7510 HW 8

Duncan Wilkie

1 November 2022

Problem 1 (D&F 7.5.2). *Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).*

Proof. Denote the quotient field of R by Q and consider the map $\iota : D^{-1}R \to Q$ that maps $\frac{r}{d}$, an equivalence class of elements of $R \times D$, to the equivalence class containing the pair (r, d) in Q. This is a homomorphism:

$$\iota\left(\frac{r}{d} \cdot \frac{r'}{d'}\right) = \iota\left(\frac{rr'}{dd'}\right) = \iota\left(\frac{r}{d}\right)\iota\left(\frac{r'}{d'}\right),$$

where multiplicative closure of D is necessary for the middle term to be interpretable, and well-definedness is used to choose (r, d) and (r', d') as representatives for the computation of the product on the right. We can immediately notice that the kernel of ι is the additive identity of $D^{-1}R$: if $\iota(\frac{r}{d}) \in 0$, then $d0 = 0 = rq$ for $q \in Q \neq 0$, and since R is an integral domain, this implies $r = 0$. By the first isomorphism theorem, then,

$$D^{-1}R \cong \iota(D^{-1}R) \leq Q.$$

□

Problem 2 (D&F 8.1.3). *Let R be a Euclidean domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.*

Proof. Suppose $a \in R$ is nonzero and has $N(a) = m \leq N(a')$, for all $a' \in R$ and N the norm on R. By the division algorithm, there exist $q, r \in R$ such that $1 = qa + r$ with $r = 0$ or $N(r) < N(a)$; the second condition is never met by minimality of the norm of a, so $r = 0$, and q is the inverse of a (since Euclidean domains are commutative), making it a unit. Accordingly, since norms must have nonnegative codomain, any element of norm zero must have minimal norm, and therefore be a unit. □

Problem 3 (D&F 8.1.7). *Find a generator of the ideal $(85, 1 + 13i)$ in $\mathbb{Z}[i]$, i.e. a greatest common divisor for 85 and $1 + 13i$, by the Euclidean algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.*

Proof. In the Gaussian rationals, the division (taking the one with larger norm in the numerator) is

$$\frac{85}{1 + 13i} = \frac{85(1 - 13i)}{170} = \frac{85}{170} - \frac{1105}{170}i$$

The nearest Gaussian integer to this (entry-wise) is $-6i$. Accordingly,

$$85 = (-6i)(1 + 13i) + (7 + 6i);$$

indeed, $N(7 + 6i) = 85 < N(1 + 13i) = 170$. Continuing,

$$\frac{1 + 13i}{7 + 6i} = \frac{(1 + 13i)(7 - 6i)}{(7 + 6i)(7 - 6i)} = \frac{85 + 85i}{85} = 1 + i,$$

so

$$1 + 13i = (1 + i)(7 + 6i) + 0$$

Accordingly, the last nonzero remainder, $7 + 6i$, is the gcd of these two Gaussian integers.

Same story:

$$\frac{53 + 56i}{47 - 13i} = \frac{(53 + 56i)(47 + 13i)}{(47 - 13i)(47 + 13i)} = \frac{1763 + 3321i}{2378} \approx 1 + i$$

$$\Rightarrow (53 + 56i) = (1 + i)(47 - 13i) + (-7 + 22i).$$

$$\frac{47 - 13i}{-7 + 22i} = \frac{(47 - 13i)(-7 - 22i)}{(-7 + 22i)(-7 - 22i)} = \frac{-43 - 1125i}{533} \approx -1 - 2i$$

$$\Rightarrow 47 - 13i = (-1 - 2i) \cdot (-7 + 22i) + (-4 - 5i).$$

$$\frac{-7 + 22i}{-4 - 5i} = \frac{(-7 + 22i)(-4 + 5i)}{(-4 - 5i)(-4 + 5i)} = \frac{-82 - 123i}{41} = -2 - 3i$$

$$\Rightarrow -7 + 22i = (-2 - 3i)(-4 - 5i) + 0.$$

The last nonzero remainder is $-4 - 5i$; this is then the gcd (up to a unit). $\square$

Problem 4 (D&F 8.1.10). *Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$*

Proof. Since $\mathbb{Z}[i]$ is a Euclidean domain, the ideal I is principal. Call its generator α. Take any representative a of any nonidentity coset; apply the division algorithm with numerator $a + \alpha$ and denominator α. Accordingly, for some $q, r \in R$ one has $a = q\alpha + r$ with either $r = 0$ or $N(r) < N(\alpha)$. However, if $r = 0$, then $a = q\alpha \Rightarrow a \in I$, but $a + I$ is assumed nonidentity. Accordingly, any nonidentity coset in $\mathbb{Z}[i]/I$ has a representative with norm less than $N(\alpha)$.

The set of all possible representatives is therefore finite: the count of integers a_1, a_2 (the parts of $a = a_1 + a_2 i$) such that $a_1^2 + a_2^2 < N(\alpha)$ is certainly finite, and this is an upper bound on the number of cosets, since every coset must have a representative in this set, and if two cosets share a representative, they're not different cosets. $\square$