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

23- Monday October 24, 2011.

Theorem 23.1: (fundamental theorem of algebra) $\mathbb{C}$ is algebraically closed.
Proof: This proof is attributed to GAUSS, and it uses analysis. If $P \in \mathbb{C}[x]$ is not constant, then $|P(z)| \to +\infty$ as $|z| \to +\infty$, so that there exists $z_0 \in \mathbb{C}$ where $|P|$ attains its minimum; if one had $P(z_0) \neq 0$, then one would use the Taylor expansion of P at z_0, which implies $P(z) = P(z_0) + a\,(z - z_0)^m Q(z - z_0)$, with $a \neq 0$, $m \geq 1$ and $Q(0) = 1$, one would choose ξ such that $a\,\xi^m = -P(z_0)$, and observing that $P(z_0 + \varepsilon\,\xi) = P(z_0)(1 - \varepsilon^m) + o(|\varepsilon^{m+1}|)$, one would have $|P(z_0 + \varepsilon\,\xi)| < |P(z_0)|$ for $\varepsilon > 0$ small.

Remark 23.2: That analysis is used in a proof which seems to be pure algebra is actually quite natural, since although $\mathbb{C}$ is constructed from $\mathbb{R}$ by algebra, the definition of $\mathbb{R}$ involves analysis. The basic property is that if $P \in \mathbb{R}[x]$ and $deg(P)$ is odd, then P has at least one root $\alpha \in \mathbb{R}$, by an argument of connectedness: for $|x|$ very large, P looks like an odd power, so that one can find $y, z \in \mathbb{R}$ with $P(y) < 0 < P(z)$, and then, since P is a continuous function, it must have a root between y and z.

In France, Theorem 23.1 is attributed to D'ALEMBERT,[1] but it seems unlikely that he had a proof, so that he may have conjectured it. There is a proof by LAPLACE which continues the case of an odd degree by considering $n = 2^k m$ for m odd,[2] by induction on k, but his proof was not accepted as valid at the time, because it assumes that the roots exist somewhere, and the method of construction of a splitting field extension was not so clear before GALOIS.

There is a proof by ARTIN which is also pure algebra after the first step of considering odd degree for $\mathbb{R}[x]$, but it uses Galois theory, for considering the Galois group of a splitting field extension, the Galois correspondence between subgroups of the Galois group and intermediate fields, and Sylow's theorem for the Galois group.

Definition 23.3: Let R be a commutative unital ring. An element $c \in R$ is called *irreducible* if $c \neq 0$, c is not a unit, and $c = a\,b$ implies that either a or b is a unit (i.e. either a or b is associate to c); if c is not irreducible, it is then called *reducible*.

An element $q \in R$ is called a *prime* if $q \neq 0$, q is not a unit, and q divides $a\,b$ implies that either q divides a or q divides b.

Remark 23.4: If R is an integral domain, then $deg(P_1 P_2) = deg(P_1) + deg(P_2)$ for all non-zero $P_1, P_2 \in R[x]$, so that $R[x]$ is an integral domain and the units of $R[x]$ are the constants which are units in R. $P = 2x$ is irreducible in $\mathbb{Q}[x]$, but it is reducible in $\mathbb{Z}[x]$ because 2 is not a unit in $\mathbb{Z}$.

If F is a field, all polynomials $P \in F[x]$ of degree 1 are irreducible, and a non-zero polynomial $P \in F[x]$ of degree $n \geq 2$ is irreducible if and only if it cannot be written as $P = P_1 P_2$ with both P_1 and P_2 having degree ≥ 1. If $P \in F[x]$ is a polynomial of degree 2 or 3, it is irreducible if and only if it has no root, since by writing $P = P_1 P_2$ with both P_1 and P_2 having degree ≥ 1, either P_1 or P_2 has degree 1, hence has a root, which is a root of P.

A field F is algebraically closed if and only if the irreducible polynomials in $F[x]$ are the polynomials of degree 1.

