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

26- Friday November 4, 2011.

Lemma 26.1: If R is an integral domain, then $c \neq 0$ is irreducible if and only if (c) is maximal in the set of all proper principal ideals, i.e. $(c) \subset (d)$ implies $(d) = (c)$ or $(d) = R$.

If R is a PID, every irreducible element is prime (recall that in an integral domain every prime element is irreducible).
Proof: If c is irreducible and $(c) \subset (d)$, it means that $c = d\,x$ for some $x \in R$, which implies that either d is a unit, in which case $(d) = R$, or x is a unit, in which case $d = x^{-1}c$ and $(d) \subset (c)$, so that $(d) = (c)$. Conversely, if (c) is maximal in the set of proper principal ideals and $c = a\,b$, then one deduces that $(c) \subset (a)$, so that either $(a) = R$, in which case a is a unit, or $(a) = (c)$, which implies $a = c\,x$, so that $c = a\,b = c\,x\,b$, i.e. $1 = x\,b$ (since R is an integral domain and $c \neq 0$), so that b is a unit.

In a PID, prime is then equivalent to irreducible, because maximality among proper principal ideals is the same as maximality among proper ideals, since all ideals are principal, so that if c is irreducible then (c) is a maximal proper ideal, hence a prime ideal, showing that c is prime.

Definition 26.2: A ring R is called a *UFD*, which stands for *unique factorization domain*, if it is an integral domain such that every $r \neq 0$ which is not a unit has a factorization $r = a_1 \cdots a_m$, where $a_1, \ldots, a_m$ are irreducible, and the factorization is unique in the sense that if $r = b_1 \cdots b_n$, where $b_1, \ldots, b_n$ are irreducible, then $m = n$ and there exists a permutation σ such that for $i = 1, \ldots, n$ one has $b_i = a_{\sigma(i)} u_i$ where u_i is a unit (i.e. b_i is an associate of $a_{\sigma(i)}$).

Lemma 26.3: Every PID is a UFD.
Proof: Assume that R is a PID, so that R is Noetherian.[1] Let $r \neq 0$, which is not a unit. If r is reducible, write $r = r_1 r_2$, where neither r_1 nor r_2 are units; if one of them, say r_1, is reducible, write $r_1 = r_{1,1} r_{1,2}$, where neither $r_{1,1}$ nor $r_{1,2}$ are units; if the process was not terminating, there would exist an infinite ascending sequence of ideals $(r) \subset (r_1) \subset (r_{1,1}) \subset \ldots$, where all inclusions are proper, contradicting the fact that R is Noetherian.

For showing the uniqueness, one proceeds by induction of the minimum number n of irreducible factors. If $n = 0$, then r is a unit, and $r = q\,c$ with q irreducible would give a contradiction, since it implies that q is a unit. If $n \geq 1$ and $r = p_1 \cdots p_n = q_1 \cdots q_m$ with $m \geq n$, then p_1 is prime (since in a PID irreducible elements are prime), and it divides $q_1 \cdots q_m$, so that it must divide a factor, say q_1: one then has $q_1 = p_1 u$ for a unit u, and then $p_2 \cdots p_n = (u\,q_2) \cdots q_m$, and one uses the induction hypothesis.

Lemma 26.4: In a UFD every irreducible element is prime.
Proof: If p is irreducible and $p \mid a\,b$ for some $a, b \in R$, then $a\,b = p\,c$ for some $c \in R$, and writing a, b, and c as products of irreducible elements, p must be associate to one of the irreducible elements occurring in the factorizations of a or b, so that p divides a or b.

Remark 26.5: Bézout's theorem,[2] is that the gcd of polynomials $P_1, \ldots, P_m \in F[x]$ for a field F can be written as $\sum_i Q_i P_i$ for some polynomials $Q_1, \ldots, Q_m \in F[x]$, and the proof is the same than for Bachet's theorem for the gcd in $\mathbb{Z}$: the ideal in $F[x]$ generated by $P_1, \ldots, P_m$ is principal, since $F[x]$ is a PID, i.e. made of the multiple of a polynomial D, which one may choose to be monic (and restrict to the case where the coefficient of highest order is $+1$), and D is obviously the gcd of $P_1, \ldots, P_m$.

