Algebra, SOLUTIONS Assignment 11
Due, Monday, Nov 27

Note: All of our rings are commutative with 1. Recall \( Z[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in Z \} \). Let us also define \( Q(\sqrt{2}) := \{ a + b\sqrt{2} : a, b \in Q \} \). For \( \alpha = a + b\sqrt{2} \in Q(\sqrt{2}) \) we set \( \overline{\alpha} = a - b\sqrt{2} \), called the conjugate of \( \alpha \).

1. On \( Q(\sqrt{2}) \) define \( d(a + b\sqrt{2}) = |a^2 - 2b^2| \). Show \( d(\alpha \beta) = d(\alpha)d(\beta) \) for all \( \alpha, \beta \in Q(\sqrt{2}) \). (It may help to note \( d(\alpha) = |a\overline{a}| \).)

Solution: Let \( \alpha = a + b\sqrt{2} \) and \( \beta = c + d\sqrt{2} \) so that \( \alpha\beta = (ac + 2bd) + (ad + bc)\sqrt{2} \) and

\[
(ac + 2bd)^2 - 2(ad + bc)^2 = (a^2 - 2b^2)(c^2 - 2d^2)
\]

This is not just serendipitous. Conjugacy satisfies \( \overline{\alpha\beta} = \overline{\alpha}\overline{\beta} \) and so

\[
d(\alpha\beta) = |\alpha\beta\overline{\alpha\beta}| = |\alpha\overline{\alpha}\beta\overline{\beta}| = d(\alpha)d(\beta)
\]

2. Now consider \( d \) defined on the nonzero elements of \( Z[\sqrt{2}] \). Show \( d(\alpha) \geq 1 \) for all such \( \alpha \) and that \( d(\alpha) \leq d(\alpha\beta) \) for any two nonzero \( \alpha, \beta \in Z[\sqrt{2}] \).

Solution: As \( d(\alpha) = |a^2 - 2b^2| \) it must be a nonnegative integer. If it were zero we would have \( a^2 = 2b^2 \), so \( (a/b)^2 = 2 \), contradicting the irrationality of \( \sqrt{2} \). Now \( d(\alpha\beta) = d(\alpha)d(\beta) \geq d(\alpha) \) as \( d(\beta) \geq 1 \).

3. Let \( \alpha, \beta \in Z[\sqrt{2}] \) with \( \beta \neq 0 \). Set \( \alpha/\beta = x + y\sqrt{2} \in Q(\sqrt{2}) \) with \( x, y \in Q \). Let \( x_0, y_0 \in Z \) with \( |x - x_0| \leq \frac{1}{2} \) and \( |y - y_0| \leq \frac{1}{2} \). Set \( q = x_0 + y_0\sqrt{2} \). Show that \( d(\alpha - q\beta) < d(\beta) \). [Note: This shows that \( Z[\sqrt{2}] \) is a Euclidean ring.]

Solution:

\[
\alpha - q\beta = (x + y\sqrt{2})\beta - (x_0 + y_0\sqrt{2})\beta = (x_1 + y_1\sqrt{2})\beta
\]

where \( x_1, y_1 \) rational, each of absolute value at most \( \frac{1}{2} \). Thus \( d(\alpha - q\beta) = d(\beta)(|x_1^2 - 2y_1^2|) \). But \( |x_1^2 - 2y_1^2| \leq \frac{1}{2} \) so \( d(\alpha - q\beta) \leq \frac{1}{4}d(\beta) \).

4. Illustrate the above by taking \( \alpha = 53 + 94\sqrt{2} \) and \( \beta = 5 + 2\sqrt{2} \) and finding specific \( q, r \) with \( \alpha = q\beta + r \) and either \( r = 0 \) or \( d(r) < d(\beta) \).

