21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

25- Wednesday November 2, 2011.

Definition 25.1: The ring $R((x))$ of *formal Laurent series* with coefficients in R is the set of elements of R indexed by $\mathbb{Z}$, i.e. $\{a_n \mid n \in \mathbb{Z}\}$, such that $a_n = 0$ for all $n \leq m$ for some $m \in \mathbb{Z}$, and it is interpreted as $\sum_{n\in\mathbb{Z}} a_n x^n$.

For $A = \sum_{n\in\mathbb{Z}} a_n x^n \in R((x))$ and $B = \sum_{n\in\mathbb{Z}} b_n x^n \in R((x))$, one has $A + B = C = \sum_{n\in\mathbb{Z}} c_n x^n$ and $A\,B = D = \sum_{n\in\mathbb{Z}} d_n x^n$, with $c_n = a_n + b_n$ for all $n \in \mathbb{Z}$, and $d_n = \sum_{j\in\mathbb{Z}} a_j b_{n-j}$ for all $n \in \mathbb{Z}$, noticing that the sum defining each d_n only has a finite number of non-zero terms.

The valuation of a non-zero element is the largest $m \in \mathbb{Z}$ such that $a_n = 0$ for all $n < m$.

Remark 25.2: If F is a field, then $F[[x]]$ is an integral domain, and its field of fractions is isomorphic to $F((x))$: indeed, a non-zero element in $R[[x]]$ has the form $a_m x^m(1 + B)$ with $a_m \neq 0$ and $val(B) \geq 1$, and for defining its inverse one needs to notice that $a_m^{-1} \in F$, $x^{-m} \in F((x))$, and the inverse of $1 - B \in F[[x]]$ is $1 + B + B^2 + \ldots \in F[[x]] \subset F((x))$. Conversely, any non-zero element $A \in F((x))$ with $val(A) < 0$ may be written as $\frac{x^m A}{x^m}$ with $m = -val(A)$ and one has $x^m A \in F[[x]]$.

Remark 25.3: The motivation for the ring of formal power series $R[[x]]$ and the ring of formal Laurent series $R((x))$ is to mimic at an algebraic level something done in analysis concerning Taylor expansions of differentiable functions in an open set of $\mathbb{R}$ or of $\mathbb{C}$. Although every function f which is indefinitely differentiable around a point x_0 can be well approached in a small ball $B(x_0, r)$ by the Taylor expansion of f at order n with an error in r^{n+1}, the Taylor series might diverge at any other point than x_0; if the Taylor expansion converges at other points it defines an *analytic function* in the case of $\mathbb{R}$, called an *holomorphic function* in the case of $\mathbb{C}$, and the radius of convergence of the power series is limited by the nearest singularity in the complex plane: for example, the Taylor expansion of $f(x) = \frac{1}{1+x^2}$ (which is analytic on the whole $\mathbb{R}$) at $x_0 \in \mathbb{R}$ has a radius of convergence $\sqrt{1 + x_0^2}$, which is the distance to the two singularities of f in $\mathbb{C}$, which are $\pm i$.

If f is holomorphic in a disc minus its center z_0, it might be that z_0 is a *removable singularity*, i.e. one can extend f by continuity at z_0; it might be that z_0 is a *pole*, i.e. the function tends to ∞ when one approaches z_0,[1] and in this case each pole has a finite order $m \geq 1$ so that $(z - z_0)^m f$ is continuous and non-zero at z_0, and it is at such poles that one uses a “Laurent” series (introduced before LAURENT by WEIERSTRASS); it might be that z_0 is an *essential singularity*, i.e. the function has no limit when one approaches z_0, and in this case the set of values taken by f in any small pointed disc around z_0 is dense in $\mathbb{C}$, as was proved by CASORATI and then WEIERSTRASS, a result then improved by PICARD,[2] who proved that f takes all values of $\mathbb{C}$ except possibly one in any small pointed disc around z_0.[3]

Definition 25.4: In a ring R, an ideal P is called *prime* if $P \neq R$ and if for any two ideals A, B of R satisfying $A\,B \subset P$ one has $A \subset P$ or $B \subset P$ (recall that $A\,B$ is the set of finite sums of terms like $a\,b$ with $a \in A$ and $b \in B$).

