Fields of fractions

$\mathbb{Z}$ has a special relationship to $\mathbb{Q}$. Namely, $\mathbb{Q}$ is the set $\{\frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0\}$. i.e. $\mathbb{Q}$ is $\mathbb{Z}$ along w/ inverses for each element. $\mathbb{Q}$ is called the field of fractions of $\mathbb{Z}$. We can define this more generally:

Def: Let R be an integral domain. The <u>field of fractions</u> F of R is the set

$$F := \left\{\frac{a}{b} \,\middle|\, a,b \in R,\ b \neq 0\right\} \quad \text{w/} \quad \frac{a}{b} = \frac{c}{d} \iff ad = cb.$$

This is a ring w/ operations $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ and $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$.

In fact, F is a field, since for $\frac{a}{b} \neq 0$, $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1$, so nonzero elements are units.

R is naturally a subring of F via the map $R \hookrightarrow F$ defined $r \mapsto \frac{r}{1}$. This is in fact an injection since $\frac{r}{1} = 0 \iff r = 0$.

Ex: The field of fractions of $\mathbb{Q}[x]$ is the set of rational functions, $\frac{f(x)}{g(x)}$, f and g polynomials. e.g. $\frac{x^2+7}{x-1}$ is a rational function.

If R is an int. domain, F its field of fractions, then $R[x] \subseteq F[x]$. $F[x]$ is a Euclidean domain and thus a UFD, so any $f \in F[x]$

can be factored uniquely into a product of irreducibles.

A natural question is: can we do the same in $R[x]$? i.e. is $R[x]$ a UFD? If R is not a UFD, then the constants in $R[x]$ can't be uniquely factored so $R[x]$ is not a UFD.

However, if R is a UFD, then $R[x]$ is! To show this, we first need the following important result:

Gauss' lemma: Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$, then it's reducible in $R[x]$.

Note that this implies that if a polynomial with integer coefficients can't be factored over $\mathbb{Z}$ then it can't be factored over $\mathbb{Q}$.

Pf of Gauss' lemma: Suppose $p(x) = A(x) B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$.

Multiplying through by a common denominator for the coefficients, we get $d\,p(x) = a'(x)\, b'(x)$, for $a'(x), b'(x) \in R[x]$, $d \in R$ nonzero.

If d is a unit in R, we're done, since $p(x) = d^{-1} a'(x)\, b'(x)$.

Thus, assume d is not a unit. We can write it as a product of irreducibles in R: $d = p_1 \cdots p_n$.

Then $(p_1) \subseteq R$ is prime, so $p_1 R[x]$ is prime as well, and $(R/p_1R)[x]$ is an integral domain.

Looking at the image of $dp(x) = a'(x) b'(x)$ in $(R/p_1R)[x]$, we get $0 = \overline{a'(x)}\,\overline{b'(x)}$. Thus, one of the factors, say $\overline{a'(x)}$, must be 0. This means all the coefficients of $a'(x)$ are divisible by p_1, so $\frac{1}{p_1} a'(x)$ has coefficients in R.

That is, we can cancel a factor of p_1 from d and from $a'(x)$ in $dp(x) = a'(x) b'(x)$ and still have an equation in $R[x]$.

We can use the same method to cancel all the factors of d, and end up w/ $p(x) = a(x) b(x)$, where $a(x), b(x) \in R[x]$. $\square$

Note that the converse doesn't hold since elements of R are not always units and can thus be irreducible.

Ex: $7x + 14 = 7(x+2)$ is reducible in $\mathbb{Z}[x]$, but not in $\mathbb{Q}[x]$, since $7 \in \mathbb{Q}[x]$ is a unit.

However, we get the following partial converse:

Cor: Let R be a UFD and F its field of fractions. Let $p(x) \in R[x]$. Suppose the g.c.d. of the coefficients is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it's irreducible in $F[x]$.

Pf: By Gauss' Lemma, if $p(x)$ is reducible in $F[x]$, it's reducible in $R[x]$. Conversely, if it's reducible in $R[x]$, then since the g.c.d. of the coefficients is 1, $p(x) = a(x)b(x)$, where neither a or b is constant. Thus, a and b aren't units in $F[x]$. □

Now we can prove the main theorem of the section:

Theorem: R is a UFD $\Leftrightarrow$ $R[x]$ is a UFD.

Pf: We already saw that $R[x]$ a UFD $\Rightarrow$ R a UFD.

Conversely, suppose R is a UFD and F its field of fractions. Let $p(x) \in R[x]$ be nonzero. Let d be the g.c.d. of the coefficients of $p(x)$ so that $p(x) = d\,p'(x)$, where the g.c.d. of the coefficients of $p'(x)$ is 1.

Since d' can be factored uniquely in R, we just need to show $p'(x)$ can be factored uniquely in $R[x]$. That is, we can just assume the g.c.d. of the coefficients of $p(x)$ is 1 and that $\deg p(x) > 0$.

$F[x]$ is a UFD, so $p(x)$ can be factored uniquely into irreducibles in $F[x]$. Thus, there is a factorization in $R[x]$ whose factors are F-multiples of the factors in $F[x]$.

Since the g.c.d. of the coeffs of $p(x)$ is 1, the g.c.d. of the coeffs in the factors must be 1. By the previous corollary, each of these factors is thus irreducible in $R[x]$.

For uniqueness, assume $p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$ are two factorizations into irreducibles. The g.c.d. of the coeffs of each of the factors is thus 1, so they each have positive degree.

Each factor is irreducible in $F[x]$, which implies $r=s$, and, up to rearrangement of the factors, $q_i(x) = \frac{a}{b} q_i'(x)$, $a, b \in R$.

Thus, $b q_i(x) = a q_i'(x)$, but since the coeffs have g.c.d. 1, $a = ub$, $u \in R$ a unit. Thus, $\frac{a}{b} = u$, which proves uniqueness. □

__Cor:__ R a UFD $\Rightarrow R[x_1, \dots, x_n]$ a UFD.