C_A - 08 MA-312 Commutative Algebra / Jan-Apr 2008

Lectures : Monday/Thursday 11:30–1:00 ; Lecture Hall-II, Department of Mathematics

1. Ideals — Operation on Ideals

Wolfgang Krull (1899-1971) †

All rings we consider in this course are commutative with an identity element, called the *unity*. For a ring A, let $\mathcal{I}_A$ denote the set of ideals in A.

1.1. (Operations on ideals) Let A be a ring and let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathcal{I}_A$.

1). (Sums, Products and Intersections) **a).** The operations sum, intersection and product on $\mathcal{I}_A$ are commutative and associative.

b). (Distributive law) $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$. (**Remark :** In the ring $\mathbb{Z}$ the operations $\cap$ and $+$ are distributive over each other. This is not the case for general rings.)

c). (Modular law) If $\mathfrak{a} \supseteq \mathfrak{b}$ or $\mathfrak{a} \supseteq \mathfrak{c}$, then $\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$.

d). $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$. (**Remark :** In the ring $\mathbb{Z}$ the equality $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ holds.)

e). $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Further, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ if $\mathfrak{a}+\mathfrak{b} = A$.

f). (Comaximal ideals) Two ideals $\mathfrak{a}, \mathfrak{b}$ are called coprime or comaximal if $\mathfrak{a}+\mathfrak{b} = A$. Therefore for coprime ideals $\mathfrak{a}, \mathfrak{b}$, we have $\mathfrak{a} \cap \mathfrak{a} = \mathfrak{a}\mathfrak{b}$.

1) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $n \geq 2$ be pairwise comaximal ideals in A, i.e. $\mathfrak{a}_i + \mathfrak{a}_j = A$ whenever $1 \leq i, j \leq n$ with $i \neq j$. Then : i) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1}$ and $\mathfrak{a}_n$ are also comaximal. ii) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

2) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$, $n, m \in \mathbb{N}$ be ideals in A with $\mathfrak{a}_i + \mathfrak{b}_j = A$ for all i, j with $1 \leq i \leq n$ and $1 \leq j \leq m$. Then the products $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ and $\mathfrak{b}_1 \cdots \mathfrak{b}_m$ are comaximal, i.e., $\mathfrak{a}_1 \cdots \mathfrak{a}_n + \mathfrak{b}_1 \cdots \mathfrak{b}_m = A$. In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal ideals in A, then the powers $\mathfrak{a}^n$ and $\mathfrak{b}^m$ are also comaximal in A for all $n, m \in \mathbb{N}$.

g). Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $n \geq 2$ be ideals in a ring A and for $i = 1, \ldots, n$, let $\pi_i : A \to A/\mathfrak{a}_i$ be the natural surjective map. Then :

1) The ring homomorphism $\pi : A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$ defined by $a \mapsto (\pi_1(a), \ldots, \pi_n(a))$ is a ring homomorphism with kernel $\operatorname{Ker} \pi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. In particular, π is injective if and only if $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = 0$.

2) (Chinese Remainder Theorem) The ring homomorphism π, in 1) above is surjective if and only if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are pairwise comaximal.

---

† **Wolfgang Krull (1899-1971)** Wolfgang Krull was born on 26 Aug 1899 in Baden-Baden, Germany and died on 12 April 1971 in Bonn, Germany.

2). (Ideal quotient) For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A, the ideal quotient of $\mathfrak{a}$ by $\mathfrak{b}$ is $(\mathfrak{a} : \mathfrak{b}) := \{a \in A \mid a\mathfrak{b} \subseteq \mathfrak{a}\}$ which is an ideal in A. In particular, $(\mathfrak{a} : \mathfrak{b})$ is $\{a \in A \mid a\mathfrak{b} = 0\}$ the annihilator of $\mathfrak{b}$ and is denoted by $\operatorname{ann}(\mathfrak{b})$. If $\mathfrak{b}$ is a principal ideal Ab, then we simply write $(\mathfrak{a} : b)$ for $(\mathfrak{a} : \mathfrak{b})$. (In the ring $A = \mathbb{Z}$, let $\mathfrak{a} = \mathbb{Z}m$, $\mathfrak{b} = \mathbb{Z}n$. Then $(\mathfrak{a} : \mathfrak{b}) = \mathbb{Z}q$, where $q = \prod_{p \text{ prime}} p^{r_p}$, $r_p := \max(v_p(m) - v_p(n), 0) = v_p(m) - \min(v_p(m) - v_p(n))$. Therefore $q = m/\gcd(m, n)$.)

For ideals $\mathfrak{a}, \mathfrak{a}_i, i \in I$, $\mathfrak{b}, \mathfrak{b}_i, i \in I$, $\mathfrak{c}$ in $\mathcal{I}_A$, we have

a). $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$. **b).** $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$. **c).** $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = \big(\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}\big)$.

d). $\big(\cap_{i\in I}\, \mathfrak{a}_i : \mathfrak{b}\big) = \cap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$. **e).** $\big(\mathfrak{a} : \sum_{i\in I} \mathfrak{b}_i\big) = \cap_{i\in I}(\mathfrak{a} : \mathfrak{b}_i)$.

