Division with Remainder

In $\mathbb{Z}$, we had the extremely important Division Algorithm. This theorem states that if a and b are integers with $b \neq 0$, then there exists a "quotient" q and a "remainder" r such that $a = qb + r$, and, moreover, the remainder is not too large – $0 \leq r < |b|$. This is the result from which most of the interesting results and algorithms in $\mathbb{Z}$ spring.

We'd like to generalize this property to integral domains. Notice that one problem is the appearance of absolute value in the bound on r: in general, rings do not have anything like absolute value, or a way to compare the "sizes" of two elements. However we did describe such a gadget for some rings: multiplicative norms. Recall that $N : R \to \mathbb{N}$ is a multiplicative norm if (1) $N(x) = 0$ iff $x = 0$, (2) $N(xy) = N(x)N(y)$, and (3) if $N(x) = 1$ then x is a unit. These properties do generalize the absolute value.

Definition 1 (Euclidean Norm)**.** *Let R be a domain.*

- *We say that a multiplicative norm $N : R \to \mathbb{N}$ is a* Euclidean norm *if for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and $0 \leq N(r) < N(b)$.*
- *If there is a Euclidean norm on R, we say that R is a* Euclidean Domain*.*

Of course $\mathbb{Z}$ is a Euclidean Domain with norm $N(a) = |a|$. The existence of a Euclidean norm on R is very powerful. For instance, many of the nice properties of $\mathbb{Z}$ which we derived from the Division Algorithm have analogues in any Euclidean Domain. More generally, the norm allows us to recover some of the benefits of mathematical induction.

Proposition 1. *Every Euclidean Domain is also a GCD Domain.*

Proof. Let R be a Euclidean domain with norm N. We want to show that for all $a \in R$, for all $b \in R$, the set $\mathsf{gcd}(a, b)$ is not empty. We proceed by strong induction on $N(a)$.

Base case. Suppose $N(a) = 0$. Then $a = 0$, and so $b \in \mathsf{gcd}(a, b)$ for all b.

Inductive Step. Let $a \in R$ and suppose that the result holds for all a' with $1 \leq N(a') < N(a)$. In particular, note that $a \neq 0$. Now let $b \in R$. By the division algorithm we may decompose b as $b = qa + r$, where $0 \leq N(r) < N(a)$. If $r = 0$ then $a|b$ and we have $a \in \mathsf{gcd}(a, b)$. If $r \neq 0$, then by the inductive hypothesis $\varnothing \neq \mathsf{gcd}(r, a) = \mathsf{gcd}(b - qa, a) = \mathsf{gcd}(b, a)$ as needed. □

Proposition 2. *Every Euclidean domain is a Unique Factorization domain.*

The proof for $\mathbb{Z}$ generalizes.

Proposition 3. *Every field is a Euclidean domain.*

Proof. Define a mapping $N : F \to \mathbb{N}$ by $N(x) = 0$ if $x = 0$ and 1 if $x \neq 0$. We can see that N is a Euclidean norm. □

Example: The Gaussian Integers

Proposition 4. *$\mathbb{Z}[i]$ is a Euclidean domain under the norm $N(a+bi) = a^2+b^2$.*

Proof. Let $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$ be Gaussian integers, with $\beta \neq 0$. Thinking of α and β as elements of $\mathbb{Q}(i)$, we have

$$\frac{\alpha}{\beta} = t_1 + t_2 i = \frac{a_1 b_1 + a_2 b_2}{b_1^2 + b_2^2} + \frac{a_2 b_1 - a_1 b_2}{b_1^2 + b_2^2} i.$$

Choose integers q_1 and q_2 such that $|q_1 - t_1| \leq \frac{1}{2}$ and $|q_2 - t_2| \leq \frac{1}{2}$. (Note that this is always possible.) Let $\gamma = q_1 + q_2 i$, and let $\delta = \alpha - \gamma\beta$. Note that by construction, γ and δ are in $\mathbb{Z}[i]$.

We now have

$$\begin{aligned} N(\delta) &= N(\alpha - \gamma\beta) = N\left((\frac{\alpha}{\beta} - \gamma)\beta \right) = N(\frac{\alpha}{\beta} - \gamma) N(\beta) \\ &= ((q_1 - t_1)^2 + (q_2 - t_2)^2) N(\beta) \leq \frac{1}{2} N(\beta) < N(\beta), \end{aligned}$$

as needed. ∎

Corollary 5. *$\mathbb{Z}[i]$ is a GCD domain and a UFD.*

Here is a worked example of the division algorithm in the Gaussian integers. Let $\alpha = 10 + 7i$ and $\beta = 3 + 2i$. Now

$$\frac{\alpha}{\beta} = \frac{44}{13} + \frac{1}{13} i = (3 + \frac{5}{13}) + (0 + \frac{1}{13}) i.$$

Let $t_1 = 3$ and $t_2 = 0$, so that $\gamma = 3$. Now $\delta = \alpha - \gamma\beta = 1 + i$. We then have $10 + 7i = 3(3 + 2i) + (1 + i)$ and $N(1 + i) < N(3 + 2i)$.

Exercises

1. (k-stage Euclidean)
2. (Factorization in $\mathbb{Z}[i]$)