Graduate Algebra, Fall 2014
Lecture 31

Andrei Jorza

2014-11-12

2 Rings

2.6 Special types of rings (continued)

2.6.3 UFD (continued)

Theorem 1. *Every PID is a UFD.*

Proof. Continued from last time.

By the proposition every factorization into irreducibles is unique, so let's show that such factorizations always exist. Suppose $x \in R$. Let (a_1) be a maximal ideal containing x. Then $x \in (a_1)$ and $x = a_1 x_1$. If x_1 is a unit, then x has a factorization. Otherwise, applying the same method get $x_1 = a_2 x_2$. After n steps $x = a_1 \dots a_n x_n$. If x_n is a unit then x has a factorization. Otherwise if x_n is never a unit, get a chain of ideals $I_n = (x_n)$ such that $I_1 \subset I_2 \subset \dots$. Let $I = \cup I_n$. Since each I_n is an ideal, if $x \in I$ and $r \in R$ then $x \in I_n$ for some n and $rx \in I_n \subset I$ and if $x, y \in I$ then $x, y \in I_n$ for some large n and so $x + y \in I_n \subset I$. Thus I is an ideal and since R is principal, $I = (a)$ for some $a \in R$. But then $a \in I$ is in some I_n and so $(x_n) = (a) = (x_{n+1})$. This contradicts the fact that $(x_n) = (a_{n+1})(x_{n+1})$ with a_{n+1} not a unit. Thus x must have a factorization and by the previous proposition such a factorization is unique. $\square$

Example 2. Any Euclidean domain is a UFD.

1. $\mathbb{Z}$
2. $F[X]$
3. $F[\![X]\!]$
4. $\mathbb{Z}[i]$
5. $\mathbb{Z}[\zeta_3]$
6. $\mathbb{Z}[\sqrt{2}]$

Example 3. The ring $\mathbb{Z}[\sqrt{-5}]$ is not UFD since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and each of these is irreducible.

Definition 4. If R is an integral domain then $\operatorname{Frac} R = \{\frac{x}{y} | x, y \in R, y \neq 0\}$ up to usual equivalences for fractions, is a field, called the fraction field of R. We'll come back to this construction when we talk about localization later.

Lemma 5 (Gauss' Lemma)**.** *Suppose R is a UFD with fraction field F. Suppose $f(X) \in R[X]$ is of the form $f(X) = g(X)h(X)$ with $g(X), h(X) \in F[X]$. Then there exists $a \in F - 0$ such that $G(X) = ag(X)$ and $H(X) = a^{-1}h(X)$ are in $R[X]$ with $f(X) = G(X)H(X)$.*

Proof. A polynomial $A(X) \in R[X]$ is said to be primitive if $a^{-1}A(X) \in R[X]$ implies $a \in R^\times$. In other words the coefficients have no nontrivial common denominator.

Clearing denominators, $ag(X) = G(X)$ and $bh(x) = H(X)$ for some $a, b \in R$ giving $abf(X) = G(X)H(X)$. Write $ab = \prod p_i$ as a product of irreducibles/primes in the UFD R. We know from homework 8 that $(p_1)[X]$ is a prime ideal of $R[X]$ and so $G(X)H(X) = 0$ in $R[X]/(p_1)[X]$ which is an integral domain. Thus either $G(X)$ or $H(X)$ is in $(p_1)[X]$ and so one of $p_1^{-1}G(X)$ and $p_1^{-1}H(X)$ is in $R[X]$, let's say the former. Then $\prod_{i>1} p_i f(X) = (p_i^{-1}G(X))H(X) = G'(X)H(X)$. Repeating the argument gives $f(X) = G(X)H(X)$ as desired. ☐

Proposition 6. *R is a UFD iff $R[X]$ is a UFD, but $R[X]$ is a PID iff R is a field.*

Proof. One direction is trivial. Suppose R is a UFD and $f(X) \in R[X]$. Then $f = P_1 \cdots P_n$ uniquely in $F[X]$ where $F = \operatorname{Frac} R$. By Gauss' lemma we may take $P_i \in R[X]$ to get $f(X) = aQ_1 \cdots Q_n$ where $a \in R$ and Q_i have coefficients with gcd 1. Each Q_i is irreducible and $a \in R$ has a unique factorization $\prod a_i$ into irreducibles. Reciprocally, any other factorization in $F[X]$ is of the form $P_1 \dots P_n$ where $P_i(X) = f_i Q_i(X)$ with $f_i \in F$. Thus any other factorization over $R[X]$ is of the form $\prod b_i \prod c_i Q_i(X)$ and since the coefficients of Q_i have gcd 1 it follows that $c_i Q_i$ is irreducible iff c_i is a unit in R. Thus $\prod a_i = \prod b_i \prod c_i$ and since R is a UFD, we get the desired unique factorization. ☐

Example 7. In class I worked out the following example: If $n \in \mathbb{Z}_{\geq 1}$ then the number of $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$ is

$$4(d_+(n) - d_-(n))$$

where $d_\pm(n)$ is the number of divisors of n which are $\equiv \pm 1 \pmod 4$.