If R is a UFD one can find a gcd for any finite number of elements $r_1, \ldots, r_m \in R$, but one has only the multiplicative approach: in the factorizations of $r_1, \ldots, r_m$, one avoids repeating associates by writing the list $s_1, \ldots, s_n$ of irreducible elements appearing in the factorizations, with s_i not being an associate of s_j for

[1] One may use the initial Definition 19.7, that an ascending chain of ideals becomes constant: it means $(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$ and the union is an ideal, equal to (b), and b must belong to some (a_{n_0}), so that $(a_n) = (a_{n_0})$ for $n \geq n_0$. It is quicker to use Lemma 19.8, that a ring is Noetherian if and only if each of its ideals is finitely generated.

[2] Étienne BÉZOUT, French mathematician, 1730–1783. He worked in Paris, France. Bézout's theorem is named after him.

$i \neq j$, and then each r_i has a factorization $r_i = u_i s_1^{k_1(i)} \cdots s_n^{k_n(i)}$ with $k_\ell(i) \geq 0$ for $\ell = 1, \ldots, n$, and u_i is a unit; a gcd is then $s_1^{\kappa_1} \cdots s_n^{\kappa_n}$, with $\kappa_\ell = \min_i k_\ell(i)$ for $\ell = 1, \ldots, n$, and it is defined up to an associate.

Remark 26.6: It will be shown in another lecture that if R is a UFD then $R[x]$ is also a UFD (and if $R[x]$ a UFD then R is a UFD), and that if R is Noetherian then $R[x]$ is also Noetherian (and if $R[x]$ is Noetherian then R is Noetherian). If R is a PID, then it is not always true that $R[x]$ is a PID: for example, if F is a field, $F[x]$ is a PID, but $F[x_1, x_2]$ is not a PID (and $F[x_1, x_2]$ is isomorphic to $R[x_2]$ with $R = F[x_1]$). However, by induction on n, $F[x_1, \ldots, x_n]$ is both a UFD and Noetherian.

Remark 26.7: We have now seen two ways to construct fields, the first one is to start from an integral domain and to consider its field of fractions, and the second one is to start from a field F, and to consider the quotient of the ring of polynomial $F[x]$ by the ideal generated by an irreducible polynomial $P \in F[x]$, and this ideal is maximal because $F[x]$ is a PID.[3]

Since $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ (but not in $\mathbb{R}[x]$), the quotient $\mathbb{Q}[x]/(x^2 - 2)$ is a field, denoted $\mathbb{Q}[\sqrt{2}]$. In each coset one considers the element of the form $a + b\,x$ with $a, b \in \mathbb{Q}$, and for finding to which coset a polynomial $P \in \mathbb{Q}[x]$ belongs, one divides P by $x^2 - 2$ and one takes the remainder. Since $x^2 = 2$ (mod $x^2 - 2$), one may then consider that $x = \sqrt{2}$, and one then writes $\mathbb{Q}[\sqrt{2}] = \{a + b\,\sqrt{2} \mid a, b \in \mathbb{Q}\}$, but one could as well consider that $x = -\sqrt{2}$, because at an algebraic level there is no reason to make any difference between the two cases. If one considers that $x = \sqrt{2}$, it is important to use the *conjugation*, which sends $z = a + b\sqrt{2}$ to $\overline{z} = a - b\sqrt{2}$, and conjugation is an automorphism of $\mathbb{Q}[\sqrt{2}]$: indeed, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ for all $z_1, z_2 \in \mathbb{Q}[\sqrt{2}]$, which show that conjugation is a ring-homomorphism, and it is injective because $\overline{1} = 1$,[4] and surjective because $\overline{\overline{z}} = z$ for all $z \in \mathbb{Q}[\sqrt{2}]$. For $z = a + b\sqrt{2} \neq 0$, the multiplicative inverse if $\frac{\overline{z}}{N(z)}$ with $N(z) = z\,\overline{z} = a^2 - 2b^2 \in \mathbb{Q}^*$, which satisfies $N(z_1 z_2) = N(z_1)\,N(z_2)$ for all $z_1, z_2 \in \mathbb{Q}[\sqrt{2}]$.