An ideal M is called *maximal* if it is a proper ideal (i.e. $M \neq R$) and it is maximal (for inclusion) among proper ideals (i.e. $M \subset N$ and N is a proper ideal, then $N = M$).

Remark 25.5: A prime element was defined at Definition 23.3 for a commutative unital ring R, by $q \neq 0$, q not a unit, and q divides $a\,b$ implies that either q divides a or q divides b. Since the definition mentions units, the ring has to be unital, but one could avoid this hypothesis by asking that $(q) \neq R$, which makes sense in a general ring, and for a commutative unital ring it is equivalent to q not being a unit, since $(q) = \{r\,q \mid r \in R\}$ in this case.

Lemma 25.6: In a commutative unital ring R, a non-zero element $q \in R$ is prime if and only if the ideal (q) which it generates is a prime ideal.

[1] One works with $\mathbb{C}\,P^1$, the projective 1-dimensional space, which adds to $\mathbb{C}$ only one point at infinity.
[2] Charles Émile PICARD, French mathematician, 1856–1941. He worked in Toulouse and in Paris, France.
[3] For example, $f(z) = e^{1/z}$ has an essential singularity at 0, and it avoids the value 0.

Proof: Suppose (q) is a prime ideal, and q divides $a\,b$, so that $a\,b \in (q)$, but in a commutative unital ring one has $(a)\,(b) = (a\,b)$, so that $(a)\,(b) \subset (q)$, hence either $(a) \subset (q)$ or $(b) \subset (q)$, but $(x) \subset (q)$ implies $x \in (q)$, i.e. q divides x.

Suppose q is prime, and two ideals A, B are such that $A\,B \subset (q)$: if one does not have $A \subset (q)$, there exists $a \in A \setminus (q)$ and since for every $b \in B$ one has $a\,b \in A\,B \subset (q)$ and q does not divide a, q must then divide b, so that $b \in (q)$, hence $B \subset (q)$.

Lemma 25.7: In a commutative unital ring R, an ideal P is prime if and only if for all $a, b \in R$, $a\,b \in P$ implies $a \in P$ or $b \in P$; in particular, the trivial ideal $\{0\}$ is prime if and only if R is an integral domain.
Proof: If P is prime and $a\,b \in P$ then $(a)(b) = (a\,b) \subset P$, so that $(a) \subset P$ or $(b) \subset P$, i.e. $a \in P$ or $b \in P$. Conversely, if A and B are ideals such that $A\,B \subset P$ but $A \not\subset P$, then there exists $a \in A \setminus P$ and for all $b \in B$ one has $a\,b \in P$, so that $b \in P$, hence $B \subset P$.

In particular, $\{0\}$ is a prime ideal if and only if there is no zero-divisor, and since R is a commutative unital ring, it means that it is an integral domain.

Lemma 25.8: If R is a commutative unital ring, and J is a proper ideal of R (i.e. $J \neq R$), then the quotient R/J is an integral domain if and only if J is prime.
Proof: Since R/J is a commutative unital ring, it is an integral domain if and only if it has no zero-divisor, but a zero-divisor is $a\,J$ with $a \notin J$ for which there exists $b\,J$ with $b \notin J$ such that $a\,b \in J$, i.e. J is not prime.

Remark 25.9: Since the initial reason for a general definition of primes was to extend the notion of primes in $\mathbb{Z}$ (actually in $\mathbb{N}$) to a general ring, it is useful to observe that, when applied to $\mathbb{Z}$, the general definition gives either a prime p or $-p$.[4]

The general definition of irreducible elements applied to $\mathbb{Z}$ also gives $\pm p$ for a prime p, but the initial difficulty was to observe that there are rings where unique factorization does not hold, and that a definition of irreducible elements is needed.

