PREPARATORY LECTURE: PRIME IDEALS IN NOETHERIAN RINGS

SYLVIA WIEGAND
UNIVERSITY OF NEBRASKA

Abstract. We discuss the basic ideas and notions for partially ordered sets of prime ideals in Noetherian rings. We give examples of such sets for the ring of integers and for one- and two-dimensional integral domains of polynomials and power series.

Thank you all for coming to this talk. We especially welcome the outstanding students and teachers in the audience.

As someone who has been involved in preparing future teachers of mathematics, I appreciate the role that algebra plays in elementary mathematics. It is very helpful for future teachers to have a strong background in algebraic concepts. For example, teachers can help elementary students learn basic facts by calling their attention to algebraic properties like the commutative property of addition of integers: $a + b = b + a$, for every pair of integers a, b. If a student knows that $5 + 2 = 7$, she sees that $2 + 5 = 7$.

preplec 1. Basics and first pictures

As always in mathematics, we begin by explaining the words we use. Informally the discipline *algebra* describes the study of sets with operations. Often the sets contain numbers and the operations are addition and multiplication; sometimes the sets consist of functions, such as polynomials. For this workshop and conference, the most basic example of a concept involving sets with operations is that of a *ring*:

ringdef **Definition 1.1.** A *ring* is a set R with two operations, addition $(+)$, and multiplication $(\cdot)$—this includes subtraction as an inverse operation to addition, but division is not always possible. A ring satisfies the usual basic properties, such as the *commutative property of addition* ($a + b = b + a$, for every pair $a, b \in R$), and the *distributive property of multiplication over addition* ($a \cdot (b + c) = a \cdot b + a \cdot c$, for every $a, b, c \in R$). Our rings are *commutative for multiplication*; that is, $a \cdot b = b \cdot a$, for every pair $a, b \in R$.

Date: 21 April, 2015.

We thank Professors Ajaya Singh and Prakash Muni Bajracharya and other organizers in the Departments of Mathematics and Mathematics Education at Tribhuvan University for their work and for providing facilities for the First International Workshop and Conference on Commutative Algebra at Tribhuvan University. The conference and workshop were enjoyable and mathematically stimulating. We are also grateful to the speakers for their willingness to participate in this project, for their fine talks, and for their kindness and cooperation in the face of some discomfort and inconvenience. Fortunately, all of the conference participants were safe. We greatly appreciate the support and help of all the Nepalese faculty and students in the aftermath of the earthquake. It was a devastating event for Nepal; we hope the Nepalese can get back to normal soon and that they can rebuild and recover much of what was lost.

Suggestion: If the concept of "ring" is new to you, try to think on your own of the complete list of ten properties that should hold for the operations and elements of a commutative ring, such as the ring of integers; see Examples **??**. Then look up the complete definition in an algebra book.

fexcr **Examples 1.2.** Examples of commutative rings:

(1) The integers $\mathbb{Z} := \{0, 1, -1, 2, -2, 3, -3, \cdots\}$; the rationals $\mathbb{Q} := \{a/b \mid a, b \in \mathbb{Z}$ and $b > 0\}$; $\mathbb{R} := \{$ directed distances (+ or −) from 0 on a number line$\}$; and $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$. All of these rings use addition and multiplication as the operations.

(2) The twelve clock & "clock arithmetic": $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, with addition and multiplication defined "mod twelve" so that

$$1 + 2 = 3, \quad 4 + 9 = 13 \equiv 1, \quad 10 + 10 \equiv 7, \quad 3 \times 4 \equiv 0.$$

(You can think of 12 as being "the same as" 0 and 24; 8 is the "same as" 20 and -4, etc.) You can add and multiply by using the clock; for 3×4, start at 4, move around 4 more, then 4 more, so see that you're back at $0 \equiv 12$. Similarly, $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, the "two clock" and $\mathbb{Z}/6\mathbb{Z}$, the "six clock", etc.

