D-MATH Algebra II FS 2014
Prof. Brent Doran

Solutions 3

Unique factorization domains

1. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

   Solution : Introduce the following size function

   $$\sigma(a+b\sqrt{2}) := \left|(a+b\sqrt{2})(a-b\sqrt{2})\right| = \left|a^2-2b^2\right|.$$

   We first want to show that $\mathbb{Z}[\sqrt{2}]$ is an integral domain. We can deduce this from the fact that the size function is multiplicative, i.e. $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ for all α, β in $\mathbb{Z}[\sqrt{2}]$. We show that division with remainder is possible with respect to σ. Let $\alpha = a+b\sqrt{2}$ and let $\gamma = c+d\sqrt{2}\neq 0$, with $a,b,c,d\in\mathbb{Z}$. Then

   $$\frac{\alpha}{\gamma} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}\cdot\frac{c-d\sqrt{2}}{c-d\sqrt{2}} = \underbrace{\frac{ac-2bd}{c^2-2d^2}}_{=:\alpha_1} + \underbrace{\frac{bc-ad}{c^2-2d^2}}_{=:\beta_1}\sqrt{2}.$$

   We write $\alpha_1\in\mathbb{Q}$ as $\alpha_1 = a_1+s_1$, whereby a_1 is the closest integer to α_1 and r_1 is the remaining fractional part. We do the same with β_1, setting $\beta_1 = b_1+t_1$. The above division is now expressed as

   $$\frac{\alpha}{\gamma} = \underbrace{\left(a_1+b_1\sqrt{2}\right)}_{=:\ q\in\mathbb{Z}[\sqrt{2}]} + \underbrace{\left(s_1+t_1\sqrt{2}\right)}_{=:\ R},$$

   and we are left to check that $r := R\gamma\in\mathbb{Z}[\sqrt{2}]$ and $\sigma(r)<\sigma(\gamma)$ if $R\neq 0$. First, observe that $r=\alpha-q\gamma\in\mathbb{Z}[\sqrt{2}]$. Second, we extend σ to $\mathbb{Q}(\sqrt{2})$ and compute

   $$\sigma(r) = \sigma(R)\sigma(\gamma) = \left|s_1^2-2t_1^2\right|\sigma(\gamma) \leqslant \left(\frac{1}{4}+\frac{1}{2}\right)\sigma(\gamma)$$

   where the last inequality comes from the triangle inequality together with the fact that $|s_1|,|t_1|<1/2$ (by assumption on the decomposition in the nearest integer value plus fractional part).

2. (a) Show that the size function on $\mathbb{Z}[i]$ is multiplicative.

   Solution : The size function for the Gaussian integers is given by $\sigma(\alpha)=\alpha\overline{\alpha}$, $\alpha\in\mathbb{Z}[i]$. It follows immediately that

   $$\sigma(\alpha\beta) = \alpha\beta\overline{\alpha}\overline{\beta} = \sigma(\alpha)\sigma(\beta).$$

(b) Describe a systematic way to do division with remainder in $\mathbb{Z}[i]$, and use it to divide $4+36i$ by $5+i$.

Solution : Let $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$. Then

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\sigma(\beta)}.$$

Let us introduce some more notation : $\alpha\overline{\beta} =: a + bi$, with $a, b \in \mathbb{Z}$, and $s := \sigma(\beta) \in \mathbb{N}$, thus

$$\frac{\alpha}{\beta} = \frac{a}{s} + \frac{b}{s}i,$$

where, for each of the fraction, we may apply division with remainder for the integers.

Implementing this for

$$\frac{4+36i}{5+i} = \frac{56}{26} + \frac{176}{26}i = 2 + 6i + \left(\frac{4}{26} + \frac{20}{26}i\right).$$

Multiplying on both sides by $5+i$ leaves us with

$$4 + 36i = (2+6i)(5+i) + \left(\frac{4+20i}{5-i}\right)$$

where the remaining fraction is given explicitly by

$$4 + 36i - (2+6i)(5+i) = 4i.$$

(c) Let $a, b \in \mathbb{Z}$. Show that their greatest common divisors in $\mathbb{Z}$ and $\mathbb{Z}[i]$ coincide.

Solution : Let $d = \gcd(a, b)$. Clearly, d also divides a and b in $\mathbb{Z}[i]$. Let $\alpha \in \mathbb{Z}[i]$ be a non-unit element such that α divides both a and b. Because by Bézout, there exist integers m and n such that $d = am + bn$, α also divides d. Hence d is also the greatest common divisor in $\mathbb{Z}[i]$.

