Prof. Dr. Marcus Greferath
Dept. of Mathematics and Systems Analysis
School of Sciences
Aalto University

Spring 2019

MS-E1997: Abstract Algebra II

Problem Set III

Problem 1: For the ring $\mathbb{Z}[i]$ of Gaussian numbers show the following:

(a) If $\varphi(a+ib) = a^2 + b^2$ then $(\mathbb{Z}[i], \varphi)$ is a Euclidean domain.

(b) A prime $p \in \mathbb{Z}$ is reducible in $\mathbb{Z}[i]$ if and only if it is a sum of two squares.

(c) Factorize 210 into irreducible elements over $\mathbb{Z}[i]$.

Work: For **(a)** we observe that $\varphi(xy) = \varphi(x)\varphi(y)$ because we know this already about the absolute value on $\mathbb{C}$. For the division algorithm let $x, y \in \mathbb{Z}[i]$ be given, then we have $x/y =: z \in \mathbb{C}$. Both real and imaginary part of z have distance ≤ 0.5 to an integer (just by rounding), and hence we find $u \in \mathbb{Z}[i]$ with $\varphi(z-u) \leq 0.5^2 + 0.5^2 = 0.5$. Defining $r = z - u$ we have $x/y = u + r$ and hence $x = uy + ry$ where obviously $\varphi(ry) = \varphi(r)\varphi(y) \leq 0.5\varphi(y) < \varphi(y)$ since $y \neq 0$. This completes the proof of the statements under **(a)**.

(b) By the multiplicativity of the φ-function we observe that units in $\mathbb{Z}[i]$ must be of φ-value 1, and this means they are one of $1, i, -i, -1$. If now p is a prime in $\mathbb{Z}$ and $p = a^2+b^2$ for $a, b \in \mathbb{Z}$, then a, b are both nonzero, which clearly leads to $p = (a+ib)(a-ib)$ and hence we have a (proper) factorization for p. Indeed, observe that $\varphi(a \pm ib) \geq 2$ these factors are definitely non-units. On the other hand, if p is a prime in $\mathbb{Z}$ which is a non-prime in $\mathbb{Z}[i]$ then there is a proper factorization $p = xy$. $\varphi(x) > 1 < \varphi(y)$ and $p^2 = \varphi(p) = \varphi(x)\varphi(y)$. But this implies $p = \varphi(x)$ (and also $p = \varphi(y)$) and the latter is clearly the sum of two squares.

(c) We first factorize over $\mathbb{Z}$ and obtain $210 = 7 \cdot 3 \cdot 5 \cdot 2$. Among these the only Gaussian non-primes are 5 and 2, as $5 = (2+i)(2-i)$ and $2 = (1+i)(1-i)$. For this reason we end up with the factorization

$$210 \;=\; 7 \cdot (2+i) \cdot (2-i) \cdot 3 \cdot (1+i) \cdot (1-i).$$

Problem 2: Show that for an integer polynomial $f \in \mathbb{Z}[x]$ a factorization over $\mathbb{Z}$ induces a factorization over $\mathbb{Z}/p\mathbb{Z}$ for all primes $p \in \mathbb{N}$ which do not divide $\mathrm{lc}(f)$. Deduce an irreducibility criterion from this.

Work: For notation purposes we agree on $\nu : \mathbb{Z} \longrightarrow \mathbb{Z}_p,\ z \mapsto \overline{z}$ standing for the natural epimorphism; furthermore we extend this epimorphism coordinatewise to $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$. We then observe that if p is a prime that does not divide the leading coefficient of $f \in \mathbb{Z}[x]$ then $\deg(\overline{f}) = \deg(f)$, and every factorization of $f = gh$ with g, h being of positive degree induces a factorization $\overline{f} = \overline{g}\,\overline{h}$ with factors of positive degree. For this reason we conclude that if $\overline{f}$ is irreducible, then f will be irreducible. The criterion should therefore be formulated as follows:

> If $f \in \mathbb{Z}[x]$ is a polynomial, and $p \in \mathbb{Z}$ a prime such that p does not divide the leading coefficient of f then the irreducibility of $\overline{f} \in \mathbb{Z}_p[x]$ implies the irreducibility of f.

Problem 3: Let F be a field and denote by D the formal derivative on $F[x]$. Show that D satisfies the sum-rule, the product rule and the chain rule.

