A.

iv) 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.

v) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Solution.

i) $\Longrightarrow$: Trivial.

$\Longleftarrow$: Let $g = \sum_{n=0}^{\infty} b_n x^n$ where $b_0 = a_0^{-1}, b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i}$, then $gf = 1$, so f is a unit.

ii) Induction on n. if $a_0, \dots, a_{n-1}$ is nilpotent, then so is $f_n = \sum_{m=0}^{\infty} a_{n+m} x^m$ (Cause $f - a_0 - a_1 x - \cdots - a_{n-1} x^{n-1} = x^n f_n$). So there exists k such that $f_n^k = 0$, hence $a_n^k = 0$.

iii) Suppose f belongs to Jacabson radical of $A[[x]]$, then for all g, $1 - fg$ is a unit. In particalur for all $b \in A$, $1 - bf$ is a unit, so by i) $1 - a_0 b$ is a unit, so a_0 belongs to Jacabson radical of A; and vice versa.

iv) If $\mathfrak{m}^c \subseteq \mathfrak{a} \neq (1)$, then $\mathfrak{a} + (x)$ is a ideal of $A[[x]]$, which contains all series of constant term $\in \mathfrak{a}$, so $\mathfrak{a} + (x) \supset \mathfrak{m}$, hence $\mathfrak{a} + (x) = \mathfrak{m}$ and $\mathfrak{a} = \mathfrak{m}^c$.

v) Let $\mathfrak{p}$ be a prime ideal of A, then $\mathfrak{p}$ is the contraction of $\mathfrak{p} + (x)$. So it is sufficient to prove $\mathfrak{p} + (x)$ is a prime ideal of $A[[x]]$.

If $f = \sum_{n=0}^{\infty} a_n x^n, g = \sum_{n=0}^{\infty} b_n x^n$, and $fg \in \mathfrak{p} + (x)$, i.e. $a_0 b_0 \in \mathfrak{p}$, then either a_0 or b_0 belongs to $\mathfrak{p}$. So either f or g belongs to $\mathfrak{p} + (x)$, hence $\mathfrak{p} + (x)$ is a prime ideal of $A[[x]]$.

□

Exercises 1.6. Let A be a ring 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.

Solution. If the Jacobson radical is not contained in the nilradical, then there exists a nonzero idempotent e belongs to the Jacobson radical, so $1 - e = 1 - 1e$ is a unit. but $e^2 = e$, hence $(1 - e)e = 0$, so $e = 0$, contradiction. $\square$

Exercises 1.7. Let A be a ring in which every element x satifies $x^n = x$ for some $n > 1$. Show that every prime ideal of A is maximal.

Solution. Let $\mathfrak{p}$ be a prime ideal, then we have $A/\mathfrak{p}$ is a intergal domain, and for all $\bar{x}$ there exists $n > 1$ such that $\bar{x}^n = \bar{x}$, hence $(\bar{x}^{n-1} - 1)\bar{x} = 0$. If $\bar{x} \neq 0$, then $\bar{x}^{n-1} - 1 = 0$, so $\bar{x}$ is a unit. Hence $A/\mathfrak{p}$ is a field, and $\mathfrak{p}$ is maximal. $\square$

Exercises 1.8. Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with repect to inclusion.

Solution. Forall chains of prime ideals $\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots$, if we let $\mathfrak{p} = \bigcap_{n=1}^{\infty} \mathfrak{p}_n$, then $\mathfrak{p}$ is an ideal. Suppose $xy \in \mathfrak{p}$, then for all n we have $xy \in \mathfrak{p}_n$, hence either x or y belongs to $\mathfrak{p}_n$, so at least one of them belongs to infinite $\mathfrak{p}_n$, hence belongs to all $\mathfrak{p}_n$, i.e. either x or y belongs to $\mathfrak{p}$. So all chains of prime ideals of A has a lower bound, so by Zorn's Lemma there exists a minimal elements along them. $\square$

Exercises 1.9. Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \iff \mathfrak{a}$ is an intersection of prime ideals.

Solution. $\Longrightarrow$: Let $\mathfrak{b}$ be the intersection of all prime ideals containing $\mathfrak{a}$. If $x \in \mathfrak{b}$, then in $A/\mathfrak{a}$, $\bar{x}$ belongs to all prime ideals, so $\bar{x}^n = 0$ for some $n > 0$, i.e. $x \in r(\mathfrak{a}) = \mathfrak{a}$. so $\mathfrak{a} = \mathfrak{b}$ is a intersection of prime ideals.

