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

21- Monday October 17, 2011.

Lemma 21.1: Every Euclidean domain R is a PID.
Proof: Let J be an ideal of R. Since $\{0\} = (0)$, one may assume that $J \neq \{0\}$, so that the set of non-negative integers $\{V(j) \mid j \in J \setminus \{0\}\}$ is not empty, and it then has a smallest element n_0, which is $V(j_0)$ for some non-zero $j_0 \in J$. For $a \in J$, one has $a = j_0 q + r$ with either $r = 0$, or $r \neq 0$ and $V(r) < V(j_0)$, but the latter cannot hold, since $j_0 q \in J$, which implies $r = a - j_0 q \in J$, so that $V(r) \geq n_0 = V(j_0)$, a contradiction; hence $r = 0$, so that $J = (j_0)$.

Lemma 21.2: (Euclidean division algorithm) If R is a unital commutative ring and $A, B \in R[x]$ with B monic,[1] then $A = B\,q + r$, with $q, r \in R[x]$, and either $r = 0$ or $deg(r) < deg(B)$; q is called the *quotient* and r the *remainder* of the (Euclidean) division of A by B, and they are uniquely determined.
Proof: If $deg(B) = m$ so that b_m is a unit, then one may choose $q = 0$ and $r = P$ if $n = deg(P) < m$, and if $n \geq m$ one uses an induction on n, writing $A = B\,b_m^{-1} a_n x^{n-m} + A_1$ with $deg(A_1) \leq n - 1$, and one concludes by the induction hypothesis.

If $A = B\,q_1 + r_1 = B\,q_2 + r_2$, and if one had $q_1 \neq q_2$, it would imply that $deg\big(B\,(q_1 - q_2)\big) = deg(r_2 - r_1) < m$, but if $deg(q_2 - q_1) = s \geq 0$ one would have $q_2 - q_1 = c_s x^s + \textit{lower order terms}$ with $c_s \neq 0$, which would imply $b_m c_s = 0$ for killing the term in x^{m+s} in $B\,(q_1 - q_2)$, hence $c_s = 0$ since b_m has an inverse for multiplication; this shows that $q_2 = q_1$, which then implies $r_2 = r_1$.

Lemma 21.3: If F is a field, then $F[x]$ is an Euclidean domain, hence a PID.
Proof: By Lemma 21.2, the Euclidean division is defined by any non-zero $B \in F[x]$, and the degree serves as the desired function V.

Definition 21.4: The *polynomial function* associated to $P = a_0 + \ldots + a_n x^n \in R[x]$ is the mapping $r \mapsto P(r) = a_0 + a_1 r + \ldots + a_n r^n$, and $\alpha \in R$ is a *root* of P (or a *zero* of P) if $P(\alpha) = 0$.

Remark 21.5: One should not confuse a polynomial with the polynomial function that it defines: if F is a finite field of order q (which is a power of a prime p), then every non-zero a satisfies $a^{q-1} = 1$, since its order in the multiplicative group F^* must divide the order of F^*,[2] which is $q - 1$, and one deduces that $a^q = a$, which is also valid for $a = 0$, so that the polynomial $x^q - x$ is non-zero but takes the value 0 at all points of F.

This cannot happen in an infinite field (or an infinite integral domain), since in that case a polynomial of degree n cannot have more than n roots, by the following Lemma 21.6.

Lemma 21.6: If R is a commutative ring, then for $P, Q \in R[x]$ and $r \in R$ one has $(P + Q)(r) = P(r) + Q(r)$ and $(P\,Q)(r) = P(r)\,Q(r)$. If moreover R is unital, then $\alpha \in R$ is a root of $P \in R[x]$ if and only if $P = (x - \alpha)\,Q$ for some $Q \in R[x]$. As a consequence, if R is an integral domain, and $P \in R[x]$ is non-zero, then P cannot have d distinct roots with $d > deg(P)$.
Proof: $(P + Q)(r) = P(r) + Q(r)$ holds without commutativity of R, and $(P\,Q)(r) = P(r)\,Q(r)$ is true if $a_i r^i b_j r^j = a_i b_j r^{i+j}$ for all i, j, which is the case if r commutes with all the coefficients b_j of Q, hence it is true for all $r \in R$ if R is commutative.