This relied on the fact that $n = x^2 + y^2 = (x + iy)(x - iy)$ in $\mathbb{Z}[i]$ which is a UFD. Here is a summary:

1. If $x = yz$ in $\mathbb{Z}[i]$ then $|x|^2 = |y|^2|z|^2$ and $|x|^2, |y|^2, |z|^2 \in \mathbb{Z}$. Thus if $|x|^2$ is an integer prime p then $x \in \mathbb{Z}[i]$ must be irreducible.

2. $2 = -i(1 + i)^2$ and $1 + i$ is irreducible by the criterion.

3. If $p \equiv 3 \pmod 4$ is an integer prime and $p \mid x^2 + y^2$ then $p \mid x, y$. Otherwise we'd get, e.g., if $p \nmid y$, that $-1 \equiv (x/y)^2 \pmod p$ and raising to $(p-1)/2$ gives a contradiction. Thus p must be a prime of $\mathbb{Z}[i]$ as well since otherwise you'd get $p = xy$ so $p^2 = |x|^2|y|^2$ and since x, y not units we'd get that $|x|^2 = |y|^2 = p$. But if $x = m + ni$ then $|x|^2 = m^2 + n^2 = p$ and this cannot be by the above.

4. If $p \equiv 1 \pmod 4$ is an integer prime. Then $\mathbb{F}_p^\times$ is cyclic of order $p-1$, divisible by 4, so there is $a \in \mathbb{F}_p^\times$ of order 4. Then $p \mid a^2 + 1 = (a + i)(a - i)$. If p we a prime of $\mathbb{Z}[i]$ then $p \mid a + i$ or $p \mid a - i$ which cannot be as $p \nmid \pm 1$. Thus p factors into irreducibles and if $p = xy$ then $|x|^2 = |y|^2 = 1$ in which case x, y are irreducibles. If $x = a + bi$ then $|x|^2 = a^2 + b^2 = p$ so $y = \overline{x} = a - bi$. For such p write $p = (a_p + ib_p)(a_p - ib_p)$ as a product of irreducibles.

5. The units of $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$. Indeed, as on the homework, $z \in \mathbb{Z}[i]$ is a unit iff $|z| = 1$ and simply solving yields the unit.

6. Decompose n in $\mathbb{Z}$ as $n = 2^a \prod_{p \equiv 1 \pmod 4} p^{n_p} \prod_{q \equiv 3 \pmod 4} q^{m_q}$. If $n = x^2 + y^2$ then $q \equiv 3 \pmod 4$ must divide both x and y. Divide out by q^2 and repeat to obtain that $n = x^2 + y^2$ implies that each m_q must be even. Now $n = (x + iy)(x - iy)$ has prime decomposition in $\mathbb{Z}[i]$ (up to units):

$$(1 + i)^{2a} \prod (a_p + ib_p)^{n_p} (a_p - ib_p)^{n_p} \prod q^{m_q}$$

and necessarily $x + iy$ must be a product of some of these prime factors (again up to units):

$$z = x + iy = (1 + i)^b \prod (a_p + ib_p)^{u_p} (a_p - ib_p)^{v_p} \prod q^{r_q}$$

But given that $z\overline{z} = n$ we deduce that $b = a$, $u_p + v_p = n_p$ and $r_q = m_q/2$ so (up to units)

$$x + iy = (1+i)^a \prod (a_p + ib_p)^{u_p} (a_p - ib_p)^{n_p - u_p} \prod q^{m_q/2}$$

and, up to units, the only choices are $0 \leq u_p \leq n_p$.

The total number of $x + iy$ is therefore

$$4 \prod (n_p + 1)$$

where 4 is the number of units.

7. A divisor $d \mid n$ is odd iff it is of the form $\prod_p p^{k_p} \prod q^{l_q}$ with $k_p \leq n_p$ and $l_p \leq m_q$. Moreover, $d \equiv (-1)^{\sum l_q} \pmod 4$. Thus

$$\begin{aligned} d_+(n) - d_-(n) &= \sum_{2 \nmid d \mid n} (d \mod 4) \\ &= \sum_{k_p, l_q} (-1)^{\sum l_q} \\ &= \sum_{k_p} \sum_{l_q} (-1)^{\sum l_q} \\ &= \prod (n_p + 1) \prod_q \sum_{l_q = 0}^{m_q} (-1)^{l_q} \\ &= \prod (n_p + 1) \end{aligned}$$

since each m_q is even and therefore the sums are all 1 in the second to last row.

Putting everything together yields the desired result.