3). (Radical of an ideal) For an ideal $\mathfrak{a}$ in A, the radical of $\mathfrak{a}$ is

$$\{a \in A \mid a^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}^+\}$$

which is an ideal in A and is denoted by $\mathrm{r}(\mathfrak{a})$ or $\sqrt{\mathfrak{a}}$.

a). $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. **b).** $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. **c).** $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b})} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ **d).** $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.

e). $\sqrt{\mathfrak{a}} = A$ if and only if $\mathfrak{a} = A$. **f).** If $\mathfrak{p}$ is a prime ideal in A, then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n \in \mathbb{N}^+$.

4). (Extensions and Contractions of Ideals) Let $\varphi : A \to B$ be a ring homomorphism.

For an ideal $\mathfrak{a}$ in A, the extension of $\mathfrak{a}$ in B under φ is the ideal $B\varphi(\mathfrak{a})$ generated by $\varphi(\mathfrak{a})$; (explicitly $B\varphi(\mathfrak{a}) = \{\sum_{j\subset J} b_j\varphi(a_j) \mid J \text{ is a finite set}, b_j \in B, a_j \in \mathfrak{a}\}$. — In general, $\varphi(\mathfrak{a})$ need not be an ideal in B, for example, let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the natural inclusion and $\mathfrak{a} := \mathbb{Z}n$, $n \neq 0$.)

For an ideal $\mathfrak{b}$ in B, the contraction of $\mathfrak{b}$ in A under φ is the ideal $\varphi^{-1}(\mathfrak{b})$; (This is always an ideal in A.)

For $\mathfrak{a} \in \mathcal{I}_A$ (resp. $\mathfrak{b} \in \mathcal{I}_B$) the extension $B\varphi(\mathfrak{a})$ of $\mathfrak{a}$ (resp. the contraction $\varphi^{-1}(\mathfrak{b})$ of $\mathfrak{b}$) is usually denoted by $\mathfrak{a}B$ (resp. $\mathfrak{b} \cap A$), when there is no possibility of confusion over which ring homomorphism is under discussion.

Let $\mathcal{C}_A^B \subseteq \mathcal{I}_A$ (resp. $\mathcal{E}_A^B \subseteq \mathcal{I}_B$) be the set of ideals in A which are contracted to A from B under φ (resp. the set of ideals in B which are extended to B from A under φ), i.e.

$$\mathcal{C}_A^B := \{\mathfrak{b} \cap A \mid \mathfrak{b} \in \mathcal{I}_B\} \text{ and } \mathcal{E}_A^B := \{\mathfrak{a}B \mid \mathfrak{a} \in \mathcal{I}_A\}.$$

a). The maps $\mathcal{C}_A^B \longrightarrow \mathcal{E}_A^B$, $\mathfrak{a} \mapsto \mathfrak{a}B$ and $\mathcal{E}_A^B \longrightarrow \mathcal{C}_A^B$, $\mathfrak{b} \mapsto \mathfrak{b} \cap A$ are inclusion preserving bijective maps which are inverses to each other. (**Hint**: For $\mathfrak{a} \in \mathcal{I}_A$ (resp. $\mathfrak{b} \in \mathcal{I}_B$), $\mathfrak{a} \subseteq \mathfrak{a}B \cap A$, (resp. $\mathfrak{b} \supseteq (\mathfrak{b} \cap A)B$) and hence $\mathfrak{b} \cap A = (\mathfrak{b} \cap A)B \cap A$ and $\mathfrak{a}B = \big(\mathfrak{a}B \cap A\big)B$.)

b). The set $\mathcal{C}_A^B$ is closed under intersections and radicals. Further, for ideals $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathcal{I}_B$,

(i) $(\mathfrak{b}_1 + \mathfrak{b}_2) \cap A \supseteq (\mathfrak{b}_1 \cap A) + (\mathfrak{b}_2 \cap A)$. (ii) $(\mathfrak{b}_1\mathfrak{b}_2) \cap A \supseteq (\mathfrak{b}_1 \cap A)(\mathfrak{b}_2 \cap A)$.
(iii) $(\mathfrak{b}_1 : \mathfrak{b}_2) \cap A \subseteq (\mathfrak{b}_1 \cap A) : (\mathfrak{b}_2 \cap A)$.

c). The set $\mathcal{E}_A^B$ is closed under sums and products. Further, for ideals $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2 \in \mathcal{I}_A$,

(i) $(\mathfrak{a}_1 \cap \mathfrak{a}_2)B \subseteq (\mathfrak{a}_1B) \cap (\mathfrak{a}_2B)$. (ii) $(\mathfrak{a}_1 : \mathfrak{a}_2)B \subseteq (\mathfrak{a}_1B : \mathfrak{a}_2B)$. (iii) $\sqrt{\mathfrak{a}}B \subseteq \sqrt{\mathfrak{a}B}$.

d). Suppose that φ is surjective. Then $\mathcal{C}_A^B = \{\mathfrak{a} \in \mathcal{I}_A \mid \operatorname{Ker}\varphi \subseteq \mathfrak{a}\}$ and $\mathcal{E}_A^B = \mathcal{I}_B$. In particular, the map $\{\mathfrak{a} \in \mathcal{I}_A \mid \operatorname{Ker}\varphi \subseteq \mathfrak{a}\} \to \mathcal{I}_B$, $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ is inclusion preserving bijective map with inverse $\mathfrak{b} \mapsto \mathfrak{b} \cap A$.

