Silvain Rideau
1091 Evans
silvain.rideau@berkeley.edu
www.normalesup.org/~srideau/en/teaching

Solutions to homework 9

Due April 17th

Problem 1 :
Let $D \in \mathbb{Z}$ and let $\alpha \in \mathbb{C}$ be such that $\alpha^2 = D$.

1. Show that $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.

   Solution: First it is a subgroup: $(a + b\alpha) - (c + d\alpha) = (a - c) + (b - d)\alpha \in \mathbb{Z}[\alpha]$ if a, b, c, $d \in \mathbb{Z}$. As for multiplication: $(a + b\alpha) \cdot (c + d\alpha) = ac + bc\alpha + ad\alpha + bd\alpha^2 = (ac + Dbd) + (bc + ad)\alpha \in \mathbb{Z}[\alpha]$. We also have $1 = 1 + 0\alpha \in \mathbb{Z}[\alpha]$.

2. If $D \equiv 1 \mod 4$, show that $\mathbb{Z}[\frac{1+\alpha}{2}] = \{a + b\frac{1+\alpha}{2} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ that contains $\mathbb{Z}[\alpha]$.

   Solution: We have $(a + b\frac{1+\alpha}{2}) - (c + d\frac{1+\alpha}{2}) = (a - c) + (b - d)\frac{1+\alpha}{2} \in \mathbb{Z}[\frac{1+\alpha}{2}]$ and $(a+b\frac{1+\alpha}{2})\cdot(c+d\frac{1+\alpha}{2}) = ac+(bc+ad)\frac{1+\alpha}{2}+bd(\frac{1+\alpha}{2})^2$ and $(\frac{1+\alpha}{2})^2 = \frac{1+2\alpha+\alpha^2}{4} = \frac{1+\alpha}{2}+\frac{D-1}{4}$. It follows that $(a + b\frac{1+\alpha}{2}) \cdot (c + d\frac{1+\alpha}{2}) = (ac + bd\frac{D-1}{4}) + (bc + ad + bd)\frac{1+\alpha}{2} \in \mathbb{Z}[\frac{1+\alpha}{2}]$ if $4|D - 1$.

   Moreover, $a + b\alpha = (a - b)2b\frac{1+\alpha}{2}$ and hence $\mathbb{Z}[\alpha] \leqslant \mathbb{Z}[\frac{1+\alpha}{2}]$.

3. Let $\beta = \frac{1+\alpha}{2}$ and $\overline{\beta} = \frac{1-\alpha}{2}$ if $D \equiv 1 \mod 4$ and $\beta = \alpha$, $\overline{\beta} = -\alpha$ otherwise. We define $N(a + \beta b) = (a + \beta b) \cdot (a + \overline{\beta} b)$. Show that for all $x \in \mathbb{Z}[\beta]$, $N(x) \in \mathbb{Z}$ and if $D < 0$, then $N(x) = |x|^2 \geqslant 0$ where $|x|$ is the complex norm.

   Solution: Let us first assume that $D \not\equiv 1 \mod 4$. We have $N(a + \beta b) = a^2 + ab\alpha - ab\alpha - \alpha^2 b^2 = a^2 - b^2 D \in \mathbb{Z}$. If $D \equiv 1 \mod 4$, $N(a+\beta b) = a^2+(\frac{1+\alpha}{2}+\frac{1-\alpha}{2})ab+\frac{1+\alpha}{2}\frac{1-\alpha}{2}b^2 = a^2 + ab + \frac{1-D}{4}b^2 \in \mathbb{Z}$.

   If $D < 0$, then α is purely imaginary so $-\alpha$ is the complex conjugate of α and $\frac{1-\alpha}{2}$ is the complex conjugate of $\frac{1+\alpha}{2}$. It follows that $N(a+\beta b) = (a+\beta b)\overline{(a + \beta b)} = |a+\beta b|^2$ and it is positive.

