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

20- Friday October 14, 2011.

Remark 20.1: In vector spaces (over a field F) one has a notion of *dimension*, so that inside a subspace of finite dimension d, all the proper subspaces have a dimension $< d$, but this property is not true for modules (over a ring R), and a ring R (which is an R-module) may be finitely generated (by 1 if it is unital) and have an ideal (which is an R-submodule) which is not finitely generated: in $R = \mathbb{Z}[x_1, x_2, \ldots]$, the (unital) ring of all polynomials in infinitely many variables (but a given polynomial is a finite sum of monomials, hence uses only a finite number of variables), the ideal $J = (x_1, x_2, \ldots)$ is not finitely generated. Indeed, if it was generated by $\{P_1, \ldots, P_k\}$ it would be generated by $\{x_1, \ldots, x_m\}$ if the variables appearing in $P_1, \ldots, P_k$ have an index $\leq m$, but all polynomials in $(x_1, \ldots, x_m)$ give the value 0 if one evaluates them at $x_1 = \ldots = x_m = 0$ and $x_{m+1} = 1$, while x_{m+1} is not 0 at this point, so that $x_{m+1} \notin (x_1, \ldots, x_m)$.

Definition 20.2: If R is an integral domain, its *field of fractions* F is defined as the equivalence classes of pairs (a, b) with $a, b \in R$ and $b \neq 0$ for the equivalence relation $(a, b)\mathcal{R}(c, d)$ if and only if $a\,d = b\,c$ (similar to $\frac{a}{b} = \frac{c}{d}$ for usual fractions). On F, addition corresponds to $(a, b) + (c, d) = (a\,d + b\,c, b\,d)$ (similar to $\frac{a}{b} + \frac{c}{d} = \frac{a\,d+b\,c}{b\,d}$ for usual fractions), and multiplication to $(a, b)\,(c, d) = (a\,c, b\,d)$ (similar to $\frac{a}{b}\,\frac{c}{d} = \frac{a\,c}{b\,d}$ for usual fractions), which are compatible with the equivalence relation $\mathcal{R}$, and it makes F a field.

Remark 20.3: It was mentioned that since addition on $\mathbb{N}$ is commutative, associative, and regular (i.e. $a + x = a + y$ implies $x = y$), it should have been natural to invent $\mathbb{Z}$ as the set of pairs (a, b) with the intuition that it means $a - b$, with the interpretation that it is like for a merchant to measure his wealth by his availablecash amount $a \in \mathbb{N}$ and the amount $b \in \mathbb{N}$ which he has borrowed (in an ideal world where one can borrow without interest).

Once one notices what is used in the construction, the same idea applies to $\mathbb{N}^\times$ for multiplication and creates the multiplicative group $\mathbb{Q}_+$, but then there is a natural symmetrization for addition on $\mathbb{Q}_+$ or a natural symmetrization for multiplication on $\mathbb{Z}$, which both permit to define $\mathbb{Q}$. If one looks at what is needed for this scheme to work, one arrives naturally at the situation described in Definition 20.2 for any integral domain, but one can be more general.