e). Let $\mathfrak{a}$ be an ideal in A and let $\pi : A \to A/\mathfrak{a}$ be the natural surjective map. Let $\varphi : A \to A[X]$ be the natural inclusion and let $\eta := \pi[X] : A[X] \to (A/\mathfrak{a})[X]$ be the ring homomorphsim defined by $\sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \pi(a_i)X^i$. Then:

1) $\operatorname{Ker}\eta = \mathfrak{a}A[X] = \left\{ \sum_{i=0}^{n} a_i X^i \in A[X] \mid n \in \mathbb{N}, a_i \in \mathfrak{a} \text{ for all } i = 0, \ldots, n \right\}$.
2) $\mathfrak{a}A[X] \cap A = \mathfrak{a}$. In particular, $\mathcal{C}_A^{A[X]} = \mathcal{I}_A$.
3) The rings $A[X]/\mathfrak{a}A[X]$ and $(A/\mathfrak{a})[X]$ are isomorphic.
4) For ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \in \mathcal{I}_A$ prove that $(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r)A[X] = (\mathfrak{a}_1 A[X]) \cap \cdots \cap (\mathfrak{a}_r A[X])$.

f). Extend the results of e) to the polynomial ring $A[X_1, \ldots, X_n]$.

g). Find an ideal in the polynomial ring $\mathbb{Z}[X]$ which is not extended from $\mathbb{Z}$ under the natural inclusion $\mathbb{Z} \to \mathbb{Z}[X]$, i.e. not in $\mathcal{E}_{\mathbb{Z}}^{\mathbb{Z}[X]}$.

1.2. (Prime ideals and Maximal ideals) Let A be a ring.

1). An ideal $\mathfrak{p}$ in A is called a prime ideal if $\mathfrak{p} \neq A$ and if $ab \in \mathfrak{p}$ for arbitrary elements a, b in A, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The set of all prime ideals in A is denoted by $\operatorname{Spec} A$.

a). For an ideal $\mathfrak{p}$ in A, the following statements are equivalent:

(i) $\mathfrak{p}$ is a prime ideal.
(ii) $A \setminus \mathfrak{p}$ is a multiplicatively closed set in A containing 1.
(iii) The residue class ring $A/\mathfrak{p}$ is an integral domain.
(iv) $\mathfrak{p} \neq A$ and for arbitrary ideal $\mathfrak{a}$, $\mathfrak{b}$ in A with $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

b). Let $\mathfrak{p}$ be a prime ideal in a ring A and let $\mathfrak{a}_1, \ldots, a_n$ be ideals in A. Show that the following statements are equivalent:

(i) $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some j with $1 \leq j \leq n$. (ii) $\mathfrak{p} \supseteq \cap_{i=1}^{n} \mathfrak{a}_i$. (iii) $\mathfrak{p} \supseteq \prod_{i=1}^{n} \mathfrak{a}_i$.

c). Let $\mathfrak{p}$ be an ideal in A. Show that $\mathfrak{p}$ is a prime ideal in A if and only if the extension $\mathfrak{p}A[X]$ is a prime ideal in $A[X]$, where $A[X]$ is the polynomial ring in one indeterminate X over A.

2). The set $\mathcal{I}_A$ is ordered by the natural inclusion, i.e. the natural inclusion $\subseteq$ is a partial order on $\mathcal{I}_A$. An ideal $\mathfrak{m}$ in A is called a maximal ideal if it is a maximal element in the partially ordered set $(\mathcal{I}_A \setminus \{A\}, \subseteq)$. Therefore an ideal $\mathfrak{m}$ is a maximal ideal in A if and only if $\mathfrak{m} \neq A$ and if $\mathfrak{a} \in \mathcal{I}_A$ with $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$, then either $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$. The set of all maximal ideals in A is denoted by $\operatorname{Max} A$. A ring A is called (quasi)-local if $\operatorname{Max}(A)$ is singleton, i.e., A has exactly one maximal ideal. (**Remark:** Prime ideals and maximal ideals play fundamental role in commutative algebra and algebraic geometry. The following THEOREM OF KRULL and its corollaries ensure that there are maximal (and hence prime) ideals, i.e. $\operatorname{Max} A \neq \emptyset$.

Theorem (KRULL) *Every non-zero ring A has at least one maximal ideal.*

Corollary 1 *Let $\mathfrak{a}$ be an ideal in A, $\mathfrak{a} \neq A$. Then there exists a maximal ideal in A which conatin $\mathfrak{a}$.*

Corollary 2. *Every non-unit in A is contained in some maximal ideal.*)

a). Prove that an ideal $\mathfrak{m}$ in A is a maximal ideal if and only if the residue class ring $A/\mathfrak{m}$ is a field. In particular, every maximal ideal in A is a prime ideal in A, i.e. $\operatorname{Max} A \subseteq \operatorname{Spec} A$.

b). Let $\mathfrak{m}$ be a maximal ideal in A. When exactly the extension $\mathfrak{m}A[X]$ is a maximal ideal in $A[X]$?, where $A[X]$ is the polynomial ring in one indeterminate X over A.