(d) Let $p \in \mathbb{N}$ be a prime with $p \equiv 3 \bmod 4$. Show that p is also prime in $\mathbb{Z}[i]$.

Solution : We show that p is prime in $\mathbb{Z}[i]$. Primes in $\mathbb{Z}[i]$ are exactly the irreducible elements. Let us write $p = \alpha\beta$ in $\mathbb{Z}[i]$. We will show that, if α is not a unit, β needs to be one. First note that the units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. In particular, β is a unit if and only if $\sigma(\beta) = 1$. Because

$$\sigma(p) = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta),$$

we need to show that $\sigma(\alpha) = p^2$. So far, we know that $\sigma(\alpha)$ divides p^2. By assuming that α is not a unit, we ruled out the possibility $\sigma(\alpha) = 1$. Suppose now that we would have

$$\sigma(\alpha) = a^2 + b^2 = p.$$

Because $p \equiv 3 \bmod 4$, it is odd and we may assume that a is odd and b even. But then $a^2 \equiv 1 \bmod 4$ and $b^2 \equiv 0 \bmod 4$, and we can not have the above equality.

(e) Decompose $-1 + 3i$ into irreducible factors in $\mathbb{Z}[i]$.

Solution : We use the fact that the size function is multiplicative. Because $\sigma(-1 + 3i) = 10$, the only potential factorisation is one in two irreducible factors of "size" 2 and 5 respectively. For instance

$$-1 + 3i = (1 + i)(1 + 2i).$$

3. Decompose $x^3 + x + 2$ into irreducible factors in $\mathbb{F}_3[x]$.

Solution : We first observe that 2 is a root of the polynomial in $\mathbb{F}_3$. This leads to the factorization

$$x^3 + x + 2 = (x - 2)(x^2 + 2x + 2)$$

in $\mathbb{F}_3[x]$. We can check directly that the polynomial $x^2 + 2x + 2$ is irreducible over $\mathbb{F}_3[x]$, hence we are done.

4. Let $F[x]$ be a polynomial ring over a field F. Prove that there are infinitely many monic irreducible polynomials in $F[x]$.
Hint : Check out Euclid's proof of the infinitude of primes.

Solution : We mimic Euclid's proof : Let $p_1, \dots, p_n$ be n monic irreducible polynomials in $F[x]$. We show that there is always more. In fact, set

$$P := p_1 \cdot p_2 \cdots p_n + 1.$$

The polynomial P is monic and can be factorized in a product of monic irreducible polynomials. (Recall that $F[x]$ is a unique factorisation domain.) Consider one of these monic irreducible factor. Let us call it p_* and show that it is distinct from every monic irreducible polynomial in $p_1, \dots, p_n$. This is the case, because otherwise, i.e. if $p_* = p_i$ for some $1 \leqslant i \leqslant n$, $p_* = p_i$ would divide P, and by the definition of P, p_i can divide P only if it divides 1. This contradicts the assumption that p_i is irreducible, and hence we can always find one more monic irreducible polynomial in $F[x]$.

5. Establish a bijective correspondence between maximal ideals of $\mathbb{R}[x]$ and points in the upper half-plane $\{(x, y) : x, y \in \mathbb{R}, y \geqslant 0\}$.

Solution : You already know the bijective correspondence between maximal ideals of $\mathbb{C}[x]$ and points in $\mathbb{C}$ from the lecture. (This is Corollarry 11.8.5 in Artin.) Explicitly, this was the correspondence between monic irreducible polynomials in $\mathbb{C}[x]$, which are of the form $x - a$ for a complex number a, and their root, i.e. a. In the real case, not all polynomials have a real root. In fact, for a polynomial of degree two, there can be one real root, two distinct real roots or two complex conjugated roots, depending on whether the discriminant of the polynomial is positive, zero or negative. Only in this last case is a polynomial of degree two irreducible over $\mathbb{R}$. On the other hand, real polynomials of degree > 2 are necessarily factorizable : Since over $\mathbb{C}$, there is a factorisation in linear terms with for each complex root, its complex conjugate also as a root, a higher degree real polynomials factors over $\mathbb{R}$ in a product of linear and quadratic polynomials.

Then, via the correspondence described above, each real root corresponds to its value on the real line, and for each complex root, since its conjugate is also a root, we assign the corresponding point in the upper half-plane.