(3) Rings of polynomials $R[x]$ over a ring R: for example, $\mathbb{Z}[x]$ is the set of all polynomials with coefficients in the integers $\mathbb{Z}$, again with addition and multiplication. That is, $\mathbb{Z}[x]$ is the set of all finite sums $\sum_{i=0}^{n} a_i x^i$ of integers a_i times powers x^i of the variable x. Therefore $0, 1, x, 1-5x, 2+x-7x^2, -3+11x^5$ are elements of $\mathbb{Z}[x]$.

(4) Power series in R over a ring R, written $R[[x]]$: the set of all "infinite polynomials" in the variable x with coefficients in R. Thus $\mathbb{Z}[[x]] = \{\sum_{i=0}^{\infty} a_i x^i$, where $a_i \in \mathbb{Z}$ and i is a nonnegative integer$\}$ and $1 + 2x + 3x^2 + \cdots \in \mathbb{Z}[[x]]$. Notice that $R[x] \subseteq R[[x]]$. (Every polynomial is a power series with only finitely many nonzero coefficients.)

Aside for teachers: In mathematics classes, sometimes students ask: "Will this be on the test?" In teacher-preparatory classes, the students ask:"How is this relevant for teaching?" Nearly everything in mathematics is relevant for teaching! Teachers should know more than what the students learn; they need to know the background, and the *reasons.* Ideally teachers should be familiar with what concepts will come later in the curriculum. We want teachers to encourage their students to think deeply about mathematics and to be able to solve problems. This means that teachers also should think deeply about mathematics and be able to solve problems at a higher level than the students.

In order to introduce prime ideals, we review some basic facts about prime numbers in the ring of integers.

primesZ

2. Prime numbers in $\mathbb{Z}$

The (positive) *prime integers* in $\mathbb{Z}$ are $\{2, 3, 5, 7, 11, 13, \cdots\}$—they have exactly two positive integer divisors in $\mathbb{Z}$. They are also called *irreducible* elements, in the sense that they cannot be factored further.

We use the following definitions more generally for any ring R:

eltdefs **Definitions 2.1.** Let R be a ring.

(1) An element u of R is a *unit* if there exists a multiplicative inverse $u^{-1} \in R$ with $u(u^{-1}) = 1$ in R. For example, 1 and -1 are the only units of $\mathbb{Z}$,

but every nonzero element of $\mathbb{Q}$ is a unit: $(-1)^{-1} = -1$ in $\mathbb{Z}$ or $\mathbb{Q}$, since $(-1)\cdot(-1) = 1$; in $\mathbb{Q}$, $(1/2)^{-1} = 2$, since $(1/2)\cdot 2 = 1$. In $\mathbb{Z}[x]$, 1 and -1 are the only units. In $R[[x]]$, every element $f(x)$ of form $f(x) = u + xg(x)$, for some u a unit of R and $g(x) \in R[[x]]$ is a unit: for example, $(1-x)^{-1} = 1 + x + x^2 + \cdots$.

(2) For $a, b \in R$, we say a *divides* b and write $a|b$, provided b is a multiple of a; that is, there exists $c \in R$ so that $a \cdot \boxed{c} = b$. We also say that a is a *factor* of b. Thus we have $2|6$ and $3d|6d$, for every $d \in \mathbb{Z}$ with $d \neq 0$ (because $3d \cdot \boxed{2} = 6d$). *Aside:* Beginning students may get a, the *divisor* mixed up with b, the *dividend.* Also they may get the vertical divides sign "|" confused with the slanted fraction notation"/", and so they mistake $a|b$, which means "a divides b", for a/b, which means the fraction $\frac{a}{b}$ or "a divided by b".