c). Let k be a field and let $a_1, \ldots, a_n \in K$, $n \in \mathbb{N}^*$. The the ideal $\mathfrak{m}_a := \{f \in k[X_1, \ldots, X_n] \mid f(a) = 0\}$ is a maximal ideal in the polynomial ring $k[X_1, \ldots, X_n]$ and is generated by the linear polynomials $X_1 - a_1, \ldots, X_n - a_n$. Further, the map $\varphi : k^n \to \operatorname{Max}(k[X_1, \ldots, X_n])$ defined by $a \mapsto \mathfrak{m}_a$ is injective. In general this map is not surjective, for example, if k is any prime field, then the map φ is not surjective!.

d). Let $\mathrm{C}_{\mathbb{R}}([0, 1])$ be the ring of all continuous real valued functions on the closed interval $[0, 1] \subset \mathbb{R}$ (with pointwise addition and pointwise multiplication of functions). Then:

1) For every $t \in [0, 1]$, $\mathfrak{m}_t := \{f \in \mathrm{C}_{\mathbb{R}}([0, 1]) \mid f(t) = 0\}$ is a maximal ideal in $\mathrm{C}_{\mathbb{R}}([0, 1])$.

2) Let $f_1, \ldots, f_n \in \mathrm{C}_{\mathbb{R}}([0,1])$ be such that $f_1, \ldots, f_n$ does not have any common zero in $[0,1]$. Then $f_1^2 + \cdots + f_n^2$ is a unit in $\mathrm{C}_{\mathbb{R}}([0,1])$.

3) Let $\mathfrak{a}$ be any non-unit ideal in $\mathrm{C}_{\mathbb{R}}([0,1])$. Show that all functions in $\mathfrak{a}$ have a common zero in $[0,1]$. (**Hint**: Use (2) and the compact ness of $[0,1]$.)

3). Let $\varphi : A \to B$ be a ring homomorphism.

a). If $\mathfrak{q}$ be a prime ideal in B, then the contraction $\mathfrak{q} \cap A$ is a prime ideal in A. —In fact, the map φ induces an injective ring homomorphism $\overline{\varphi} : A/\mathfrak{q} \cap A \to B/\mathfrak{q}$. If $\mathfrak{n}$ is a maximal ideal in B, then contraction $\mathfrak{n} \cap A$ need not be a maximal ideal in A.

b). Suppose that φ is surjective. Then

1) There a bijection between the prime ideals of A containing $\mathrm{Ker}\,\varphi$ onto the set of all prime ideals in B. (**Hint**: In fact, the map $\mathfrak{p} \mapsto \mathfrak{p}B$ is a bijection with inverse $\mathfrak{q} \mapsto \mathfrak{q} \cap A$. See 1.1-(4)-d))
2) Then there a bijecction between the maximal ideals of A containing $\mathrm{Ker}\,\varphi$ onto the set of all maximal ideals in B. (**Remark**: In the case when φ is injective, the general situation is very complicated. In fact the behavaour of prime ideals under extensions of this sort is one of the central problems of *algebraic number theory*.)

c). Consider the natural inclusion $\mathbb{Z} \to \mathbb{Z}[\mathrm{i}]$, where $\mathrm{i} := \sqrt{-1}$. A prime ideal $\mathbb{Z}p$ in $\mathbb{Z}$ may or may not remain prime when it is extended to $\mathbb{Z}[\mathrm{i}]$. For example:

1) The extension of the prime ideal $\mathfrak{p} = \mathbb{Z}2$ to $\mathbb{Z}[\mathrm{i}]$ is the square of the prime ideal $(1+\mathrm{i})^2$ in $\mathbb{Z}[\mathrm{i}]$.
2) Let p be a prime number with $p \equiv 1 \pmod 4$, then $p\mathbb{Z}[\mathrm{i}]$ is a product of two distinct prime ideals in $\mathbb{Z}[\mathrm{i}]$. (for example $5\mathbb{Z}[\mathrm{i}] = (2+\mathrm{i})(2-\mathrm{i})$.)
3i) Let p be a prime number with $p \equiv 3 \pmod 4$, then $p\mathbb{Z}[\mathrm{i}]$ is a prime ideal in $\mathbb{Z}[\mathrm{i}]$.

1.3. (Nil-radical and Jacobson-radical)

1). The set of all nilpotent elements in a ring A is an ideal. This ideal is called the nil-radical of A and is denoted by $\mathfrak{n}_A$.

a). The nil-radical of A is the intersection of all the prime ideal in A. i.e. $\mathfrak{n}_A = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, A} \mathfrak{p}$.

b). For the polynomail ring $A[X]$ over a ring A, show that $\mathfrak{n}_{A[X]} = (\mathfrak{n}_A)[X]$ and $\mathrm{Z}(A[X]) = \mathrm{Z}(A) + (\mathfrak{n}_A)[X]$. (**Hint**: Use T1.12-1) and 3).)

