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

19- Wednesday October 12, 2011.

Definition 19.1: The *characteristic* of a unital ring R is the smallest $n \geq 2$ such that $n\,1 = 0$ if there exists a non-zero integer m with $m\,1 = 0$, or it is 0.

Remark 19.2: For $n \geq 2$, the characteristic of $\mathbb{Z}_n$ is n; for $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the characteristic is 0.

Using $(m_1 1)\,(m_2 1) = (m_1 m_2)\,1$, one deduces that if R is unital with no zero-divisor (in particular for an integral domain), then the characteristic is either 0 or a prime p.

Definition 19.3: In a ring R, if $A_1, \ldots, A_m$ are ideals (with $m \geq 2$), then $A_1 \cdots A_m$ denotes the sums of products of the form $a_1 \cdots a_m$ with $a_j \in A_j$ for $j = 1, \ldots, m$.[1] In particular, if A is an ideal of R, then $A^m = \left\{ \sum_{i=1}^{n} a_{i,1} \cdots a_{i,m} \mid a_{i,j} \in A \text{ for } i = 1, \ldots, n, j = 1, \ldots, m, n \geq 1 \right\}$.

Remark 19.4: If R is commutative and unital,[2] $A_1 \cdots A_m$ is the smallest ideal containing $A_1, \ldots, A_m$, since any ideal containing $A_1, \ldots, A_m$ must contain terms like $a_1 \cdots a_m$ with $a_j \in A_j$ for $j = 1, \ldots, m$, hence sums of such products, and the set of such finite sums is an ideal.

Definition 19.5: If $x, y \in R$ and R is a commutative ring, one says that x *divides* y, noted $x \mid y$, if there exists $r \in R$ such that $r\,x = y$. One says that x and y are *associates* if x divides y and y divides x.

Remark 19.6: If R is commutative and unital, then x divides y if and only if $y \in (x)$, since in this case the ideal generated by x is $(x) = \{r\,x \mid r \in R\}$, and one deduces that x and y are associates if and only if $(x) = (y)$.

In $2\mathbb{Z}_{16}$, which is not unital (since $2x\,2y = 2y \pmod{16}$ is false for y odd), one has $6 + 6 + 6 = 2 \pmod{16}$, so that $2 \in (6)$, hence $(2) = (6) = 2\mathbb{Z}_{16}$, but 6 does not divide 2, since $2x \cdot 6 = 2 \pmod{16}$ is false for all x.

If R is an integral domain (i.e. commutative, unital, and with no zero-divisor), then x and y are associates if and only if $y = x\,u$ for a unit u (so that $x = y\,u^{-1}$ and u^{-1} is a unit), since when x, y are non-zero, $y = x\,u$ and $x = y\,v$ imply $u\,v = 1$.

In $\mathbb{Z}_{12}$ (which is commutative and unital, but not an integral domain), 4 divides 8, since $2 \cdot 4 = 8$ (modulo n for all n), but also 8 divides 4, since $2 \cdot 8 = 16 = 4 \pmod{12}$. However 2 is not a unit.

Definition 19.7: A ring R is *Noetherian* if it satisfies the *ascending chain condition* on ideals,[3] i.e. if $J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$ are ideals of R, then there exists n with $J_n = J_{n+1} = \cdots$, and one also says that every increasing sequence of ideals becomes constant; equivalently, every non-empty family of ideals has a maximal element.[4] A ring R is *Artinian* if it satisfies the *descending chain condition* on ideals of R, i.e. if $\cdots \subset J_k \subset \cdots \subset J_2 \subset J_1$ are ideals, then there exists n with $\cdots = J_{n+1} = J_n$,[5] and one also says that every decreasing sequence of ideals becomes constant; equivalently, every non-empty family of ideals has a minimal element.

Lemma 19.8: A ring R is Noetherian if and only if every ideal of R is finitely generated (so that principal ideal rings, and in particular PID, are Noetherian).

---

[1] Recall that for subgroups $H, K \leq G$, $H\,K$ is just the set of elements of the form $h\,k$ with $h \in H, k \in K$.

[2] If R is not commutative, then one must also consider for any permutation σ (of $\{1, \ldots, n\}$) terms $a_1 \cdots a_m$ with $a_j \in A_{\sigma(j)}$ for $j = 1, \ldots, m$.

[3] Emmy Amalie NOETHER, German-born mathematician, 1882–1935. Until 1933 she worked at Georg-August-Universität, Göttingen, Germany, and then in Bryn Mawr, PA.

[4] If a non-empty family $\mathcal{I}$ of ideals had no maximal element, one would pick any $J_1 \in \mathcal{I}$, and since J_1 is not maximal there would exist $J_2 \neq J_1$ with $J_1 \subset J_2$, and by induction one would obtain an increasing sequence of ideals which would not become constant, since all its terms are distinct. Conversely, any increasing sequence of ideals $J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$ contains a maximal element, which is J_n for some n, so that $J_{n+k} = J_n$ for all $k \in \mathbb{N}$.

[5] Emil ARTIN, Austrian-born mathematician, 1898–1962. He worked in Hamburg, Germany, at University of Notre Dame, IN, at Indiana University, Bloomington, IN, and at Princeton University, Princeton, NJ.

Proof: Assumes that R is Noetherian but there exists an ideal J of R which is not finitely generated, then one constructs by induction a sequence $r_k \in J$, $k \geq 1$, such that $r_{k+1} \notin (r_1, \ldots, r_k)$ for all $k \geq 1$, and then $J_k = (r_1, \ldots, r_k)$ would be an increasing sequence of ideals which is not eventually constant.