Lemma 23.5: If $P \in \mathbb{R}[x]$, and if $a \in \mathbb{C}$ is a root of P (considered as an element of $\mathbb{C}[x]$), then $\overline{a}$ is a root of P, having the same multiplicity than a. Every $P \in \mathbb{R}[x]$ of degree $n \geq 1$ can then be written as $c \prod_{i=1}^m (x - r_i) \prod_{j=1}^k (x - z_j)\,(x - \overline{z_j})$ for elements $r_1, \ldots, r_m \in \mathbb{R}$, $z_1, \ldots, z_k \in \mathbb{C} \setminus \mathbb{R}$, and $m + 2k = n$, and $(x - z_j)\,(x - \overline{z_j}) = x^2 - 2\Re(z_j)\,x + |z_j|^2 \in \mathbb{R}[x]$ can be any polynomial $x^2 + a_j x + b_j$ with $a_j^2 < 4b_j$. An irreducible polynomial $P \in \mathbb{R}[x]$ either has degree 1, with $P = a_0 + a_1 x$ with $a_1 \neq 0$, or has degree 2, with $P = a_0 + a_1 x + a_2 x^2$ with $a_2 \neq 0$ and $a_1^2 < 4a_0 a_2$.
Proof: For $P \in \mathbb{R}[x]$, one has $\overline{P(a)} = P(\overline{a})$ for all $a \in \mathbb{C}$, and the same property holds for the successive derivatives of P, so that if a is a root of P of multiplicity k, the derivatives of P up to order $k - 1$ at a

[1] Jean LE ROND, known as D'ALEMBERT, French mathematician, 1717–1783. He worked in Paris, France.
[2] Pierre-Simon LAPLACE, French mathematician, 1749–1827. He was made comte in 1806 by Napoléon I and marquis in 1817 by Louis XVIII. He worked in Paris, France.

are 0 but not the kth derivative, so that the same is true at $\overline{a}$, hence $\overline{a}$ is also a root of multiplicity k. If $a \in \mathbb{C} \setminus \mathbb{R}$, then $\overline{a} \neq a$, so that putting the two factors $(x-a)^k$ and $(x-\overline{a})^k$ together gives $\big((x-a)\,(x-\overline{a})\big)^k$, and $(x-a)\,(x-\overline{a})$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$. There are then irreducible polynomials of degree 2, which are those whose complex roots are not real (i.e. those with discriminant < 0).

Remark 23.6: If $P(x) \geq 0$ for all $x \in \mathbb{R}$, then each real root has an even multiplicity, so that $c \prod_{i=1}^m (x-r_i) = Q^2$ for some $Q \in \mathbb{R}[x]$, and if $\prod_{j=1}^k (x-z_j) = R + i\,S$ for $R, S \in \mathbb{R}[x]$, then $\prod_{j=1}^k (x-z_j)\,(x-\overline{z_j}) = (R+i\,S)\,(\overline{R+i\,S}) = R^2 + S^2$, so that $P = (Q\,R)^2 + (Q\,S)^2$ is a sum of two squares of polynomials.

If $P \in \mathbb{R}[x_1, x_2]$ has degree 4 and satisfies $P(x_1, x_2) \geq 0$ for all $x_1, x_2 \in \mathbb{R}$, HILBERT proved in 1888 that P is the sum of three squares of polynomials, but that for degree ≥ 6 there are non-negative polynomials which are not sums of squares of polynomials, and the same negative result holds for degree 4 in three real variables.[3] HILBERT did not exhibit counter-examples, and the simplest ones were shown by MOTZKIN in the 1960s,[4] using the arithmetic-geometric inequality:[5] $x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 + 1 \pm 4x_1x_2x_3 \geq 0$ in $\mathbb{R}^3$, and $x_1^4x_2^2 + x_1^2x_2^4 + 1 - 3x_1^2x_2^2 \geq 0$ in $\mathbb{R}^2$, but these polynomials cannot be written as sums of squares of polynomials.[6]

E. ARTIN showed that any non-negative polynomial in ℓ real variables can be written as a sum of squares of rational fractions.

Definition 23.7: For a polynomial $P = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, one defines the *content* $C(P)$ of P as the *gcd* of $a_0, \ldots, a_n$; one calls a polynomial $P \in \mathbb{Z}[x]$ *primitive* if $C(P) = 1$ (so that one always has $P = C(P)P_0$ with P_0 primitive).