2). The intersection of all maximal ideals in a ring A is called the Jacobson-radical of A and is denoted by $\mathfrak{m}_A$.

a). For an element $x \in A$, the following statements are equivalent:

(i) $x \in \mathfrak{m}_A$.
(ii) For every $a \in A$, $1 - ax$ is a unit in A.

b). Let $\mathrm{P} := A[X_i]_{i \in I}$ with $I \neq \emptyset$. Then the Jacobson-radical $\mathfrak{m}_{\mathrm{P}}$ and the nil-radical $\mathfrak{n}_{\mathrm{P}}$ of P are equal. (**Hint**: $1 + X_i \mathfrak{m}_{\mathrm{P}} \subseteq \mathrm{P}^{\times}$.))

c). Let $R := A[\![X]\!]$ be the formal power series ring one indeterminate X over A. Then:

1) The Jacobson-radical $\mathfrak{m}_{\mathrm{R}} = \{f \in \mathrm{R} \mid f(0) \in \mathfrak{m}_A\}$ and the nil-radical $\mathfrak{n}_{\mathrm{R}} = \{f \in \mathrm{R} \mid$ all coefficients of $f \subseteq \mathfrak{n}_A\}$. (**Hint**: Use T1.13.)

2) If $\mathfrak{M} \in \mathrm{Max}\,(\mathrm{R})$, then $\mathfrak{M}$ is generated by $(\mathfrak{M} \cap A) \cup \{X\}$ and the contraction $\mathfrak{M} \cap A$ of $\mathfrak{M}$ is a maximal ideal of A.

3) Show that each prime ideal of A is a contarction of a prime ideal of R,.

1.4. (Prime Avoidance Theorem) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, $n \geq 2$, be ideals in A such that at most two of $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are not prime and let S be an additive subgroup of A which is closed under multiplication. (for example, S could be an ideal of A or a subring of A.) Suppose that $S \subseteq \cup_{i=1}^n \mathfrak{p}_i$. Then $S \subseteq \mathfrak{p}_j$ for some j with $1 \leq j \leq n$. (**Remark:** The Prime Avoidance Theorem is most frequently used in situations where S is actually an ideal of A and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are all prime ideals of A. However, there are some occasions when it is helpful to have more of the full force of the above statament available. The name ''Prime Avoidance Theorem'' is explained in the following reformulation of its statement: *If $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, $n \geq 2$, be ideals in A and at most two of $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are not prime and if, for each $i = 1, \ldots, n$, we have $S \not\subseteq \mathfrak{p}_i$, then there exists $c \in S \setminus \cup_{i=1}^n \mathfrak{p}_i$ so that c ''avoids'' all the ideals $\mathfrak{p}_i, \ldots, \mathfrak{p}_n$, ''most'' of which are prime.*)

The following refinements of the Prime Avoidance Theorem are extremely useful:

a). Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals in A, $\mathfrak{a}$ be an ideal in A and let $a \in A$ be such that $Aa + \mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then show that there exists $c \in \mathfrak{a}$ such that $a + c \notin \cup_{i=1}^n \mathfrak{p}_1$.

b). Let A be a ring which contain an infinite field as subring. and let $\mathfrak{a}, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$, $n \geq 2$, be ideals in A such that $\mathfrak{a} \subseteq \cup_{i=1}^n \mathfrak{b}_i$, then prove that $\mathfrak{a} \subseteq \mathfrak{b}_j$ for some j with $1 \leq j \leq n$.

1.5. (Minimal prime ideals) Let A be a ring and let $\mathfrak{a}$ be an ideal in A. A minimal element in the set $V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subseteq \mathfrak{p}\}$ (partially ordered by the inclusion) is called a minimal prime ideal of $\mathfrak{a}$. If $A \neq 0$, then a minimal prime ideal of the zero ideal 0 in A is called a minimal prime ideal in A. The set of minimal prome ideals of $\mathfrak{a}$ is denoted by $\operatorname{Min}(\mathfrak{a})$.

a). Every prime ideal in A containing the ideal $\mathfrak{a}$ in A contains a minimal prime ideal of $\mathfrak{a}$. (**Hint:** For $\mathfrak{p} \in V(\mathfrak{a})$, the set $\{\mathfrak{p}' \in \operatorname{Spec} A \mid \mathfrak{a} \supseteq \mathfrak{p}' \supseteq \mathfrak{p}\}$ is inductively ordered with respect to the reverse inclusion and hence by Zorn's lemma has a maximal elements with respect to the reverse inclusion, i. e., has a minimal element with respect to the inclusion.))

b). The radical of the ideal $\mathfrak{a}$ is the intersection of the minimal prime ideals of $\mathfrak{a}$, i.e. $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \operatorname{Min}(\mathfrak{a})} \mathfrak{p}$. In particular, *the nil-radical of A is the intersection of the minimal prime ideals of A.*

c). If $\mathfrak{a}$ is a radical ideal, i. e. $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then the set of elements $\{a \in A \mid a \text{ is a zero-divisor in } A/\mathfrak{a}\}$ is the union of the minimal prime ideals of $\mathfrak{a}$, i. e, $Z(A/\mathfrak{a}) = \mathfrak{a} = \bigcup_{\mathfrak{p} \in \operatorname{Min}(\mathfrak{a})} \mathfrak{p}$. In particular, *the set of zero-divisors in A is the union of the minimal prime ideals of A and hence all elements of a minimal prime ideals of A are zero-divisors.*

d). Suppose that A is noetherian. Then the set of minimal prime ideals of $\mathfrak{a}$ is finite. (**Hint:** Let $\mathfrak{a}$ be a maximal in the set of the ideals $\{\mathfrak{a} \mid \operatorname{Min}(\mathfrak{a}) \text{ is not finite }\}$ in A. There exist elements $a, b \in A$ such that $a \notin \mathfrak{a}$, $b \notin \mathfrak{a}$, $ab \in \mathfrak{a}$. Now, consider the minimal prime ideals of $\mathfrak{a} + Aa$, $\mathfrak{a} + Ab$.))