If R is a commutative ring and $D \subset R$ is non-empty, stable by multiplication (i.e. $d_1, d_2 \in D$ implies $d_1 d_2 \in D$) and contains no zero-divisor, it is natural to construct a commutative unital ring (denoted $D^{-1}R$) which contains (an isomorphic copy of) R as a subring and such that every element of D is a unit in $D^{-1}R$: the equivalence relation $\mathcal{R}$ is defined on $R \times D$ (with (r, d) intuitively meaning $\frac{r}{d}$) by $(r_1, d_1)\mathcal{R}(r_2, d_2)$ meaning $r_1\,d_2 = r_2\,d_1$, addition is defined on $R \times D$ by $(r_1, d_1) + (r_2, d_2) = (r_1 d_2 + r_2 d_1, d_1 d_2)$ and multiplication is defined on $R \times D$ by $(r_1, d_1) \cdot (r_2, d_2) = (r_1 r_2, d_1 d_2)$, and both these operations extend to the quotient $R \times D/\mathcal{R}$, and give a structure of commutative unital ring; the element 1 is the equivalence class of (d, d) for any $d \in D$ (and one has $(d_1, d_1)\,\mathcal{R}\,(d_2, d_2)$ for all $d_1, d_2 \in D$); that $D^{-1}R$ contains (an isomorphic copy of) R is seen by mapping $r \in R$ to the equivalence class of $(r\,d, d)$ (which intuitively means $\frac{r\,d}{d}$) for any if $d \in D$ (and one has $(r\,d_1, d_1)\,\mathcal{R}\,(r\,d_2, d_2)$ for all $d_1, d_2 \in D$); that elements of D become units in $D^{-1}R$ is related to the fact that the inverse of the equivalent class of $(d\,d_1, d_1)$ is the equivalent class of $(d_2, d\,d_2)$ for any $d_1, d_2 \in D$. For example, if $R = \mathbb{Z}$ and $D = \{2, \ldots, 2^n, \ldots\}$, then one obtains the elements of $\mathbb{Q}$ whose reduced form has a denominator which is a power of 2. Definition 20.2 corresponds to the possibility of taking $D = R \setminus \{0\}$, and in this case $D^{-1}R$ is a field.

Of course, Definition 20.2 (or the generalization just mentioned) makes sense if one checks what it claims, that $\mathcal{R}$ is an equivalence relation on $R \times D$, that the addition or the multiplication of two elements of $R \times D$ gives something equivalent if one replaces each of the two elements by an equivalent element, that associativity holds for addition and for multiplication, that 0 corresponds to $(0, d)$ and $-(r, d)$ corresponds to $(-r, d)$, and that multiplication is distributive with respect to addition: it is a little tedious but it presents no real difficulty.

Definition 20.4: If R_1, R_2 are two rings, a mapping f from R_1 into R_2 is a *ring-homomorphism* if $f(x+y) = f(x) + f(y)$ for all $x, y \in R_1$, and $f(x\,y) = f(x)\,f(y)$ for all $x, y \in R_1$. The *kernel* of f is $\{x \in R_1 \mid f(x) = 0\}$.

Remark 20.5: If f is a ring-homomorphism from R_1 into R_2, then its kernel $ker(f) = f^{-1}(\{0\})$ is an ideal of R_1 (since $f(a) = 0$ implies $f(r\,a) = f(a\,s) = 0$ for all $r, s \in R$), and its image $f(R_1)$ is a subring of R_2, so that f induces an injective ring-homomorphism from the quotient $R_1/ker(f)$ into R_2, hence $R_1/ker(f)$ is isomorphic to the image $f(R_1)$ as rings (first isomorphism theorem).

A ring-homomorphism f from R_1 into R_2 is an homomorphism of the additive groups, so that $f(0) = 0$ and $f(-r) = -f(r)$ for all $r \in R_1$, but one should pay attention that R_1 may be unital while R_2 may not be unital, so that one may wonder what $f(1_{R_1})$ is. For example, $R_1 = \mathbb{Z}_5$ is a field, and $R_2 = 2\mathbb{Z}_{20}$ is a ring which is not unital, and the mapping defined by $f(x) = 16x \pmod{20}$ is a ring homomorphism from R_1 into R_2, because $16 \cdot 5 = 0 \pmod{20}$ and $16x \cdot 16y = 16x\,y \pmod{20}$ for all x, y (since $256 = 16 \pmod{20}$; one has $f(R_1) = 4\mathbb{Z}_{20}$, and $f(1_{R_1}) = 1_{f(R_1)} = 16$.