Solution:

\[
\frac{53 + 94\sqrt{2}}{5 + 2\sqrt{2}} = \frac{53 + 94\sqrt{2}}{5 + 2\sqrt{2}} \cdot \frac{5 - 2\sqrt{2}}{5 - 2\sqrt{2}} = \frac{-111 + 364\sqrt{2}}{17}
\]

so take \( q = -7 + 21\sqrt{2} \). Then \( q\beta = 49 + 91\sqrt{2} \) and \( r = 4 + 3\sqrt{2} \) and \( d(r) = |16 - 9 \cdot 2| = 2 < d(\beta) = 17 \).
5. Show that no $\alpha \in \mathbb{Z}[\sqrt{2}]$ has $d(\alpha) = 3$. (Hint: Look at $a, b$ modulo 3.)
Solution: If $\alpha = a + b\sqrt{2}$ we would have $a^2 - 2b^2 = \pm 3$. But then $a^2 - 2b^2 \equiv 0 \mod 3$ which has only the solution $a \equiv b \equiv 0 \mod 3$. But if $a, b$ are both divisible by 3 then $a^2 - 2b^2$ would be divisible by 9 and so couldn’t be three.

6. Show that a nonzero $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $d(\alpha) = 1$.
Solution: If $d(\alpha) = 1$ then $|\alpha\overline{\alpha}| = 1$ so $\alpha\overline{\alpha} = \pm 1$ so either $\alpha^{-1} = \overline{\alpha}$ or $\alpha^{-1} = -\overline{\alpha}$ and either way $\alpha^{-1} \in \mathbb{Z}[\sqrt{2}]$. Conversely, if $\alpha$ was a unit we would have a $\beta$ with $1 = \alpha\beta$ but then $d(\alpha) \leq d(1) = 1$ but the only values of $d(\cdot)$ are nonnegative integers so $d(\alpha) = 1$.

7. Show that if $\pi$ is a nonunit of $\mathbb{Z}[\sqrt{2}]$ and $d(\pi)$ is a prime in the natural numbers then $\pi$ is a prime in $\mathbb{Z}[\sqrt{2}]$.
Solution: Say $\pi = \alpha\beta$. Then $d(\pi) = d(\alpha)d(\beta)$. As $d(\pi)$ is a prime in the natural numbers one of $d(\alpha), d(\beta)$ must be one and so (by previous part) it must be a unit.

8. Which of the following are primes: $2, 5 + \sqrt{2}, 17 + 8\sqrt{2}, 7, 3$. For those that are not primes, give a nontrivial factorization (including the argument that the factors are not themselves units) and for those that are primes give an argument why they are.
Solution:

(a) $2 = \sqrt{2}\sqrt{2}$, composite. Nontrivial factorization as $d(\sqrt{2}) = 2$.
(b) Prime as $d(5 + \sqrt{2}) = |25 - 2| = 23$ is prime in the integers.
(c) $17 + 8\sqrt{2} = (3 + \sqrt{2})(5 + \sqrt{2})$ (not easy to find!), composite.
   Nontrivial as $d(3 + \sqrt{2}) = 7$ and $d(5 + \sqrt{2}) = 23$.
(d) $7 = (3 + \sqrt{2})(3 - \sqrt{2})$ composite. Nontrivial as $d(3 \pm \sqrt{2}) = 7$.
(e) Prime. If $3 = \alpha\beta$ then $9 = d(\alpha)d(\beta)$. If $d(\alpha) = 1$ then (previous part) $\alpha$ is a unit so factorization trivial and similarly if $d(\beta) = 1$.
   So for the factorization to be nontrivial we must have $d(\alpha) = d(\beta) = 3$ but (previous part), there ain’t no such animal.

Mathematics seems much more real to me than business - in the sense that, well, what’s the reality in a McDonald’s stand? It’s here today and gone tomorrow. Now, the integers - that’s reality.
When you prove a theorem, you’ve really done something that has substance to it, to which no business venture can compare for reality.
   – Jim Simons