Lemma 23.8: (Gauss's lemma)[7] One has $C(P\,Q) = C(P)C(Q)$ for all $P, Q \in \mathbb{Z}[x]$; equivalently, the product of primitive polynomials in $\mathbb{Z}[x]$ is primitive.
Proof: Let $P_0 = a_0 + \ldots \in \mathbb{Z}[x]$ and $Q_0 = b_0 + \ldots \in \mathbb{Z}[x]$ be primitive, but assume that $P_0Q_0 = c_0 + \ldots$ is not primitive, so that there exists a prime p which divides all c_k. Since p does not divide all a_i, there exists $i_0 \geq 0$ such that $p \mid a_i$ for $i < i_0$ but p does not divide a_{i_0} (which is then $\neq 0$), and since p does not divide all b_j, there exists $j_0 \geq 0$ such that $p \mid b_j$ for $j < j_0$ but p does not divide b_{j_0} (which is then $\neq 0$); however, this leads to a contradiction, since $c_{i_0+j_0} - a_{i_0}b_{j_0} = \sum_{i<i_0} a_ib_{i_0+j_0-i} + \sum_{j<j_0} a_{i_0+j_0-j}b_j$, which is a multiple of p, and since p divides $c_{i_0+j_0}$ it must divide $a_{i_0}b_{j_0}$.[8]

Lemma 23.9: If $P \in \mathbb{Z}[x]$ is primitive of degree ≥ 1 then it is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.
Proof: Notice that the result is not true if $C(P) > 1$: for example, $2 + 2x$ is reducible in $\mathbb{Z}[x]$ because 2 and $1 + x$ are not units in $\mathbb{Z}[x]$. Since one assumes $C(P) = 1$, if P is reducible in $\mathbb{Z}[x]$ then $P = P_1P_2$ with $P_1, P_2 \in \mathbb{Z}[x]$ and neither P_1 nor P_2 being a constant different from ± 1, so that the degrees of P_1, P_2 are

---

[3] For a non-negative polynomial of degree 2 in ℓ real variables, Gauss's decomposition of quadratic forms shows it is a sum of at most ℓ squares of affine functions plus a non-negative constant.

[4] Theodore Samuel MOTZKIN, German-born mathematician, 1908–1970.

[5] For $a_1, \ldots, a_m > 0$, one has $\sqrt[m]{a_1 \cdots a_m} \leq \frac{a_1+\ldots+a_m}{m}$, which after writing $a_j = e^{b_j}$ is just the convexity of the exponential function.

[6] If $x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 + 1 \pm 4x_1x_2x_3 = \sum_j Q_j^2$, each Q_j must have degree ≤ 1 in each variable and total degree ≤ 2, and the Q_j cannot have terms in x_1, x_2, x_3 since it would create terms in x_1^2, x_2^2, x_3^2 with positive coefficients, but it implies that there is no term in $x_1x_2x_3$ in Q_j^2. If $x_1^4x_2^2 + x_1^2x_2^4 + 1 - 3x_1^2x_2^2 = \sum_j Q_j^2$, each Q_j must have degree ≤ 2 in each variable and total degree ≤ 3, and the Q_j cannot have terms in x_1^2, x_2^2 since it would create terms in x_1^4, x_2^4 with positive coefficients, but then the Q_j could not have terms in x_1, x_2 either, since it would create terms in x_1^2, x_2^2 with positive coefficients, hence the term in $x_1^2x_2^2$ in Q_j^2 has a coefficient which is ≥ 0.

[7] Since GAUSS was a mathematical genius, he proved many results, and a few different ones are known as Gauss's lemma.

[8] Said otherwise, the projection π from $\mathbb{Z}$ onto $\mathbb{Z}_p$ induces a ring-homomorphism from $\mathbb{Z}[x]$ into $\mathbb{Z}_p[x]$, and the images $\pi(P_0), \pi(Q_0) \in \mathbb{Z}_p[x]$ of $P_0, Q_0 \in \mathbb{Z}[x]$ are assumed to satisfy $\pi(P_0\,Q_0) = 0$, but since it means $\pi(P_0)\,\pi(Q_0) = 0$ and $\mathbb{Z}_p[x]$ is an integral domain, either $\pi(P_0) = 0$ or $\pi(Q_0) = 0$, i.e. all the coefficients of P_0 or all the coefficients of Q_0 are multiple of p.