In general $f(1_{R_1})$ is an element of R_2 which is *idempotent*, i.e. satisfies $r^2 = r$, since $1^2 = 1$ implies $\big(f(1)\big)^2 = f(1)$. If R is an integral domain then only 0 and 1_R are idempotent (since $r\,(r-1) = 0$ implies $r = 0$ or $r - 1 = 0$), but if $n = m_1 m_2$ with $m_1, m_2 \geq 2$ and relatively prime, then $\mathbb{Z}_n$ (which is commutative and unital) has (at least) two idempotent elements different from 0 or 1: $a = 0 \pmod{m_1}$ and $a = 1 \pmod{m_2}$ gives a idempotent; $b = 1 \pmod{m_1}$ and $b = 0 \pmod{m_2}$ gives b idempotent. Actually, if R is commutative and $r \in R$ is idempotent, the ideal $J = (r)$ is unital with $1_J = r$ (since $r\,(r\,x) = r\,x$ for all $x \in R$), and defining f by $f(x) = r\,x$ gives a ring-homomorphism from R into J.

If V is a vector space of dimension ≥ 2 over a field F, then $R = L(V;V)$ is a non-commutative unital ring (with identity denoted I), and a nilpotent element P is called a *projection*: $X = ker(P)$ and $Y = ker(I - P)$ are supplementary vector subspaces (i.e. such that $X \cap Y = \{0\}$ and $X + Y = V$) so that every $v \in V$ has a unique decomposition $x = (I - P)\,x + P\,x$ into an element of X (which is $x - P\,x$) plus an element of Y (which is $P\,x$). In general, if V_1 is a subspace, a projection onto V_1 is specified as being parallel to a subspace V_2 which is supplementary to V_1, and P is defined by $P\,v = v$ if $v \in V_1$ and $P\,v = 0$ is $v \in V_2$.

Remark 20.6: If two elements a, b in a ring R commute, then one has the binomial formula $(a + b)^k = \sum_{j=0}^{k} \binom{k}{j} a^j b^{k-j}$, obtained in developing $(a + b) \cdots (a + b)$ and observing that (because a and b commute) there are as many terms $a^j b^{k-j}$ as subsets of size j in $\{1, \ldots, k\}$, but if R is not unital, one may prefer to write it $(a + b)^k = a^k + \sum_{j=1}^{k-1} \binom{k}{j} a^j b^{k-j} + b^k$ for avoiding a^0 and b^0, since one cannot use the convention that it means 1_R which does not exist, or one may say that the convention is that $a^0 x$ means x for all $x \in R$.

If R is a commutative unital ring of *prime* characteristic p, then $(a + b)^p = a^p + b^p$ for all $a, b \in R$, because one has $\binom{p}{k} = 0 \pmod{p}$ if $k \neq 0, p$ (since p is prime), and $p\,r = 0$ for all $r \in R$.

Definition 20.7: An integral domain R is an *Euclidean domain* if there is a function V (sometimes called valuation,[1] or norm,[2] or gauge) from $R \setminus \{0\}$ into $\mathbb{N}$ such that, for all $a, b \in R$ with $b \neq 0$ one can write $a = b\,q + r$ with either $r = 0$ or $V(r) < V(b)$ (one usually adds $V(x) \leq V(x\,y)$ for all $x, y \neq 0$, shown to be superfluous by K. Rogers & E. G. Straus,[3,4] by replacing V by W defined by $W(x) = \min_{z \neq 0} V(x\,z)$.)

Remark 20.8: This definition, obviously suggested by the Euclidean division algorithm in $\mathbb{Z}$, may have been introduced by Gauss for what one now calls the *Gaussian integers*, $\mathbb{Z}[i] = \{z = a + i\,b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Definition 20.9: A *polynomial* P over a ring R is a list $(a_0, \ldots, a_n, \ldots)$ with $a_i \in R$ for all $i \geq 0$, and only a finite number of a_i are $\neq 0$, and one also writes $P = \sum_{n \geq 0} a_n x^n$. The *ring of polynomials* $R[x]$ is the set of all polynomials over R equipped with addition and multiplication defined as follows:[5] if $P = \sum_n a_n x^n$

[1] The term valuation will be used for polynomials with a different meaning, while V will be the degree of the polynomial.