1.6. (Zero-divisors) In this Exercise an important assertions proved in the Exercise 1.5 - c), d) about the set $Z(A)$ of zero divisors in noetherian ring A are proved by using an idea of I. KAPLANSKY). If A is reduced then by Exercise 1.5-c) and d) is a union of the finitely minimal prime ideals in A. We would like to show that: *the set of zer-divisors in a noetherian ring is a finite union of prime ideals* – For this first assume that A, aia an arbitrary ring. The set of zero-divisors in A is the union of the annihilators $\operatorname{Ann}_A a := \{b \in A \mid ba = 0\}$, $a \in A \setminus \{0\}$.

a). In the set of ideals $\{\operatorname{Ann}_A a \mid a \in A \setminus \{0\}\}$, a maximal element with respect to the natural inclusion is a prime ideal. (**Remark:** The prime ideals of the form $\operatorname{Ann}_A a$ $a \in A \setminus \{0\}$ are called the associated prime ideals of A)

b). If A is noetherian the set $\{\mathrm{Ann}_A\, a \mid a \in A \setminus \{0\}\}$ has only finitely many maximal elements (with respect to the natural inclusion). In particular, the set of zero-divisors in $A|$, is a finite union of prime ideals which are precisely the annihilators of elements of A. (**Hint:** Let $\mathrm{Ann}_A\, a_i$, $i \in I$ be the maximal elements and let $a_{i_1}, \ldots, a_{i_n}$ be a finite generating system for the ideal $\sum_{i\in I} Aa_i$ and $\mathfrak{p}_\nu := \mathrm{Ann}_A\, a_{i_\nu}$ for $\nu = 1, \ldots, n$. Then from $\cap_{\nu=1}^n \mathfrak{p}_\nu \subseteq \mathrm{Ann}_A\, a_i$ it follows that $\mathfrak{p}_{\nu_0} \subseteq \mathrm{Ann}_A\, a_i$ and hence $\mathfrak{p}_{\nu_0} = \mathrm{Ann}_A\, a_i$ for some $\nu_0 \in \{1, \ldots, n\}$.)

c). Let $\mathfrak{a}$ be an ideal in a noetherian ring A. Then $\mathfrak{a}$ contains a non-zero divisor if and only if $\mathrm{Ann}_A\, \mathfrak{a} = 0$. (**Hint:** Use the part b) and the Prime Avoidance Theorem, See Exercise 1.4.)

Below one can see (simple) test-exercises which are meant to test the basic concepts and definitions.

Test-Exercises

T1.1. For $n \in \mathbb{N}^*$, let Z_n denote a cyclic (additively written) group of order n. If $N \subseteq \mathbb{N}^*$ is an infinite subset of the set of positive natural numbers, then the additive group $\bigoplus_{n\in N} Z_n$ is not a ring (with unity) with any multiplication.

T1.2. Let A be a ring.

1). Suppose that $\mathrm{Char}\, A \neq 1, \neq 2$ and the unit group $A^\times$ of A is cyclic. Then $A^\times$ is finite and the cardinality $|A^\times|$ is an even number.

2). If $u \in A$ is unipotent, then so is u^{-1}. If $u, v \in A$ are unipotent and commute, then uv is also unipotent. Therefore the set of unipotent elements in A is a subgroup of $A^\times$.

3). Suppose that the characteristic of A is p^n, where p is a prime number. An element $u \in A$ is unipotent if and only if u is a unit in A and the order of u in $A^\times$ is a power of p. If A has no non-zero nilpotent elements and if $a \in A^\times$ is an element of finite order, then $\gcd(p, \mathrm{Ord}\, a) = 1$.

4). Let a, b be idempotent elements in A.

a). $a + b$ is idempotent if and only if $ab = ba$ and $2ab = 0$. Further, $a - b$ idempotent if and only if $ab = ba$ and $2(1 - a)b = 0$.

b). If $ab = ba$, then ab, $a + b - ab$ and $(a - b)^2 = a + b - 2ab$ are idempotent.

c). If $ab = ba$ and $a - b$ nilpotent, then $a = b$.

5). Let $\mathrm{Idp}(A)$ be the set of all idempotent elements in A. Then $(\mathrm{Idp}(A), \triangle, \cdot)$ is a Boolean ring, with the addition $a \triangle b := (a - b)^2$ and the multiplication induced from the multiplication from A. (the rings $(\mathrm{Idp}(A), \triangle, \cdot)$ and $(A, +, \cdot)$ are equal if and only if A if A is a Boolean ring).

T1.3. Let Q be the quotient field of the integral domain A. Then $\mathrm{card}(Q) = \mathrm{card}(A)$. (**Hint:** For an infinite set X, $\mathrm{card}(X \times X) = \mathrm{card}(X)$ — this can be easily proved by using Zorn's lemma.)

T1.4. In a finite ring every non-zero divisor is a unit. In particular, a non-zero domain is a divison ring. (**Remark:** A famous theorem of Wedderburn states that: *every finite division ring is commutative and hence a field*.)