≥ 1, and P is reducible in $\mathbb{Q}[x]$. Conversely, if $P = P_1 P_2$ in $\mathbb{Q}[x]$, then there exist positive integers m_1, m_2 such that $P_1 = \frac{Q_1}{m_1}$ and $P_2 = \frac{Q_2}{m_2}$ with $Q_1, Q_2 \in \mathbb{Z}[x]$, and then by Gauss's lemma one has $C(Q_1)C(Q_2) = C(Q_1 Q_2) = C(m_1 m_2 P) = m_1 m_2$, and $P = \frac{Q_1 Q_2}{m_1 m_2} = \frac{Q_1}{C(Q_1)} \frac{Q_2}{C(Q_2)}$ is the product of two polynomials in $\mathbb{Z}[x]$.

Lemma 23.10: (Eisenstein's criterion) If $P = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ and a prime p divides $a_0, \ldots, a_{n-1}$ but not a_n, and p^2 does not divide a_0, then P is irreducible in $\mathbb{Q}[x]$ (and if $C(P) = 1$ it is irreducible in $\mathbb{Z}[x]$).
Proof: One notices that p does not divide $C(P)$, since p does not divide a_n, and by dividing P by $C(P)$, one may then assume that P is primitive. If $P = Q_1 Q_2$ with $Q_1, Q_2 \in \mathbb{Q}[x]$, one may assume that $Q_1, Q_2 \in \mathbb{Z}[x]$ by Lemma 23.9. One has $Q_1 = b_0 + \ldots + b_{m_1} x^{m_1}$ and $Q_2 = c_0 + \ldots + c_{m_2} x^{m_2}$ with $m_1, m_2 < n$, and then because $p \mid a_0 = b_0 c_0$ one has either $p \mid b_0$ or $p \mid c_0$, but not both because p^2 does not divide a_0, so that one may assume that $p \mid b_0$ but p does not divide c_0; then, $p \mid a_1 = b_0 c_1 + b_1 c_0$ implies $p \mid b_1 c_0$, hence $p \mid b_1$, and then $p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ implies $p \mid b_2$, and by induction one finds that p divides all b_i (because $m_1 < n$), which is a contradiction since it implies that p divides all a_k.[9]

Remark 23.11: One may generalize Gauss's lemma and Eisenstein's criterion to the case where $\mathbb{Z}$ is replaced by a UFD (unique factorization domain) D, and $\mathbb{Q}$ is replaced by F, the field of fractions of D.

By Eisenstein's criterion, there are irreducible polynomials in $\mathbb{Q}[x]$ of any degree.

It can be shown that for every prime p and every $m \geq 2$ there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree m, but it is not so elementary: writing $F_0 = \mathbb{Z}_p$, and denoting $q = p^m$, one first invokes the construction of a splitting field extension F for the polynomial $Q = x^q - x$ over F_0; then, since F is an F_0-vector space, it has characteristic p, and from $(a+b)^p = a^p + b^p$ for all $a, b \in F$, one deduces that $(a+b)^q = a^q + b^q$ for all $a, b \in F$, and this permits to show that the roots of Q form a field, which is F, and since these roots are distinct because $Q' = -1$ (hence a multiple root cannot exist), F has q elements, i.e. F is an F_0-vector space of dimension m; then, to each non-zero $a \in F$ is attached an irreducible polynomial P_a of degree $\leq m$ such that $P_a(a) = 0$ (and P_a divides Q), and for being sure that one P_a has degree m, one observes that the (Abelian) multiplicative group $F^* = F \setminus \{0\}$ is cyclic (or order $q-1$) and any of its generators (and there are $\varphi(q-1)$ of them) is such an a.

[9] Said otherwise, Q_1 and Q_2 define polynomials $\pi(Q_1), \pi(Q_2) \in \mathbb{Z}_p[x]$ and $\pi(Q_1)\,\pi(Q_2) = c\,x^n$ in $\mathbb{Z}_p[x]$ with $0 \neq c \in \mathbb{Z}_p$, so that one must have $\pi(Q_1) = a\,x^{m_1}$ and $\pi(Q_2) = b\,x^{m_2}$ with $a\,b = c$ and $m_1 + m_2 = n$ (since $\mathbb{Z}_p[x]$ is a PID, hence a UFD). Then, Q_1 has all its coefficients up to degree $m_1 - 1$ which are multiple of p, and Q_2 has all its coefficients up to degree $m_2 - 1$ which are multiple of p, hence P has all its coefficients up to degree $\min\{m_1, m_2\} - 1$ which are multiple of p^2.