$\Longleftarrow$: If $\mathfrak{a} = \bigcap_\alpha \mathfrak{p}_\alpha$, then $r(\mathfrak{a}) = \bigcap_\alpha r(\mathfrak{p}_\alpha) = \bigcap_\alpha \mathfrak{p}_\alpha = \mathfrak{a}$. $\square$

Exercises 1.10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following are equivalent:

i) A has exactly one prime ideal.

ii) every element of A is either a unit ot nilpotent.

iii) $A/\mathfrak{N}$ is a field.

Solution. i) $\Longrightarrow$ ii): If $a \notin \mathfrak{N}$ is not a unit, then there exists a prime ideal $\mathfrak{p}$ containing a, so $\mathfrak{p}$ is the onlyprime ideal. But then $\mathfrak{N} = \mathfrak{p}$, contradiction.

ii) $\Longrightarrow$ iii): Every elements $\notin \mathfrak{N}$ is a unit, so every elements of $A/\mathfrak{N}$ is a unit, therefore $A/\mathfrak{N}$ is a field.

iii) $\Longrightarrow$ i): $\mathfrak{N}$ is a maximal ideal and the intersection of all prime ideals. So the only prime ideal of A is $\mathfrak{N}$ itself. $\square$

Exercises 1.11. A ring A is *Boolean* if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that

i) $2x = 0$ for all $x \in A$.

ii) every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements.

iii) every finitely generated ideal in A is principal.

Solution. i) $x + 1 = (x+1)^2 = x^2 + 2x + 1 = 3x + 1$, so $2x = 0$ for all $x \in A$.

ii) Suppose $x \notin \mathfrak{p}$. By $x(1-x) = x - x^2 = 0 \in \mathfrak{p}$ we have $1 - x \in \mathfrak{p}$. So $A = \mathfrak{p} \cup (1 - \mathfrak{p})$, and $A/\mathfrak{p}$ only contains two elements, hence is a field, and $\mathfrak{p}$ is maximal.

iii) For any $a_1, a_2, \ldots, a_n \in A$, let $a = 1 - \prod_{i=1}^{n}(1-a_i)$, then $a_i a = a_i - a_i(1-a_i)\prod = a_i$, so $(a_1, a_2, \ldots, a_n) = (a)$.

□

Exercises 1.12. A local ring contains no idempotent $\neq 0, 1$.

Solution. Let $\mathfrak{m}$ be the only maximal ideal of A. For any idempotent e, if e is a unit then $e = e^{-1}e^2 = e^{-1}e = 1$. If e is not unit, then $e \in \mathfrak{m} = \mathfrak{R}$ (the Jacabson radical of A), so $1 - e$ is a unit. but $(1-e)^2 = 1 - 2e + e^2 = 1 - e$ is also idempotent, so $1 - e = 1$, therefore $e = 0$. □

Exercises 1.13. K field, Σ the set of all irreducible monic polynomials f of one indeterminate with coefficients in K. Let A be the polynomial ring over K generated bt indeterminates x_f, one for each $f \in \Sigma$. Let $\mathfrak{a}$ be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $\mathfrak{a} \neq (1)$.

Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$, and let $K_1 = A/\mathfrak{m}$. Then $K_1$is an extension field of K in which each $f \in \Sigma$ has a root. Repeat the construction with K_1 in place of K, obtaining a field K_2, and so on. Let $L = \bigcup_{n=1}^{\infty} K_n$, Then L is a field in which each $f \in \Sigma$ splits completely into linear factors. Let $\bar{K}$ be the set of all elements of L which are algebraic over K. Then $\bar{K}$ is an algebraic closure of K.

Solution. Let $1 \in \mathfrak{a}$, then 1 can be written in a finite sum of finite products of $f(x_f)$-s. Choose one form containing least f-s, suppose it contains $a_1 = f_1(x_{f_1}), a_2 = f_2(x_{f_2}), \ldots, a_n = f_n(x_{f_n})$. then $(a_1, a_2, \ldots, a_{n-1}) \neq (1)$ but $(a_1, a_2, \ldots, a_{n-1}) + (a_n) = (1)$.

Hence $(a_1, a_2, \ldots, a_{n-1})(a_n) = (a_1, a_2, \ldots, a_{n-1}) \cap (a_n)$, so $a_n \in (a_1, a_2, \ldots, a_{n-1})(a_n)$, i.e. exists $b \in (a_1, a_2, \ldots, a_{n-1})$ such that $ba_n = a_n$. Obviously A is an intergal domain, so $b = 1$; but then $(a_1, a_2, \ldots, a_{n-1}) = (1)$, contradiction.

If $f \in \Sigma$, then $f(x_f) \in \mathfrak{a}$, so $f(\bar{x_f}) = 0$ in $K_1 = A/\mathfrak{m}$, and f can be written as $f(x) = (x - x_f)f_1(x)$. Repeat this progress then in $K_{\deg(f)}$, f splits into linear factors. □

Exercises 1.14. In a ring a, let Σ be all ideals in which every element is a zero-divisior. Show that the set Σ has maximal elements, and every maximal element of Σ is a prime ideal. Hence the set of zero-divisiors in A is a union of prime ideals.

