MATH 494 2018 DISCUSSION 4: SOME FACTS ABOUT UFDS

BEN GOULD

Contents

1. Introduction

We will prove[1] some interesting results about unique factorization domains, or UFDs. UFDs and their special properties come up surprisingly often in algebra and algebraic geometry, and their proofs often use only 494-type material.

We recall the definition: a commutative ring S with identity 1 is a UFD when every nonunit in S can be written as a product of irreducible elements, such that this expression is unique up to reordering of the irreducibles and scaling by a unit. There are *many* equivalent definitions. One should recall that in a UFD, an element is prime if and only if it is irreducible.

We will prove three interesting statements about them, namely the following. Throughout, R will be a commutative ring with multiplicative identity 1.

Theorem 1.1 (Gauss' Lemma)**.** *If F is the fraction field of R, then $f \in R[x]$ is irreducible over R if and only if f is irreducible and primitive over F.*

Theorem 1.2. *If R is a UFD, then the colon[2] of principal ideals is principal. If R is additionally assumed to be Noetherian, then the converse is also true.*

Theorem 1.3 (Kaplansky)**.** *If R is a UFD, then every nonzero prime ideal contains a nonzero principal prime ideal (equivalently, an irreducible element).*

Let's get started.

[1]Some of the claims and proofs presented here come from Morandi's book *Field and Galois Theory.*

[2]We'll define this below.

2. Gauss' Lemma

We restate the proposition: *If F is the fraction field of R, then $f \in R[x]$ is irreducible over R if and only if f is irreducible and primitive over F.*

This is known as Gauss' Lemma, apparently. Recall that a polynomial $f \in S[x]$, where S is a UFD (more generally, a GCD domain) with 1, is *primitive* provided that the gcd in S of its coefficients is 1. Additionally, one may always write a polynomial $g \in S[x]$ as $c(g) \cdot g_*$, where $c(g) = \gcd_S(g\text{'s coefficients})$, and g_* is obtained from g by dividing by $c(g)$. Then $c(g)$ is defined to be the *content of g*, with g_* its *primitive part*. We will also use the convention that a polynomial is primitive if its content is a unit.

Assume first that f is irreducible and primitive over F. Suppose that f factors as $f = gh$ in $R[x]$; since g and h naturally lie also in $F[x]$ and f is irreducible over F, (WOLOG) g is a constant. However then g divides the coefficients of f, contradicting that f is primitive. So f is irreducible over R.

For the next part of the proof, prove the following lemma (which is often also called Gauss' Lemma):

Lemma 2.1. *When R is a UFD with $f, g \in R[x]$, we have $c(fg) = c(f) \cdot c(g)$. In particular, deduce that the product of primitive polynomials is primitive. (Hint: for a contradiction, consider a prime π dividing the coefficients of fg, and the domain $(R/(\pi))[x]$.)*

Conversely, assume that f is irreducible over R. We may write, as above, $f = c(f) \cdot f_*$, where since f is irreducible over R, $c(f)$ is a unit in R; it follows that f is primitive. If f is not irreducible over F, then write $f = gh$ with $g, h \in F[x]$ both of degree ≥ 1. We may write $gh = (a/b)g_* \cdot h_*$ with $g_*, h_* \in R[x]$ primitive parts, and $a, b \in R$ relatively prime (why?). Thus $bf(x) = ag_* \cdot h_*$, so $b = b \cdot c(f) = c(b \cdot f) = a \cdot c(g_* h_*) = a$ by the lemma. However a and b are relatively prime, so they both must be units in R. However then $(a \cdot g_*)(b^{-1} \cdot h_*)$ is a nontrivial factorization of f, contradicting irreducibility over R. So f is irreducible over F, as required.

3. Colon criterion (Noetherian rings)

We restate the proposition: *If R is a UFD, then the colon of principal ideals is principal. If R is additionally assumed to be Noetherian, then the converse is also true.*

First we note that in a Noetherian ring R, the decomposition of any element into irreducibles is immediately given (though not in general unique). To see this, consider the family of non-zero, non-unit elements a of R not equal to a product of irreducibles. Recall one of the equivalent definitions of a Noetherian ring to choose a maximal such (a). Then writing $a = a_1 a_2$, as a is not irreducible, we may assume that a_1 is also not a product of irreducibles. However then (a_1) strictly contains (a), contradicting maximality of a.

For ideals $I, J \subset R$ we define the ideal

$$I : J := \{b \in R \mid bJ \subset I\}$$

called the *colon* of I and J in R, or the *fractional ideal* of I and J in R. Of course we have the analogous notion for principal ideals; the statement in the theorem says that for $f, g \in R$ there is $\phi \in R$ such that $(f) : (g) = (\phi)$.

We assume both f and g are nonzero, avoiding trivialities. Write $f = u\pi_1^{m_1} \cdots \pi_r^{m_r}$ and $g = v\pi_1^{n_1} \cdots \pi_r^{nr}$ for irreducibles π_i and u, v units in R. It is clear (is it?) that

$$(f) : (g) = \left(\prod_{i=1}^{r} \pi_i^{\min\{m_i - n_i, 0\}} \right).$$

The interesting part of the statement is the Noetherian case. Prove the following lemma:

Lemma 3.1. *If T is a domain with the product that every element is a product of irreducibles, then T is a UFD if and only if every irreducible of T is prime.*

Then it suffices, following the lemma, to show that if $\pi \in R$ is irreducible, then it is prime. Suppose that π divides ab, so that $b \in (\pi) : (a)$. Choose $h \in R$ such that $(\pi) : (a) = (h)$; then $\pi \in (h)$, and since π is irreducible, we conclude that h is a unit or $(\pi) = (h)$. In the former case, π divides a; in the latter, π divides b.

4. Kaplansky's Theorem

We restate the proposition: *If R is a UFD, then every nonzero prime ideal contains a nonzero principal prime ideal (equivalently, an irreducible element).*

Let P be a nonzero prime ideal of R. For $a \in P$ nonzero, write $a = \pi_1 \cdots \pi_n$ for irreducibles $\pi_i \in R$. As P is prime, one of the π_i lies in P. Therefore P contains the principal prime (π_i).

Conversely, suppose every nonzero prime of R contains a nonzero principal prime. Define

$$\mathcal{S} := \{a \in R \setminus \{0\} : a \text{ is a unit or factors into a product of primes}\}.$$

Of course, if $\mathcal{S} = R \setminus \{0\}$ then R is a UFD (if this is not clear, prove it). Else, let $0 \neq a \in R \setminus \mathcal{S}$. Applying Zorn's lemma, let I be the ideal of R containing a be maximal among ideals disjoint from $\mathcal{S}$; we claim that I is prime. Modulo the proof of this statement, we may find $\pi \in I$ a prime in R. However then $\pi \in \mathcal{S}$ as π is prime, so we obtain a contradiction. It follows that R is a UFD.

Now we prove that I is prime. If not, there are $b, c \in R \setminus I$ such that $ab \in I$. Then $I + bR$ and $I + cR$ contain I, so that they must intersect $\mathcal{S}$. Choose $x \in \mathcal{S} \cap (I + bR)$ and $y \in \mathcal{S} \cap (I + cR)$. Write $x = u_1 + br_1$ and $y = u_2 + cr_2$ with $c_i \in I$, $r_i \in R$. Then $xy = u_1(u_2 + cr_2) + bcr_1r_2 \in I$, since $bc \in I$. However $xy \in \mathcal{S}$. Thus $\mathcal{S} \cap I \neq \emptyset$, a contradiction. It follows that I is prime, finishing the proof.