4. Show that for all x, $y \in \mathbb{Z}[\beta]$, $N(xy) = N(x)N(y)$.

   Solution: Let us first assume that $D \not\equiv 1 \mod 4$. We have $(a + b\alpha)(c + d\alpha) = (ac + Dbd) + (bc + ad)\alpha$ and thus $N((a + b\alpha) \cdot (c + d\alpha)) = (ac + Dbd)^2 - D(bc + ad)^2 = a^2c^2 + 2acDbd + D^2b^2d^2 - D(b^2c^2 + 2bcad + a^2d^2) = a^2c^2 + D^2b^2d^2 - Db^2c^2 - Da^2d^2 = (a^2 - Db^2)(c^2 - Dd^2) = N(a + b\alpha)N(c + d\alpha)$.

   The equality for $D \equiv 1 \mod 4$ can also be shown by a computation as above, but it is very cumbersome. Let us try to be more subtle. Let us denote by $\overline{a + b\beta} = a + b\overline{\beta}$. Let us now compute $\overline{(a + b\beta)} \cdot \overline{(c + d\beta)} = (a + b\frac{1-\alpha}{2})(c + d\frac{1-\alpha}{2}) = ac + (bc + ad)\frac{1+\alpha}{2} + bd(\frac{1-\alpha}{2})^2$. We also have $(\frac{1-\alpha}{2})^2 = \frac{1-2\alpha+\alpha^2}{4} = \frac{1-\alpha}{2} + \frac{D-1}{4}$ and $\overline{(a + b\beta)} \cdot \overline{(c + d\beta)} = (ac + bd\frac{D-1}{4}) + (bc + ad + bd)\frac{1-\alpha}{2} = \overline{(a + b\beta)(c + d\beta)}$. It follows that $N((a + b\beta)(c + d\beta)) = (a+b\beta)(c+d\beta)\overline{(a + b\beta)(c + d\beta)} = (a+b\beta)(c+d\beta)(a+b\overline{\beta})(c+d\overline{\beta}) = N(a+b\beta)N(c+d\beta)$.

5. Show that $x \in \mathbb{Z}[\beta]$ is a unit if and only if $N(x) \in \{1, -1\}$.

   Solution: If $N(a+b\beta) = \varepsilon \in \{1,-1\}$ then $(a+b\beta)\varepsilon(a+b\overline{\beta}) = 1$. Note that, if $D \not\equiv 1 \mod 4$, $a+b\overline{\beta} = a-b\beta \in \mathbb{Z}[\beta]$ and if $D \equiv 1 \mod 4$, $a+b\frac{1-\alpha}{2} = (a+b) - b\frac{1+\alpha}{2} \in \mathbb{Z}[\beta]$ so $\varepsilon(a+b\overline{\beta})$ is the inverse of $a+b\beta$ in $\mathbb{Z}[\beta]$.

   Conversely, if $x \in \mathbb{Z}[\beta]$ is invertible, then $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$ and hence $N(x) \in \mathbb{Z}^\star = \{1,-1\}$.

6. Let us now assume that $D = -3$, show that for all $x \in \mathbb{C}$ there exists $a \in \mathbb{Z}[\beta]$ such that $|x-a| < 1$.

   Solution: Pick any $x \in \mathbb{C}$ and write it as $a + b\frac{1+\alpha}{2}$, where $a, b \in \mathbb{R}$. We can do so because 1 and $\frac{1+\alpha}{2}$ are not colinear in $\mathbb{C}$ as an $\mathbb{R}$-vector space. There exists a_0 and $b_0 \in \mathbb{Z}$ such that $|a-a_0| \leqslant \frac{1}{2}$ and $|b-b_0| \leqslant \frac{1}{2}$. Let $y = a_0 + b_0\beta \in \mathbb{Z}[\beta]$. We have $|x-y| = |(a-a_0) + (b-b_0)\beta| \leqslant |(a-a_0)| + |b-b_0| \cdot |\beta| \leqslant 1$ because $|\beta| = 1$. Note that we might have equality if and only if $|a-a_0| = |b-b_0| = \frac{1}{2}$ and in that case $|(a-a_0)+(b-b_0)\beta|^2 = |\frac{3}{4} + \frac{i\sqrt{3}}{4}|^2 = \frac{9}{16} + \frac{3}{16} = \frac{3}{4} < 1$, so $|x-y| < 1$.