Work: For the sum rule we (may) assume that $f, g \in F[x]$ are given by $f = \sum_{i=0}^{n} f_i x^i$ and $g = \sum_{i=0}^{n} g_i x^i$. Then we can write

$$\begin{aligned} D(f+g) &= D\sum_{i=0}^{n}(f_i + g_i)x^i = \sum_{i=1}^{n} i(f_i+g_i)x^{i-1} \\ &= \sum_{i=1}^{n} i f_i x^{i-1} + \sum_{i=1}^{n} i g_i x^{i-1} = Df + Dg. \end{aligned}$$

For the product rule we first show the claim for polynomials of the form $f = a\,x^m$ for some $m \in \mathbb{N}$. So, we obtain

$$\begin{aligned} D(fg) &= D(ax^m \sum_{i=0}^{n} g_i x^i) = D\sum_{i=0}^{n} a g_i x^{i+m} \\ &= \sum_{i=0}^{n} a(i+m) g_i x^{i+m-1} = amx^{m-1}\sum_{i=0}^{n} g_i x^i + ax^m \sum_{i=1}^{n} g_i i x^{i-1} \\ &= (Df)g + f(Dg), \end{aligned}$$

as required. This result combined with the sum rule then shows the product rule in general. In particular we obtain F-linearity of the derivative, meaning $D(af) = aDf$ for $a \in F$.

Finally, for the chain rule we do a similar reduction: we assume $f = x^m$ and work with general g. Then $D(f \circ g) = D(g^m)$ which by successive application of the product rule (induction) can be seen to be the same as $mg^{m-1}Dg$, for all $m \in \mathbb{N}$. From here we get the general result again via the sum rule.

Problem 4: Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$. What is the degree of of this extension over $\mathbb{Q}$. Compute the multiplicative inverse of each nonzero element in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and represent it as a linear combination in with respect to the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Work: To begin with, the set $S := \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ certainly forms a subring of $\mathbb{R}$, and to make it a field, we only have to show that it contains the multiplicative inverse of each of its elements. We write $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = x+y\sqrt{3}$ where $x = a+b\sqrt{2}$ and $y = c + d\sqrt{2}$. The inverse of $x + y\sqrt{3}$ is given by

$$\frac{1}{x + y\sqrt{3}} \quad = \quad \frac{x - y\sqrt{3}}{x^2 - 3y^2},$$

where $x^2 - 3y^2 = a^2 + 2b^2 - 3c^2 - 6d^2 + 2\sqrt{2}(ab - 3cd)$. Setting $\overline{x} := a - b\sqrt{2}$ and $\overline{y} := c - d\sqrt{2}$ we obtain similarly $\overline{x}^2 - 3\overline{y}^2 = a^2 + 2b^2 - 3c^2 - 6d^2 - 2\sqrt{2}(ab - 3cd)$, and hence

$$(x^2 - 3y^2)(\overline{x}^2 - 3\overline{y}^2) \ = \ (a^2 + 2b^2 - 3c^2 - 6d^2)^2 - 8(ab - 3cd)^2 \ \in \ \mathbb{Q}.$$

For this reason we finally have

$$\frac{1}{x + y\sqrt{3}} \quad = \quad \frac{(x - y\sqrt{3})(\overline{x}^2 - 3\overline{y}^2)}{(x^2 - 3y^2)(\overline{x}^2 - 3\overline{y}^2)}$$

which is obviously an element of S. Thus we see that S is a field extension of $\mathbb{Q}$ that contains $\sqrt{2}$ and $\sqrt{3}$, and therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq S$. On the other hand every field extension of $\mathbb{Q}$ that contains $\sqrt{2}$ and $\sqrt{3}$ must also contain $\sqrt{6}$ and hence it must contain S. For this reason it is clear that $S \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which proves equality.

As to the degree of this extension we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ provided $x^2 - 3$ does not already split over $\mathbb{Q}(\sqrt{2})$. Then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ as required. In fact if $x^2 - 3$ splits over $\mathbb{Q}(\sqrt{2})$ then we would have $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. This immediately leads to $3 = a^2 + 2b^2 + 2\sqrt{2}ab$ which in turn implies $\sqrt{2}$ to be a rational number unless one of a or b is zero. If $a = 0$ then we have $3 = 2b^2$ which finally leads to a contradiction to irrationality of $\sqrt{3}$, and assuming $b = 0$ we come to the same conclusion. Hence we have a degree 4 extension.

You are encouraged to collaborate in preparing solutions, however, please submit individual write-ups.