(3) An element p of a ring R is *prime* provided p is *not* a unit, and, whenever $a, b \in R$ satisfy $p|(a\cdot b)$, we have $p|a$ or $p|b$. For example 4 is *not* prime in $\mathbb{Z}$, since $4|(6\cdot 2)$, but 4 does not divide 6 and 4 does not divide 2. Also 2 is prime because if $2|(a\cdot b)$, then $a\cdot b$ is an even integer, and then at least one of the factors is even, so we do have that $2|a$ or $2|b$. The prime integers 2 and -2 are called *associates*, since $2 = (-1)(-2)$; that is, 2 is a unit times (-2). When we make a list of prime integers "up to associates", we list only one of each pair of associates. Usually we take the non-negative prime elements for that list. Unlike common usage, we do consider that 0 is a prime element of $\mathbb{Z}$.

One reason that prime numbers are important is because of the Fundamental Theorem of Arithmetic:

FTA **Theorem 2.2.** *The Fundamental Theorem of Arithmetic. For every integer $n > 1$, there exists a unique expression $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots p_t^{e_t}$, with each p_i a positive prime integer, each $e_i \geq 1$ and $p_1 < p_2 < \ldots p_t$; for example, $36 = 2^2 \cdot 3^2$.*

In most rings there is no such theorem. For example in the ring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ we have $6 = (1+\sqrt{-5})\cdot(1-\sqrt{-5}) = 2\cdot 3$, and so there are two different expressions into irreducible elements. None of $2, 3, 1-\sqrt{-5}$, or $1+\sqrt{-5}$ are prime elements of $\mathbb{Z}[\sqrt{-5}]$. The Fundamental Theorem does not hold.

Around 1870, Dedekind and Kummer developed an "ideal theory" using what they called "ideals" and "prime ideals" to try to extend unique factorization.

idealdef **Definition 2.3.** Let R be a ring. Defined precisely, an *ideal* of R is a nonempty subset I of R such that, (i) For every $a, b \in I, a - b \in I$ and, (ii) For every $a \in I$ and $r \in R$, $ar \in I$. Property ii is the "sponge" property— multiplication from anywhere in the ring is absorbed into the ideal.

For our purposes, an *ideal* I is a sum of multiples of particular elements of R, e.g., for $a, b, a_1, a_2, \ldots, a_n \in R$, a ring, you could take $I = (a) = Ra = \{ra \mid r \in R\}$ or $I = (a, b) = Ra + Rb = \{ra + sb \mid r, s \in R\}$ or $I = (a_1, a_2, \ldots, a_n) = Ra_1 + Ra_2 + \ldots + Ra_n = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}$.

vecideals **Remark 2.4.** This is the same idea as taking spans of vectors in the vector space $\mathbb{R}^3$. There you use diagonal brackets "< >" to mean "all sums of multiples of". For example

$$\left\langle \begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}3\\4\\1\end{bmatrix} \right\rangle = \mathbb{R}\cdot\begin{bmatrix}1\\2\\0\end{bmatrix} + \mathbb{R}\cdot\begin{bmatrix}3\\4\\1\end{bmatrix} = \{r_1\begin{bmatrix}1\\2\\0\end{bmatrix} + r_2\begin{bmatrix}3\\4\\1\end{bmatrix}, \text{ where } r_1, r_2 \in \mathbb{R}\},$$

would be the "ideal" of $\mathbb{R}^3$ generated by the two vectors given. (But actually $\mathbb{R}^3$ is not a ring—multiplication of two vectors is not defined; the multiplication used is an element of $\mathbb{R}$ times a vector in $\mathbb{R}^3$. The span of a set of vectors in a vector space makes a *subspace*.)

In this talk we are concerned with *Noetherian* rings, named for the famous woman mathematician Emmy Noether, who studied these rings.

Noethdef **Definition 2.5.** A ring R is *Noetherian* if every ideal is finitely generated. That is, for every set I that satisfies (precise) Definition **??** (first paragraph), there are finitely many elements $a_1, a_2, \dots, a_n$ so that $I = Ra_1 + Ra_2 + \dots + Ra_n$ (as in the second paragraph of Definition **??**).