T1.5. Let $m_1, \ldots, m_r$ be non-zero pairwise relatively prime natural numbers and $m := m_1 \cdots m_r$. Then $A := \prod_{i=1}^r \mathrm{A}_{m_i}$ is a prime ring of the characteristic m. the unit group of A is the direct product of the unit groups of the prime rings A_{m_i}. What can you now conclude for the Euler's φ-function?

T1.6. Let A be a ring.

1). Let e be an idempotent element in A. For every $a \in A$, show that $Aa \cap Ae = Aae$.

2). Let $a, b \in A$ with $ab = 0$. Suppose that the ideal $Aa + Ab$ contain a non-zero divisor. Then show that $Aa \cap Ab = 0$, and that $a + b$ is a non-zero divisor in A.

T1.7. **1).** Let A_i, $1 \leq i \leq n$, be rings and let A be the product ring $\prod_{i=1}^n A_i$ and $p_i : A \to A_i$ be the canonical projections. Let $\mathfrak{a} \subseteq A$ be an ideal. Show that for every i, $\mathfrak{a}_i := p_i(\mathfrak{a})$ is an ideal in A_i, and that $\mathfrak{a} = \prod_{i=1}^n \mathfrak{a}_i$. Conversely, if $\mathfrak{a}_i \subseteq A_i$, are ideals, then show that $\mathfrak{a} := \prod_{i=1}^n \mathfrak{a}_i$ is an ideal in A.

2). Let $A_1, \ldots, A_n$ be principal ideal rings. Show that the direct product $\prod_{i=1}^n A_i$ ring is also a principal ideal ring.

3). All subrings of $\mathbb{Q}$ are principal ideal domains. (**Hint:** Let A be a subring of $\mathbb{Q}$. Show that $\mathfrak{a} = (\mathfrak{a} \cap \mathbb{Z})A$ for every ideal $\mathfrak{a}$ in A.)

T1.8. **1).** Compute the Jacobson-radicals $\mathfrak{m}_{\mathbb{Z}}$, $\mathfrak{m}_{\mathrm{A}_m}$ and the nil-radicals $\mathfrak{n}_{\mathbb{Z}}$, $\mathfrak{n}_{\mathrm{A}_m}$, where A_m is a prime ring of characteristic of $m > 0$.

2). Let A_i, $i \in I$, be a family of rings. For the product ring $A = \prod_{i \in I} A_i$, show that $\mathfrak{m}_A = \prod_{i \in I} \mathfrak{m}_{A_i}$ and $\mathfrak{n}_A \subseteq \prod_{i \in I} \mathfrak{n}_{A_i}$ (give example where the inclusion is proper!).

T1.9. Let A be a ring, $\mathfrak{a}$ be a left ideal in A, which contain only nilpotent elements ($\mathfrak{a}$ need not be a nilpotent ideal!), and $\mathfrak{m}$ be an arbitrary maximal ideal in A. Show that $\mathfrak{a} \subseteq \mathfrak{m}$. (**Hint:** Consider $\mathfrak{a} + \mathfrak{m}$; if $1 = a + x \in \mathfrak{a} + \mathfrak{m}$ with $a \in \mathfrak{a}$ and $x \in \mathfrak{m}$, then $x = 1 - a \in A^\times$.)

T1.10. Show that the ring $A := \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2)$ is an integral domain.

T1.11. Let k be a field and let $a_1, \ldots, a_n \in K$, $n \in \mathbb{N}^*$. Show that the chain

$$0 \subsetneq (X_1 - a_1) \subsetneq (X_1 - a_1, X_2 - a_2) \subsetneq \cdots \subsetneq (X_1 - a_1, \ldots, X_n - a_n)$$

is a strictly ascending chain of prime ideals in the polynomial ring $k[X_1, \ldots, X_n]$ over k.

T1.12. Let A be a ring, P be the polynomial algebra $A[X_i]_{i \in I}$ and $f = \sum a_\nu X^\nu \in \mathrm{P}$.

1). f is nilpotent if and only if all the coefficients of f are nilpotent.

2). f is a unit in P if and only if a_0 is a unit in A and all coefficients a_ν, $\nu \neq 0$, of f are nilpotent. (**Hint:** We may assume that $\mathrm{P} = A[X]$. Let $m := \deg f > 0$. It is enough to prove that a_m is nilpotent. But $fg = 1$ with $g = b_0 + \cdots + b_n X^n$, and so by induction $a_m^{i+1} b_{n-i} = 0$ for $i = 0, \ldots, n$. Variant: Pass to the ring A_S, $S := \mathrm{S}(a_m)$, and apply the degree formula.)

3). (Theorem of McCoy) f is a zero-divisor in P if and only if there exists $a \in A$, $a \neq 0$ such that $af = 0$. (**Hint:** We may assume that I is finite. First suppose that $\mathrm{P} = A[X]$, $fg = 0$, $m := \deg f$, $\deg g > 0$. In the case $a_i g = 0$ for all i is the assertion is trivial. Otherwise, let r the maximum of i with $1 \leq i \leq m$ and $a_i g \neq 0$. Then $\deg(a_r g) < \deg g$ and $f \cdot (a_r g) = 0$. — Now, suppose that $n \geq 1$ and $f = \sum_{i=0}^m f_i X_n^i$ with $f_i \in \mathrm{Q} := A[X_1, \ldots, X_{n-1}]$. If $fg = 0$ with $g \in \mathrm{Q}$, $g \neq 0$, then $hg = 0$ for all $h = \sum_{i=0}^m f_i X_{n-1}^{s_i}$ in Q with $s_i \in \mathbb{N}$ arbitrary. Apply the induction hypothesis to h and choose s_i so that s_{i+1} enough bigger than s_i.)