As mentioned at the end of lecture 21, $(4+\sqrt{10})\,(4-\sqrt{10}) = 6 = 2\cdot 3$ in $\mathbb{Z}[\sqrt{10}]$, and $4+\sqrt{10}, 4-\sqrt{10}, 2, 3$ are irreducible. Since multiples of 2 have the form $a + b\sqrt{10}$ with a, b even, neither $4+\sqrt{10}$ nor $4-\sqrt{10}$ are multiples of 2, hence 2 is not prime in $\mathbb{Z}[\sqrt{10}]$; similarly, 3 is not prime in $\mathbb{Z}[\sqrt{10}]$, since neither $4+\sqrt{10}$ nor $4-\sqrt{10}$ are multiples of 3, which have the form $a+b\sqrt{10}$ with a, b multiple of 3. $4+\sqrt{10}$ and $4-\sqrt{10}$ are not prime either since they divide neither 2 nor 3, and it is checked more easily by noticing that $N(4\pm\sqrt{10}) = 6$ while $N(2) = 4$ and $N(3) = 9$, which are not multiples of 6, where $N(a+b\sqrt{10}) = a^2 - 10b^2$, which satisfies $N(z_1 z_2) = N(z_1)\,N(z_2)$ for all $z_1, z_2 \in \mathbb{Z}[\sqrt{10}]$.

Lemma 25.10: If R is a commutative unital ring, and J is a proper ideal of R (i.e. $J \neq R$), then the quotient R/J is a field if and only if J is maximal.
Proof: If J is maximal and $a \notin J$, then the ideal generated by $\{a\} \cup J$ is R (since it contains J strictly and J is maximal), so that 1 can be expressed as $r_0 a + j$ with $j \in J$ for some $r_0 \in R$ (but $r_0 \notin J$ since $J \neq R$), and this shows that the inverse of $a + J$ in the quotient is $r_0 + J$, so that every non-zero element of R/J has an inverse, hence R/J is a field. Conversely, if R/J is a field and $a \notin J$, then $a + J$ has an inverse $b + J$ in the quotient, so that $a\,b \in 1 + J$, hence the ideal generated by a and J contains 1, so that it is R, which shows that there cannot be a proper ideal containing J strictly (since it would contain some $a \notin J$), i.e. J is maximal.

Remark 25.11: If R is a commutative unital ring, every maximal (proper) ideal is prime, since every field is an integral domain, and the converse is obviously not true: for example if $D \in \mathbb{Z}$ is not a square, then $\mathbb{Z}[\sqrt{D}]$ is an integral domain, but not a field since $z = a + b\sqrt{D}$ is a unit if and only if $N(z) = \pm 1$, with $N(a+b\sqrt{D}) = a^2 - D\,b^2$, so that since $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[x]/(x^2 - D)$, one finds that $(x^2 - D)$ is a prime ideal but not a maximal ideal of $\mathbb{Z}[x]$.

Of course, each proper ideal J is contained in a maximal ideal M by Zorn's lemma, and the hypothesis of Zorn's lemma consists in checking that if $J_i, i \in I$, is a totally ordered family of proper ideals (indexed by a nonempty set I) then it has a least upper bound (in the ordered set of proper ideals), which is simply $\bigcup_{i\in I} J_i$: the fact that it is an additive subgroup of R relies on the fact that if $i_1 \neq i_2$ one of the two ideals

[4] General definitions cannot actually differentiate between the various associates of an element.

J_{i_1} and J_{i_2} is included in the other, and the union is a proper ideal, since if it contained 1, then 1 would belong to one J_i, which then would not be proper.

In a field F the only ideals are $\{0\}$ and F, and $\{0\}$ is both prime and maximal.

Remark 25.12: If R is an integral domain, every prime element is irreducible: if $p = a\,b$ then $p \mid a$ or $p \mid b$, and if $p \mid a$, one has $a = p\,x$, so that $p = a\,b = p\,x\,b$, i.e. $1 = x\,b$, so that b is a unit.

The converse is not true, since one has seen a few irreducible elements of $\mathbb{Z}[\sqrt{10}]$ which are irreducible but not prime, and for $D \in \mathbb{Z}$ not a square $\mathbb{Z}[\sqrt{D}]$ is an integral domain.

The next step will be to compare irreducible elements and prime elements, and define what a UFD (unique factorization domain) is.