Exercise 2.6. Prove that the ring of integers $\mathbb{Z}$ is Noetherian.

Hilbthm **Theorem 2.7** (Hilbert). *If a commutative ring R is Noetherian, then (i) $R[x]$ is Noetherian (Hilbert's Basis Theorem) and (ii) $R[[x]]$ is Noetherian.*

Exercise 2.8. Prove or find a reference for proofs of (i) and (ii).

submoreexri 3. More examples of rings and ideals

exZi **Example 3.1.** For $R = \mathbb{Z}$, some ideals are: $(2) = 2\mathbb{Z} = \{0, 2, -2, 4, -4, \cdots\} = \{$ Even integers $\}$; $(6) = 6\mathbb{Z}$; $0\cdot\mathbb{Z} = \{0\}$.

idunR **Exercise 3.2.** Prove that if an ideal I of a ring R contains a unit u, then $I = R$. (Use the "precise" part of Definition **??**. Also see Example **??** for some ideas.)

idZprinc **Exercise 3.3.** Prove that in $\mathbb{Z}$ every ideal is generated by one element; that is, I an ideal of $\mathbb{Z} \implies I = n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

exZxid **Example 3.4.** Let $R = \mathbb{Z}[x] = \{$polynomials with coefficients in $\mathbb{Z}\}$. Some elements are $0, 1, x+1, x^2+1, 7x^3+x-2$. Here are some ideals: $I_1 = (x) = x\mathbb{Z}[x] = \{0, x, x^2+x, x^3+x, 7x^4+x^2-2x, \cdots\}$; $I_2 = (6) = \{0, 6, 6x+6, 6x^2+6, 42x^3+6x-12, \cdots\}$; $(x, 6) = x\mathbb{Z}[x] + 6\mathbb{Z}[x] = \{$ the set of all sums of elements from I_1 and $I_2\} = \{0, x, 6, x^2+x, x^2+x+6, x^3+x, x^3+x, 7x^4+x^2-2x, \cdots\} = \{$polynomials with the constant term a multiple of $6\}$.

exZloc **Example 3.5.** We define a new ring $R = \mathbb{Z}_{(2)}$, called "the localization of $\mathbb{Z}$ at (2)", by

$$\mathbb{Z}_{(2)} = \{\frac{a}{b} \in \mathbb{Q} \text{ in "lowest terms" with } b \textit{ not} \text{ a multiple of } 2\} = \{0 = \frac{0}{1}, \frac{1}{3}, \frac{2}{9}, \frac{5}{7}, \cdots\}.$$

Thus $\mathbb{Z}_{(2)}$ is a subset of $\mathbb{Q} = \{$ rational numbers $\}$, consisting of the fractions with odd denominators in lowest terms. Some ideals are $(2) = 2\mathbb{Z}_{(2)} = \{0 = \frac{0}{1}, \frac{2}{3}, \frac{4}{9}, \cdots\}$; $(6) = 6\mathbb{Z}_{(2)} = \{0, \frac{2}{3} = 6\cdot\frac{2}{9}, \frac{4}{9} = 6\cdot\frac{2}{2}7, \cdots\} = (2)$; $(4) = 4\mathbb{Z}_{(2)} = \{0, \frac{4}{3} = 4\cdot\frac{1}{3}, 4\cdots\} \subsetneq (2)$; $(3) = 3\mathbb{Z}_{(2)} = \{0, 1 = 3\cdot\frac{1}{3}, \frac{1}{3} = 3\cdot\frac{1}{9}, \cdots\} = \mathbb{Z}_{(2)}$.

Exercise 3.6. For $R = \mathbb{Z}/12\mathbb{Z}$, find all the distinct ideals. *Hint:* There are only 5.

Exercise 3.7. For $R = \mathbb{Z}[[x]]$, (a) Describe all the ideals that contain x. (b) Prove or disprove: Every ideal of $\mathbb{Z}[[x]]$ is generated by one element.