4). f is idempotent if and only if $f = a_0$ is a constant polynomial and a_0 is idempotent in A. (**Hint:** We may assume that $\mathrm{P} = A[X]$. Since f is idempotent so are a_0 and $(f - a_0)^2$, and hence $(f - a_0)^2 = 0$ and $f = a_0$.)

T1.13. Let A be a ring, R be the formal power series ring $A[\![X]\!]$ in one indeterminate X over A and $f = \sum_{n=0}^\infty a_\nu X^\nu \in \mathrm{R}$.

1). If f is nilpotent, then all the coefficients of f are nilpotent. Is the converse true?

2). f is a unit in R if and only if a_0 is a unit in A.

---

† **Wolfgang Krull (1899-1971)** Wolfgang Krull was born on 26 Aug 1899 in Baden-Baden, Germany and died on 12 April 1971 in Bonn, Germany. Wolfgang Krull's father was Helmuth Krull and his mother was Adele Siefert Krull. Helmuth Krull had a dentist's practice in Baden-Baden and it was in that town that Krull attended school. After graduating from secondary school in 1919 he entered the University of Freiberg. It was the custom in those days for students in Germany to move around various universities during their period of study and Krull was no exception. He spent time at the University of Rostock before moving to Göttingen in 1920. From 1920 to 1921 he studied at Göttingen with Klein but was most influenced by Emmy Noether. He attended Klein's seminar in the session 1920-21 and he then returned to Freiberg and

presented his doctoral thesis on the theory of elementary divisors in 1922. Ring theory results from this thesis have recently been found important in the area of coding theory.

Appointed as an instructor at Freiberg on 1 October 1922 he was promoted to extraordinary professor in 1926. He remained there until 1928 when he moved to Erlangen. His inaugural address on becoming a full professor at Erlangen was one which says much of how Krull saw mathematics. He saw the role of a mathematician as:

... not merely ... finding theorems and proving them. He wants to arrange and group these theorems together in such a way that they appear not only as correct but also as imperative and self-evident. To my mind such an aspiration is an aesthetic one and not one based on theoretical cognition

If Emmy Noether had the greatest influence on the topics which Krull would spend his life researching, it can be seen from this inaugural address that it was Klein who had the greatest influence on Krull's large scale view of mathematics. In 1929 he married Gret Meyer and they would have two daughters. The ten years Krull spent in Erlangen were the most productive period of his career. The years Krull spent as a full professor in Erlangen were the high point of his creative life. About thirty-five publications of fundamental importance for the development of commutative algebra and algebraic geometry date from this period. At Erlangen he was involved in university life as well as concentrating on his research, being elected Head of the Faculty of Science.

In 1939 Krull left Erlangen to take up a chair at Bonn. However, his career was disrupted by the Second World War which began shortly after Krull was appointed to the University of Bonn. During the war he undertook war duties, working in the naval meteorological service. When his war service had ended in 1946, Krull took up again his post at the University of Bonn and he would remain there for the rest of his life. In this final period of his career Krull continued his high level of productivity (he wrote 50 papers in his post-war years in Bonn) and also broadened his mathematical interests. He continued his earlier studies, but also dealt with other fields of mathematics: group theory, calculus of variations, differential equations, Hilbert spaces.

Krull's first publications were on rings and algebraic extension fields. In 1925 he proved the Krull-Schmidt theorem for decomposing abelian groups of operators. He then studied Galois theory and extended the classical results on Galois theory of finite field extensions to infinite field extensions. In passing from the finite to the infinite case Krull introduced topological ideas.

In 1928 he defined the Krull dimension of a commutative Noetherian ring and brought ring theory into in new setting in which he was able to show that the principal ideal theorem held. Perhaps the reason that the idea of the Krull dimension is such a natural concept is that it encapsulates in an abstract setting the analogues of geometric dimensions. The principal ideal theorem was quickly recognised as a decisive advance in Noether's programme of emancipating abstract ring theory from the theory of polynomial rings.

Krull carried his work forward, defining further concepts which are today central to modern research in ring theory. In 1932 he defined valuations which are today known as Krull valuations. He then wrote the remarkable treatise Ideal Theory which remains a beautiful introduction to ring theory but is simply a theory built from the results that Krull had himself proved. One could say that Krull had achieved the goal he had in some sense set himself in his Erlangen address and arranged his theory to be self-evident.

Another major topic in ring theory is the study of local rings, that is rings having a unique maximal ideal, and they are used in the study of local properties of algebraic varieties. The concept was introduced by Krull in 1938 and his fundamental results were developed into a major theory by mathematicians such as Chevalley and Zariski.

He supervised 35 doctoral students, and rather remarkably, 32 of these were students which he supervised after the end of World War II. Krull's papers are marked by the profundity of his ideas, the rigour of his proofs, and also by a strong aesthetic sense. Indeed much of modern ring theory is still following the path which Krull took, building on the foundations which Emmy Noether had laid.