If every ideal is finitely generated and $J_1 \subset J_2 \subset \ldots$ is an increasing sequence of ideals, one defines $J_\infty = \bigcup_{k \geq 1} J_k$, so that J_∞ is an ideal,[6] and by hypothesis J_∞ is generated by a finite set X, but X being finite one has $X \subset J_m$ for some m large enough, and since it implies $(X) \subset J_m$, one deduces that $J_n = J_m$ for all $n \geq m$.

Remark 19.9: $\mathbb{Z}$ is not Artinian (since (2^n) is a decreasing sequence of ideals which does not become constant), but it is Noetherian since it is a PID: indeed, an ideal being an additive subgroup has the form $n\,\mathbb{Z}$ for some n, and $n\,\mathbb{Z} = (n)$. It is useful to recall the proof based on the Euclidean division algorithm: if $J \subset \mathbb{Z}$ is an ideal, either it is $\{0\}$ or it contains a positive integer, so that it contains a smallest positive integer $d \in J$, and then any $n \in \mathbb{Z}$ may be written as $n = d\,q + r$ for a *quotient* $q \in \mathbb{Z}$ and a *remainder* $r \in \{0, \ldots, r-1\}$, but then $r \in J$ (since n and $d\,q$ belong to J), so that r must be 0 by definition of d.

The property of $\mathbb{Z}$ being a PID easily gives Bachet's theorem,[7] that if a, b are positive integers and their gcd (greatest common divisor) is d, then there exists $x, y \in \mathbb{Z}$ such that $a\,x + b\,y = d$. One should observe that the usual way to compute the gcd is to look at the factorization using a common list of (distinct) prime numbers $p_1, \ldots, p_k$, so that $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ with $\alpha_j, \beta_j \geq 0$ and $\max\{\alpha_j, \beta_j\} \geq 1$ for $j = 1, \ldots, k$, and then the gcd (a, b) is $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ with $\gamma_j = \min\{\alpha_j, \beta_j\}$ for $j = 1, \ldots, k$. The theorem of Bachet then introduces addition in a problem where everyone was thinking in term of multiplication, a little like for the *Goldbach conjecture*,[8] that every even integer ≥ 4 is the sum of two primes, an additive question about primes, whose definition only involves multiplication.

Since $a = b\,q + r$ implies that the ideal (a, b) generated by a and b coincides with (b, r) generated by b and r,[9] it gives a quite efficient algorithm for finding the gcd of two numbers, with a number of operations estimated by Lamé: if $a, b \leq Fib_n$, the nth Fibonacci number, the number of operations is bounded by n; in contrast, no efficient algorithm for factorization of integers is known, and cryptography uses this fact extensively.

Remark 19.10: It will be seen that for a field F the ring $F[x]$ of polynomials in one variable with coefficients in F is a PID, and even an Euclidean domain, but the ring $F[x_1, x_2]$ of polynomials in two variables with coefficients in F is not a PID, and since it is isomorphic to $R[x_2]$ with $R = F[x_1]$, one deduces that if a ring R is a PID, then the ring $R[x]$ of polynomials in one variable with coefficients in R is not necessarily a PID. It is then useful to find properties $\mathcal{P}$ such that if R has property $\mathcal{P}$, then $R[x]$ has property $\mathcal{P}$: being commutative, being unital, being an integral domain are such properties, and then two such other properties have been found, being a UFD (unique factorization domain) or being Noetherian, and *Hilbert's basis theorem* (which will be proved in another lecture) states that for R a commutative ring, $R[x]$ is a Noetherian ring if and only if R is a Noetherian ring.

One of the goals of Hilbert was to understand ideals in $F[x_1, \ldots, x_N]$, for example comparing the ideal $\mathcal{I}_1 = (P_1, \ldots, P_m)$ generated by polynomials in $F[x_1, \ldots, x_N]$, and the ideal $\mathcal{I}_2$ of polynomials which are 0 on the set of common zeros of $P_1, \ldots, P_m$: one has $\mathcal{I}_1 \subset \mathcal{I}_2$, and *Hilbert's nullstellensatz* states that if F is algebraically closed,[10] then $P \in \mathcal{I}_2$ if and only if P belongs to the radical of $\mathcal{I}_1$, i.e. there exists $k \geq 1$ with $P^k \in \mathcal{I}_1$; a weaker form is that if the set of common zeros of $P_1, \ldots, P_m$ is empty, then $1 \in \mathcal{I}_1$.

Such questions which interested algebraists in the 19th century were considered "pure mathematics" until recently, but since applications of algebra have appeared, it is useful to wonder if they were thought of by mathematicians who had an interest in questions from outside mathematics, or if they were imagined by engineers who had enough background in algebra for solving the questions which they had encountered.

---

[6] If $a, b \in J_\infty$, then $a \in J_j$ and $b \in J_k$ and one may assume that $j \leq k$ (or one exchanges a and b), so that $a, b \in J_k$, hence $a + b \in J_k \subset J_\infty$; of course $-a \in J_j \subset J_\infty$ and $r\,a, a\,r \in J_j \subset J_\infty$ for all $r \in R$.

[7] Claude Gaspard Bachet, sieur de Méziriac, French mathematician, 1581–1638.

[8] Christian Goldbach, German-born mathematician, 1690–1764. He worked in St Petersburg, Russia.

[9] Notice the danger of confusion with the notation: (a, b) either designates the gcd of a and b, or the ideal generated by a and b.

[10] A field F is algebraically closed if every non constant $P \in F[x]$ has a root. $\mathbb{C}$ is algebraically closed, but not $\mathbb{R}$ or $\mathbb{Q}$.