NAP 2019, CLASS #7, MAY 16, 2019

ROGER & SYLVIA WIEGAND

• In section 3.6 on "Highest Common Factors", also called "Greatest Common Divisors" (GCDs), we outlined a procedure for finding GCD(a, b) and also LCM(a, b) for a, b both nonzero in a unique factorization domain (UFD) R. Namely, write a, b as products of irreducible elements (possibly multiplied by units), and group associates and elements together so that

$$a = a_1^{e_1} \cdot a_2^{e_2} \cdots a_m^{e_m}, \quad b = a_1^{f_1} \cdot a_2^{f_2} \cdots a_m^{f_m} u$$

where u is an appropriate unit of R, the a_i are irreducible elements, e_i and f_j are non-negative integers (possibly 0), and a_i and a_j are not associates if $i \neq j$. Then it is easy to see that GCD$(a, b) = a_1^{d_1} \cdot a_2^{d_2} \cdots a_m^{d_m}$, where each $d_i = \min(e_i, f_i)$ and LCM$(a, b) = a_1^{c_1} \cdot a_2^{c_2} \cdots a_m^{c_m}$, where each $c_i = \max(e_i, f_i)$. We also described how to find GCDs and LCMs by iterating the procedure, that is, GCD$(a, b, c) =$ (GCD(GCD$(a, b), c)$), etc. This is done more rigorously in Theorem 3.10 of Garling. We will not need to worry about GCDs and LCMs of infinite sets.

Notice that GCDs and LCMs are not usually unique. If GCD$(a, b) = d$ and u is a unit, then $ud =$ GCD(a, b) also. Similarly LCMs.

• Discussed forming a *field of fractions* F of an integral domain R. This is done more completely in Section 3.2 of Garling. To summarize:
$F = \frac{R \times R^*}{\sim}$, where $R^* = R \setminus \{0\}$, the nonzero elements of R, and $\sim$ is the relation $(a, b) \sim (c, d) \iff ad = bc$, for pairs $(a, b), (c, d) \in R \times R^*$. We showed that $\sim$ is an *equivalence relation*. Therefore the equivalence classes $[(a, b)]$ form a *partition* of $R \times R^*$. For convenience we refer to an equivalence class $[(a, b)]$ as "$\frac{a}{b}$" from now on. We showed that inverses exist for nonzero a/b. The rest of the proof that F is a field is in Garling. Basically all of this works the same as building $\mathbb{Q}$ from $\mathbb{Z}$.

• In Section 3.7, Polynomials over UFDs, we defined *primitive polynomial* and the *content* $C(f)$ for a polynomial f of a UFD R, and proved:

Theorem 3.12: Let R be a UFD. If $f, g \in R[x]$ are primitive, then fg is primitive. (We used "reduction mod p" to show that no irreducible element p of R divides all the coefficients of fg. It really just amounts to the fact that a polynomial ring over a domain is a domain.)

Theorem 3.11: Let F be a the field of fractions of a UFD R. If $f \in F[x]$ is nonzero, then there exists $\beta \in F \setminus \{0\}$ such that $f(x) = \beta g(x)$ and $g(x)$ is primitive in $R[x]$. Moreover if also $f(x) = \beta' g'(x)$, where $\beta' \in F \setminus \{0\}$ and $g'(x)$ is primitive in $R[x]$, then there exists a unit u of R such that $g(x) = ug'(x)$ and $\beta' = u\beta$.