Since $x - \alpha$ is monic (and one needs R to be unital for having $x \in R[x]$), $P = (x - \alpha)\,Q + r$ holds by Lemma 21.2, and r is a constant, and one wants to show that this constant is $P(\alpha)$: as in footnote # 1, by

[1] If R is unital but not commutative, one may be interested in solving $A = B\,q_1 + r_1$ or in solving $A = q_2 B + r_2$, with either $r_j = 0$ or $deg(r_j) < deg(B)$, and it may happen that $q_1 \neq q_2$. In the case $B = x - \alpha$, with $A = a_0 + \ldots + a_n x^n$, with $\alpha, a_0, \ldots, a_n \in R$, one has $x^k - \alpha^k = (x - \alpha)\,(x^{k-1} + \ldots + \alpha^{k-1}) = (x^{k-1} + \ldots + \alpha^{k-1})\,(x - \alpha)$ for $k \geq 1$, so that after multiplication by a_k on the right or on the left and summing in k, one has $A - \sum_{k=0}^{n} \alpha^k a_k = B\,q_1$ with $q_1 = \sum_{k=1}^{n} (x^{k-1} + \ldots + \alpha^{k-1})\,a_k$, or $A - A(\alpha) = q_2 B$ with $q_2 = \sum_{k=1}^{n} a_k (x^{k-1} + \ldots + \alpha^{k-1})$.

[2] In a unital ring R, R^* denotes the multiplicative group of units of R, so that if F is a field, $F^* = F \setminus \{0\}$.

multiplying $x^k - \alpha^k = (x-\alpha)\,(x^{k-1} + \ldots + \alpha^{k-1})$ for $k \geq 1$ by a_k and summing in k, one deduces that $P - P(\alpha) = (x-\alpha)\,Q$ with $Q = \sum_{k=1}^{n} a_k (x^{k-1} + \ldots + \alpha^{k-1})$.

If R is an integral domain, and $P \in R[x]$ is non-zero, and has distinct roots $\alpha_1, \ldots, \alpha_d$, then $P = (x-\alpha_1)\,Q_1$ and one has $0 = P(\alpha_j) = (\alpha_j - \alpha_1)\,Q_1(\alpha_j)$, and since $\alpha_j - \alpha_1 \neq 0$ for $j \neq 1$, one deduces that Q_1 has distinct roots $\alpha_2, \ldots, \alpha_d$, and one concludes by induction on d that P is divisible by $(x-\alpha_1) \cdots (x-\alpha_d)$, so that the degree of P is $\geq d$ (since in an integral domain the degree of a product of non-zero polynomials is the sum of their degrees).

Remark 21.7: Since a odd implies $a^2 = 1 \pmod 8$, $x^2 - 1$ has four roots in $\mathbb{Z}_8$, namely $1, 3, 5, 7$, corresponding to the factorizations $x^2 - 1 = (x-1)\,(x+1) = (x-3)\,(x+3) = (x-5)\,(x+5) = (x-7)\,(x+7) \pmod 8$, showing that the hypothesis that R has no zero divisors is crucial for the last result of Lemma 21.6 to hold, that there are not more roots than the degree of the polynomial.

Remark that $\mathbb{Z}_8$ is a principal ideal ring, since all its ideals are principal, because besides $\{0\} = (0)$ and $\mathbb{Z}_8 = (1)$ the ideals of $\mathbb{Z}_8$ are $2\mathbb{Z}_8 = \{0, 2, 4, 6\} = (2)$ and $4\mathbb{Z}_8 = \{0, 4\} = (4)$, but it is not a PID, since it is not an integral domain (because 2, 4, and 6 are zero-divisors).