Remark 3.8. (1) Ideals of a ring can be "added" and "multiplied" to give other ideals. For ideals I and J of a ring R, we set

$$I + J \;=\; \{a + b \mid a \in I, b \in J\} \quad I \cdot J \;=\; \{ \text{ finite sums } \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_j \in J\}$$

(2) In $\mathbb{Z}$, $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$, whereas $2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z}$.

Exercise 3.9. Prove that if I and J are ideals of a ring R, then $I + J$ and $I \cdot J$ are also ideals of R. Use the "precise" part of Definition **??**, and do it rigorously. (First check that each of these is nonempty, then check (i) and (ii).)

pridsex

4. Prime ideals and examples

In certain rings (*Dedekind domains*) every ideal is a product of a group of special ideals, called *prime ideals* and the product has a certain uniqueness. We hope to demonstrate that these ideals are useful and lead to beautiful results even when there is no such factorization.

primeiddef

Definition 4.1. Let P be an ideal of a ring R such that (i) $P \neq R$ and (ii) If $a, b \in R$ satisfy $a \cdot b \in P$ then a or $b \in P$. Then P is a *prime* ideal.

primeidex

Examples 4.2.
1. For $R = \mathbb{Z}$, (2) is a prime ideal because $ab \in (2) \implies ab = 2c$, for some $c \in \mathbb{Z} \implies 2|(a \cdot b) \implies 2|a$ or $2|b$, since 2 is a prime element. Similarly for every prime integer p, (p) is a prime ideal of $\mathbb{Z}$. Also $\{0\} = (0)$ is a prime ideal, since $a, b \in \mathbb{Z}$ and $a \cdot b = 0 \implies a$ or $b = 0$.
2. For $R = \mathbb{Z}[x]$, (x) is a prime ideal. Why? If $f(x) \cdot g(x) \in (x)$, say $f(x) = a_n x^n + \cdots + a_0 \in (x)$ and $g(x) = b_m x^m + \cdots + b_0 \in \mathbb{Z}[x]$. Then $f(x)g(x)$ has constant term $0 \implies a_0 b_0 = 0 \implies a_0 = 0$ or $b_0 = 0 \implies f(x)$ or $g(x) \in (x)$.

Exercise 4.3. Prove $(x, 2)$, (2), and $(x + 1)$ are prime ideals of $\mathbb{Z}[x]$. (You may assume they are ideals.)

xonlyinQxx

Exercise 4.4. Prove (x) is the only non-zero prime ideal of $\mathbb{Q}[[x]]$.

1sppics

5. First Spec Pictures

For R a commutative ring, let $\operatorname{Spec} R := \{$ prime ideals of $R\}$, the *prime spectrum* of R, partially ordered by inclusion $\subseteq$.

hgtdimdef

Notation 5.1. The *height* of a prime ideal P in a commutative Noetherian ring R is the length h of a maximal chain $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_h = P$ ordered by inclusion of prime ideals that ends at P. In a Noetherian ring, this length is always finite. The "height" of an element u of a partially ordered set U is the length of a maximal chain of elements in the partial order leading up to the element u.[1] The *Krull dimension* of a ring R or of a partially ordered set U is the maximum height that occurs among all prime ideals, etc.

We like to draw pictures of the spectrum, where we put the height-zero prime ideals at the bottom and draw lines to higher prime ideals to show containments.

[1] In the partially ordered sets we encounter here, this length is always finite.

SpZpic **Examples 5.2.** (1) For $R = \mathbb{Z}$, $\text{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), \cdots\}$; that is, there are countably (infinitely) many height-one prime ideals in $\text{Spec}(\mathbb{Z})$—the ideals generated by the positive prime numbers, and a unique height-zero prime ideal $(0) = \{0\}$, which is less than every other prime ideal. The picture of the partially ordered set $\text{Spec}(\mathbb{Z})$ is shown in Diagram **??**.a. The lines signify containment; e.g. $(0) \subseteq (2)$, $(0) \subseteq (3)$ etc.