[2] In algebra, the term "norm" is used with a different meaning than in analysis, where a norm $||\cdot||$ is defined on a vector space V over $\mathbb{R}$ of $\mathbb{C}$, and satisfies $||x|| > 0$ if $x \in V \setminus \{0\}$, $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$, and $||\lambda\,v|| = |\lambda|\,||v||$ for all $v \in V$ and all scalars λ (in $\mathbb{R}$ or $\mathbb{C}$.

[3] Kenneth Rogers, English-born mathematician, 1930–2010. He worked at University of Hawaii at Manoa, Honolulu, HI.

[4] Ernst Gabor Straus, German-born mathematician, 1922–1983. He worked at UCLA (University of California at Los Angeles) Los Angeles, CA.

[5] Checking that $R[x]$ has all the properties for being a ring is not difficult, but it is a little tedious.

and $Q = \sum_n b_n x^n$, then $P+Q = \sum_n c_n x^n$ and $P\,Q = \sum_n d_n x^n$, with $c_n = a_n + b_n$ for all $n \ge 0$, and $d_n = \sum_{j=0}^n a_j b_{n-j}$ for all $n \ge 0$.[6]

For $P \ne 0$, the *degree* of P, denoted $deg(P)$, is the highest n for which $a_n \ne 0$, and the *valuation* of P, denoted $val(P)$, is the smallest n for which $a_n \ne 0$, so that $val(P) \le deg(P)$ for $P \ne 0$. For $P, Q \ne 0$, one has $deg(P+Q) \le \max\{deg(P), deg(Q)\}$ and $deg(P\,Q) \le deg(P) + deg(Q)$, $val(P+Q) \ge \min\{val(P), val(Q)\}$ and $val(P\,Q) \ge val(P) + val(Q)$.

If R is unital, a non-zero polynomial P is *monic* if a_n is a unit for $n = deg(P)$, but one often impose $a_n = 1$ for monic polynomials.

Remark 20.10: The degree of a non-zero constant (i.e. $P = a_0 \ne 0$) is 0, and some authors consider that the zero polynomial has degree 0, but a better convention is to consider that $deg(0) = -\infty$ and $val(0) = +\infty$ (so that $deg(0) < val(0)$), and this permits to have $deg(P\,Q) = deg(P) + deg(Q)$ and $val(P\,Q) = val(P) + val(Q)$ if R has no zero divisors, for all $P, Q \in R[x]$. One reason for this convention comes from the generalizations to the ring of *formal power series* $R[[x]]$, and the ring of *formal Laurent series* $R((x))$.[7]

Lemma 20.11: If R is commutative, then $R[x]$ is commutative. If R is unital, then $R[x]$ is unital, and a product of monic polynomials is monic. If R has no zero divisor, then $R[x]$ has no zero divisor, and $deg(P\,Q) = deg(P) + deg(Q)$ for non-zero polynomial $P, Q \in R[x]$. If R is an integral domain, then $R[x]$ is an integral domain.
Proof: Of course, the identity in $R[x]$ is $1 = (1, 0, \ldots, 0, \ldots)$. If $n = deg(P)$ and $m = deg(Q)$ then $deg(P\,Q) \le m + n$ and $d_{m+n} = a_m b_n$, which is $\ne 0$ if R has no zero divisor, in which case $deg(P\,Q) = m + n$; similarly, $a_m b_n$ is a unit if a_m and b_n are units.

[6] Notice that x is not an element of R, and that it commutes with all elements of R; if R is unital, then $x = (0, 1, 0, \ldots, 0, \ldots) \in R[x]$.

[7] Pierre Alphonse LAURENT, French mathematician, 1813–1854. Laurent series are named after him, although WEIERSTRASS had introduced the notion in 1841, two years before him.