Definition 21.8: If R is a commutative unital ring, and $P \in R[x]$, then $a \in R$ is called a *multiple root* of P if $P = (x-a)^k Q$ for some $Q \in R[x]$ and $k \geq 2$, in which case it is a *root of multiplicity* k (or order k) if P cannot be written as $(x-a)^{k+1} Q_1$ with $Q_1 \in R[x]$, and a is a *simple root* if it is a root but not a multiple root, in which case one counts its "multiplicity" as 1.

Remark 21.9: In the case where R is an integral domain, if P has distinct roots $a_1, \ldots, a_m$ with respective multiplicities $k_1, \ldots, k_m$ then $s = \sum_{j=1}^{m} k_j \leq deg(P)$, and one says that P has s roots *counting multiplicity*.

After proving a criterion for multiple roots using the derivative of a polynomial, the following question will be to describe if there are non-constant polynomials without roots, and the notion of algebraically closed field will be introduced, an example being $\mathbb{C}$, while $\mathbb{R}$ is not algebraically closed and there are polynomials of degree 2 in $\mathbb{R}[x]$ without roots, namely $a\,x^2 + b\,x + c$ when $b^2 < 4a\,c$, but in $\mathbb{Q}$ it will be shown (by Eisenstein's criterion) that there are polynomials in $\mathbb{Q}[x]$ of any degree $d \geq 2$ which are irreducible,[3] i.e. cannot be factored into a product of polynomials of lower order.

The notion of irreducible elements will be introduced in a general context, and compared to another related notion, of prime elements.

Remark 21.10: For $D \in \mathbb{Z}$ not a square, $\mathbb{Z}[\sqrt{D}] = \{z = a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (or $\subset \mathbb{R}$ if $D > 0$) is an integral domain; defining the conjugate of $z = a + b\sqrt{D}$ to be $\overline{z} = a - b\sqrt{D}$, one writes $N(z) = z\,\overline{z} = a^2 - D\,b^2$, and from the fact that $\overline{z_1 z_2} = \overline{z_1}\;\overline{z_2}$, one deduces that $N(z_1 z_2) = N(z_1)\,N(z_2)$, so that if z is a unit one must have $N(z) = \pm 1$ (and for $D > 0$ the equation $a^2 - D\,b^2 = \pm 1$ is wrongly called Pell's equation);[4] conversely, if $N(z) = \pm 1$, then z is a unit, and its inverse is $\pm\overline{z}$.

Gauss had found nine values of $D < 0$ (namely $-1, -2, -3, -7, -11, -19, -43, -67, -163$) for which $\mathbb{Z}[\sqrt{D}]$ is a PID, and his conjecture that there are no further values was proved one hundred years later by Heegner,[5] Baker,[6] and Stark.[7]

In $\mathbb{Z}[\sqrt{10}]$, one has $(4 + \sqrt{10})\,(4 - \sqrt{10}) = 6 = 2 \cdot 3$, so that there not a unique factorization of 6 as a product of irreducible elements, which like $4 \pm \sqrt{10}, 2, 3$ cannot be written as $z_1\,z_2$ with neither z_1 nor z_2 a unit, because one would have $N(z) \in \{\pm 2, \pm 3\}$, which is impossible, since it implies $a^2 = \pm 2 \pmod 5$.

---

[3] Ferdinand Gotthold Max Eisenstein, German mathematician, 1823-1852. Eisenstein series are named after him.

[4] John Pell, English mathematician, 1611–1685. Pell's equation is named after him, although he had little to do with it, and it had been studied first by Brahmagupta.

[5] Kurt Heegner, German mathematician, 1893–1965. Heegner numbers are named after him.

[6] Alan Baker, English mathematician, born in 1939. He received the Fields Medal in 1970. He worked at University College, London, and at Cambridge, England.

[7] Harold Mead Stark, American mathematician, born in 1939. He worked at University of Michigan, Ann Arbor, MI, at MIT (Massachusetts Institute of Technology), Cambridge, MA, and at UCSD (University of California at San Diego), La Jolla, CA.