(2) Similarly, for $R = \mathbb{Q}[x]$, the partially ordered set $\text{Spec}(\mathbb{Q}[x])$ consists of the ideals generated by irreducible polynomials—they have height one—and the unique height-zero prime ideal $(0) = \{0\}$, which is less than every other prime ideal, as is shown in Diagram **??**.b.

(2) (3) (5) (7) $\cdots$ $\qquad$ (x) $(x+1)$ (x^2+2) $\cdots$

(0) $\qquad$ (0)

Diagram **??**.a. $\text{Spec}(\mathbb{Z})$ $\qquad$ Diagram **??**.b. $\text{Spec}(\mathbb{Q}[x])$

Since the two prime spectra shown are both countable, they exactly match up in a way that preserves the ordering. That is, $\text{Spec}(\mathbb{Z})$ is *order-isomorphic* to $\text{Spec}(\mathbb{Q}[x])$; they are essentially the same partially ordered set, and we write $\text{Spec}(\mathbb{Z}) \cong \text{Spec}(\mathbb{Q}[x])$. They each look like a countable fan.

Here are more one-dimensional spectra:

SpZloc **Examples 5.3.** Let $\mathbb{Z}_{(2)} = \{a/b \mid a, b \in \mathbb{Z} \text{ and } b \notin 2\mathbb{Z}\}$. That is, we enlarge $\mathbb{Z}$ to include $\mathbb{Z}$ and all fractions with odd denominators. The effect of this is that all the prime numbers of $\mathbb{Z}$ other than (2) become units; for example, $3^{-1} = 1/3$. *Facts:* (1) Every ideal of $\mathbb{Z}_{(2)}$ has the form $a\mathbb{Z}_{(2)}$, for some integer a. (2) The prime ideals of $\mathbb{Z}_{(2)}$ are $a\mathbb{Z}_{(2)}$, where a is a prime number in $\mathbb{Z}_{(2)}$ and $a\mathbb{Z}_{(2)} \neq \mathbb{Z}_{(2)}$. It follows from these facts that $\mathbb{Z}_{(2)}$ has only one prime ideal besides (0), namely $2\mathbb{Z}_{(2)}$. Similarly $\mathbb{Z}_{(3)}$ is all rational numbers, fractions $\frac{a}{b}$ of integers a and b, such that with the fraction in lowest terms the denominator b is not a multiple of 3; the only prime ideals of $\mathbb{Z}_{(3)}$ are (0) and $3\mathbb{Z}_{(3)}$. To extend this idea, we let $\mathbb{Z}_{(2)\cup(3)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \notin 2\mathbb{Z} \text{ and } b \notin 3\mathbb{Z}\}$. The only prime ideals of $\mathbb{Z}_{(2)\cup(3)}$ are (0), $2\mathbb{Z}_{(2)\cup(3)}$ and $3\mathbb{Z}_{(2)\cup(3)}$. We show these spec pictures below:

(2) $\qquad$ (2) (3)

(0) $\qquad$ (0)

Diagram **??**.a. $\text{Spec}(\mathbb{Z}_{(2)})$ $\qquad$ Diagram **??**.b. $\text{Spec}(\mathbb{Z}_{(2)\cup(3)})$

By the discussion above, the prime spectrum of $\mathbb{Z}_{(3)}$ is order-isomorphic to $\text{Spec}(\mathbb{Z}_{(2)})$. The prime spectrum of $\mathbb{Q}[[x]]$ is also order-isomorphic to $\text{Spec}(\mathbb{Z}_{(2)})$ by Exercise **??**.

ExSpZ2x **Exercise 5.4.** Make diagrams of $\text{Spec}(\mathbb{Z}_{(2)}[x])$ and $\text{Spec}(\mathbb{Z}_{(2)}[[x]])$. Justify.

Note. These and other topics are continued in the Research Lecture.