Notice that $\mathbb{Z}[\sqrt{2}] = \{a + b\,\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain, subring of $\mathbb{Q}[\sqrt{2}]$, and that its field of fraction is isomorphic to $\mathbb{Q}[\sqrt{2}]$: if the inverse of $a + b\,\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is $c + d\,\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, then for $m \in N^\times$ multiple of the denominators of c and of d, one may write $c + d\,\sqrt{2} = \frac{m\,c + m\,d\,\sqrt{2}}{m}$, and $m\,c + m\,d\,\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

With (a, b) interpreted as $a + b\,x$, one then has put on $\mathbb{Q} \times \mathbb{Q}$ a structure of field with $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and $(a_1, b_1) \star (a_2, b_2) = (a_1 a_2 + 2b_1 b_2, a_1 b_2 + b_1 a_2)$.

Remark 26.8: Since $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ (but not in $\mathbb{R}[x]$), the quotient $\mathbb{Q}[x]/(x^3 - 2)$ is a field, which one denotes $\mathbb{Q}[\sqrt[3]{2}]$. In each coset one considers the element of the form $a + b\,x + c\,x^2$ with $a, b, c \in \mathbb{Q}$, i.e. for finding to which coset $P \in \mathbb{Q}[x]$ belongs, one divides P by $x^3 - 2$ and one takes the remainder. Since $x^3 = 2$ (mod $x^3 - 2$), one may then consider that $x = \sqrt[3]{2}$, and one writes $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, but in this case there is no automorphism of $\mathbb{Q}[\sqrt[3]{2}]$ to consider. For $z = a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4} \neq 0$, there is a multiplicative inverse, but it is not as simple as in the previous example to explain how to compute it.

If (a, b, c) is interpreted as $a + b\,x + c\,x^2$, then one has put on $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ a structure of field with $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$ and $(a_1, b_1, c_1) \star (a_2, b_2, c_2) = (a_1 a_2 + 2b_1 c_2 + 2c_1 b_2, a_1 b_2 + b_1 a_2 + 2c_1 c_2, a_1 c_2 + a_2 c_1 + b_1 b_2)$.

In $\mathbb{Q}[\sqrt[3]{2}]$, the polynomial $x^3 - 2$ is not irreducible, since $x^3 - 2 = (x - \sqrt[3]{2})\,(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})$, but $x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4}$ is irreducible in $\mathbb{Q}[\sqrt[3]{2}]$.

Remark 26.9: It looks feasible to check directly that the operations $+, \star$ on $\mathbb{Q} \times \mathbb{Q}$ mentioned at Remark 26.7 define a field. However, checking that the operations $+, \star$ on $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ mentioned at Remark 26.8 define a field seems a daunting task. The power of algebra is precisely that one should avoid doing that, and observe that $\star$ is the product of the polynomials $a_1 + b_1 x + c_1 x^2$ and $a_2 + b_2 x + c_2 x^2$ when x^3 is replaced by 2, and that if the coefficients $a_1, b_1, c_1, a_2, b_2, c_2$ belong to a commutative ring R, one is considering the ring structure of the quotient $R[x]/(x^3 - 2)$, which is unital if R is unital, an integral domain if R is an integral domain where no element has cube 2, and a field if moreover R is a field.

[3] If P has degree ≥ 2, this new field is not isomorphic to F, and it is a *finite extension* (hence an *algebraic extension*) of F. If F is algebraically closed, P must have degree 1, and one finds a field isomorphic to F, because there is no algebraic extension of F different from F itself, but one may consider a *transcendental extension* like $F(x)$, which is the field of fractions of $F[x]$.

[4] If ψ is a ring-homomorphism from a field F (or a division ring) into a ring R, then ψ is injective if and only if $\psi(1) \neq 0$, since for $x \neq 0$ one has $\psi(x)\,\psi(x^{-1}) = \psi(x\,x^{-1}) = \psi(1) \neq 0$, so that $\psi(x) \neq 0$, hence $ker(\psi) = \{0\}$.