Solution. For every chain in Σ $\{\mathfrak{a}_\alpha\}_\alpha$, it has a upperbound $\bigcup_\alpha \mathfrak{a}_\alpha$. So by Zorn's Lemma Σ has maximal elements.

Suppose $\mathfrak{m}$ is a maximal element of Σ, and $xy \in \mathfrak{m}$. Consider $\mathfrak{m} + (x)$ and $\mathfrak{m} + (y)$. If neither belongs to Σ, then there exists $a, b \in \mathfrak{m}, u, v \in A$ such that $a + ux, b + vy$ are both not zero-divisior. But $(a+ux)(b+vy) \in \mathfrak{m}$ is a zero-divisior, contradiction. So at least one of $\mathfrak{m}+(x), \mathfrak{m}+(y)$ belongs to Σ, i.e. $x \in \mathfrak{m}$ or $y \in \mathfrak{m}$. □

Exercises 1.15. Let A be a ring and let X be the set of all prime ideals of A. For eah subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

i) if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

ii) $V(0) = X, V(1) = \varnothing$.

iii) if $(E_i)_{i\in I}$ is any family of subsets of A, then

$$V\left(\bigcup_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i)$$

iv) $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$.

Solution.

i) If $E \subseteq \mathfrak{p}$ then also is $\mathfrak{a} = (E)$. If $\mathfrak{a} \subseteq \mathfrak{p}$ and $x^n \in \mathfrak{a} \subseteq \mathfrak{p}$ then by definition $x \in \mathfrak{p}$, so $r(\mathfrak{a}) \subseteq \mathfrak{p}$. The inverse is trivial.

ii) Trivial.

iii) Trivial.

iv) If $\mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{p}$ then $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$. So $V(\mathfrak{a}\cap\mathfrak{p}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. $\supseteq$-s are triival.

□

Exercises 1.16. Draw pictures of $\mathtt{Spec}(\mathbb{Z}), \mathtt{Spec}(\mathbb{R}), \mathtt{Spec}(\mathbb{C}[x]), \mathtt{Spec}(\mathbb{R}[x]), \mathtt{Spec}(\mathbb{Z}[x])$.

Solution.

i) In $\mathtt{Spec}(\mathbb{Z})$ there is countable infinite closed points (p_i), and a generic point 0.

ii) Cause R is a field, it have only one prime ideal 0. So $\mathtt{Spec}(\mathbb{R})$ is a trivial topology space with only one point.

iii) In $\mathbb{C}[x]$ a prime ideal is 0 or $(x-z)$ with $z \in \mathbb{C}$, it's similar to $\mathtt{Spec}(\mathbb{Z})$ but with uncountable infinite points.

iv) In $\mathbb{R}[x]$ a prime ideal is $0, (x-r)$ or (x^2+px+q) with $p^2-4q < 0$, actually it's isomorphic to $\mathtt{Spec}(\mathbb{C}[x])$

v) In $\mathbb{Z}[x]$ there are three sorts of prime ideals: 0 or (p); $(F(x))$ where F is a irreducible polynomial over $\mathbb{Z}[x]$ (or equivalentlly irreducible polynomial over $\mathbb{Q}[x]$); $(p, F(x))$ where $F(x)$ is a monic irreducible polynomial over $\mathbb{Z}/p\mathbb{Z}$. For the Zariski topology, there is a closed base of it: $\{(p, F(x)) | F(x) \text{ irreducible over } \mathbb{Z}_p[x]\}$ for all p; $\{(p, G(x)) | G(x) \text{ divides } F(x) \text{ over } \mathbb{Z}_p[x]\} \cup \{(F(x))\}$ for all irreducible $F(x) \in \mathbb{Z}[x]$; $\{(p, F(x))\}$ for all $F(x)$ irreducible over $\mathbb{Z}_p[x]$.

$\square$

Exercises 1.17. For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \texttt{Spec}(A)$. The sets X_f are open. Show that they form a basis of the Zariski topology, and that

i) $X_f \cap X_g = X_{fg}$.

ii) $X_f = \varnothing \iff f$ is nilpotent.

iii) $X_f = X \iff f$ is a unit.

iv) $X_f = X_g \iff r((f)) = r((g))$.

v) X is quasi-compact (every open covering of X has a finite sub-covering)

vi) More generating, each X_f is quasi-compact.

vii) An open subset of X is quasi-compact if and only if it is a finite union of sets X_f.

The sets X_f are called basic open sets of $X = \texttt{Spec}(A)$.