   We can also see that in a more geometric way. The points in $\mathbb{Z}[\beta]$ form equilateral triangles whose side is 1. Any point in $\mathbb{C}$ is in one of those triangles and hence is at most at the distance of the center of symmetry from one vertex of the triangle. We can actually compute this distance to get a better estimate but, in any case, that distance is at most the height of the triangle: $\frac{\sqrt{2}}{3} < 1$.

7. Let us still assume that $D = -3$, show that $\mathbb{Z}[\beta]$ is Euclidian (for the norm N).

   Solution: Pick a, $b \in \mathbb{Z}[\beta]$ such that $b \neq 0$ and let $c = \frac{a}{b} \in \mathbb{C}$. By the above, we find $q \in \mathbb{Z}[\beta]$ such that $N(q-c) < 1$. Let $r = a - bq \in \mathbb{Z}[\beta]$. We have $N(r) = |b(c-q)|^2 = N(b)|c-q|^2 < N(b)$.

8. (Harder) Assume $D < 0$ and $D \equiv 1 \mod 4$, show that for all $x \in \mathbb{C}$ there exists $a \in \mathbb{Z}[\beta]$ such that $|x-a| \leqslant \frac{1+|D|}{4\sqrt{|D|}}$. Conclude that, if $D \in \{-3,-7,-11\}$, $\mathbb{Z}[\beta]$ is Euclidian for the norm N.

   Solution: The points of $\mathbb{Z}[\beta]$ form parallelograms in $\mathbb{C}$ that are translations of each other, so we can focus on the parallelogram whose summits are 0, 1, β and $1+\beta$. The vertical line at abscissa $\frac{1}{2}$ (resp. 1) separates points in the parallelogram closest to 0 (resp. β) from those closest to 1 (resp. $1+\beta$). The perpendicular to the side $[0;\beta]$ (resp. $[1;1+\beta]$) that goes through its center separates the points closest to 0 (resp. 1) from the points closest to β (resp $1+\beta$). Finally the perpendicular to the diagonal $[\beta;1]$ separates the points closer to β from those closer to 1 (the other perpendicular to the diagonal is not relevant because points equi-distant to 0 and $1+\beta$ are in fact to β or 1). If you draw all those lines you partition the parallelogram into four polygon that contain the points closer to each of the summits. You should really draw the situation to see what I am talking about.

   The equation of the perpendicular to the side $[0;\beta]$ is $y = \frac{\sqrt{|D|}}{4} - |D|^{-\frac{1}{2}}(x - \frac{1}{4})$ so this line crosses the vertical line at abscissa 0 at $a_1 = (0, \frac{|D|+1}{4\sqrt{|D|}})$ and the vertical line at abscissa $\frac{1}{2}$ at $a_2 = (\frac{1}{2}, \frac{|D|-1}{4\sqrt{|D|}})$. It follows that the polygon whose summits are 0, a_1, a_2 and $\frac{1}{2}$ contains the points that are closest to 0. The polygons for the other summits can be determined similarly. Actually if you draw the four parallelograms around 0, you will see that the points closet to 0 in $\mathbb{C}$ form an hexagon whose summits

are $(0, \frac{|D|+1}{4\sqrt{|D|}})$, $(\frac{1}{2}, \frac{|D|-1}{4\sqrt{|D|}})$, $(\frac{1}{2}, \frac{1-|D|}{4\sqrt{|D|}})$, $(0, -\frac{|D|+1}{4\sqrt{|D|}})$, $(-\frac{1}{2}, \frac{1-|D|}{4\sqrt{|D|}})$ and $(-\frac{1}{2}, \frac{|D|-1}{4\sqrt{|D|}})$. One can easily compute that 0 is at distance $\frac{|D|+1}{4\sqrt{|D|}}$ from each of those points and that, the above hexagon being convex, any point in it is also at distance at most $\frac{|D|+1}{4\sqrt{|D|}}$ from 0. It follows that any point in $\mathbb{C}$ is at distance at most $\frac{|D|+1}{4\sqrt{|D|}}$ from a point in $\mathbb{Z}[\beta]$.

Now, if $D \in \{-3, -7, -11\}$, $\frac{(|D|+1)^2}{16|D|} \in \{\frac{1}{3}, \frac{4}{7}, \frac{9}{11}\}$ and each of these are smaller than 1. The same proof as for $D = -3$ therefore applies to $D = -7$ and $D = -11$.