Solutions 10

P10.1. Consider the subrings $\mathbb{Z}[\sqrt{17}] := \{a + b\sqrt{17} \mid a, b \in \mathbb{Z}\}$ and

$$\mathbb{Z}\left[\tfrac{1+\sqrt{17}}{2}\right] := \left\{a + b\left(\tfrac{1+\sqrt{17}}{2}\right) \,\middle|\, a, b \in \mathbb{Z}\right\}$$

of the field $\mathbb{R}$ of real numbers. For each subring, describe the elements in the field of fractions. Are these two fields the same? Is one contained in the other?

Solution. From the inclusions

$$\mathbb{Z}[\sqrt{17}] \subset \mathbb{Z}\left[\tfrac{1+\sqrt{17}}{2}\right] \subset \mathbb{R}\,,$$

we see that the subrings are domains. We claim that the field of fractions for both these subrings is

$$\mathbb{Q}(\sqrt{17}) := \left\{a + b\sqrt{17} \,\middle|\, a, b \in \mathbb{Q}\right\} \subset \mathbb{R}\,.$$

By construction, $\mathbb{Q}(\sqrt{17})$ is the smallest subfield of $\mathbb{R}$ containing 1 and $\sqrt{17}$. Since both subrings contain 1 and $\sqrt{17}$, their fields of fractions also contain $\mathbb{Q}(\sqrt{17})$.

For the reverse inclusion in the first case, observe that every element in the field of fractions for the domain $\mathbb{Z}[\sqrt{17}]$ can be expressed, for some integers a, b, c, and d with $(c, d) \neq (0, 0)$, in the form

$$\begin{aligned}
\frac{a + b\sqrt{17}}{c + d\sqrt{17}} &= \left(\frac{a + b\sqrt{17}}{c + d\sqrt{17}}\right)\left(\frac{c - d\sqrt{17}}{c - d\sqrt{17}}\right) \\
&= \frac{(a\,c - 17\,b\,d) + (b\,c - a\,d)\sqrt{17}}{c^2 - 17\,d^2} \\
&= \left(\frac{a\,c - 17\,b\,d}{c^2 - 17\,d^2}\right) + \left(\frac{b\,c - a\,d}{c^2 - 17\,d^2}\right)\sqrt{17} \in \mathbb{Q}(\sqrt{17})\,.
\end{aligned}$$

Notice that the only rational solution to the equation $c^2 - 17\,d^2 = 0$ is $c = d = 0$.

For the second case, set $\xi := \frac{1+\sqrt{17}}{2}$. Observe that $\xi^2 - \xi - 4 = 0$, $1 - \xi = \frac{1-\sqrt{17}}{2}$, and $\xi(1 - \xi) = -4$. Every element in the field of fractions for the domain $\mathbb{Z}[\xi]$ can be expressed, for some integers a, b, c, and d with $(c, d) \neq (0, 0)$, in the form

$$\begin{aligned}
\frac{a + b\,\xi}{c + d\,\xi} &= \left(\frac{a + b\,\xi}{c + d\,\xi}\right)\left(\frac{c + d\,(1 - \xi)}{c + d\,(1 - \xi)}\right) \\
&= \frac{(a\,c + a\,d - 4\,b\,d) + (-a\,d + b\,c)\,\xi}{c^2 + c\,d - 4\,d^2} \\
&= \left(\frac{a\,c + a\,d - 4\,b\,d}{c^2 + c\,d - 4\,d^2}\right) - \left(\frac{a\,d - b\,c}{c^2 + c\,d - 4\,d^2}\right)\xi \in \mathbb{Q}(\sqrt{17})\,.
\end{aligned}$$

Again, the only rational solution to the equation $c^2 + c\,d - 4\,d^2 = 0$ is $c = d = 0$. □

P10.2. **i.** Confirm that the ring

$$\mathbb{Z}[\sqrt{-2}] := \left\{a + b\sqrt{-2} \in \mathbb{C} \,\middle|\, a, b \in \mathbb{Z}\right\}$$

is a Euclidean domain with the Euclidean function $\nu \colon \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \to \mathbb{N}$ defined, for any integers a and b, by $\nu(a + b\sqrt{-2}) := a^2 + 2\,b^2$.

ii. Find a greatest common divisor of 12 and $1 + 2\sqrt{-2}$ in the ring $\mathbb{Z}[\sqrt{-2}]$.

Solution. Observe that

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

i. Let a, b, c, and d be integers. Divide the complex number $w := a + b\sqrt{-2}$ by the complex number $z := c + d\sqrt{-2}$. In other words, there is a complex number $c = x + y\sqrt{-2}$ where x and y are real numbers such that $w = c\,z$. Choose a nearest element $p + q\,\mathrm{i}$ in $\mathbb{Z}[\sqrt{-2}]$, so $x := p + x_0$ and $y := q + y_0$ where p and q are integers and $-\frac{1}{2} \leqslant x_0, y_0 < \frac{1}{2}$. The product $(p + q\sqrt{-2})\,z$ is the required point in the principal ideal $\langle z \rangle$ because

$$\left|x_0 + y_0\sqrt{-2}\right|^2 = x_0^2 + 2\,y_0^2 < \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$$

and

$$\begin{aligned} \left|w - (p + q\sqrt{-2})\,z\right|^2 &= \left|c\,z - (p + q\sqrt{-2})\,z\right|^2 \\ &= \left|(x_0 + y_0\sqrt{-2})\,z\right|^2 = \left|(x_0 + y_0\sqrt{-2})\right|^2 |z|^2 < \frac{3}{4}|z|^2 < |z|^2 . \end{aligned}$$

Setting $q := p + q\sqrt{-2}$ and $r := w - (p + q\sqrt{-2})\,z$, we conclude that $w = q\,z + r$ where $r = 0$ or $\nu(r) < \nu(z)$.

ii. In the field $\mathbb{C}$ of complex numbers, we have

$$\frac{12}{1 + 2\sqrt{-2}} = \frac{12}{1 + 2\sqrt{-2}}\left(\frac{1 - 2\sqrt{-2}}{1 - 2\sqrt{-2}}\right) = \frac{12 - 24\sqrt{-2}}{9} = 1.3333\ldots - 2.6666\ldots\sqrt{-2}.$$

As $(1-3\sqrt{-2})(1+2\sqrt{-2}) = 1-3\sqrt{-2}$, division with remainder in the ring $\mathbb{Z}[\sqrt{-2}]$ gives $12 = (1 - 3\sqrt{-2})(1 + 2\sqrt{-2}) + (-1 + \sqrt{-2})$. Again, working in $\mathbb{C}$, we have

$$\frac{1 + 2\sqrt{-2}}{-1 + \sqrt{-2}} = \frac{1 + 2\sqrt{-2}}{-1 + \sqrt{-2}}\left(\frac{-1 - \sqrt{-2}}{-1 - \sqrt{-2}}\right) = \frac{3 - 3\sqrt{-2}}{3} = 1 - \sqrt{-2}.$$

As $(1 - \sqrt{-2})(-1 + \sqrt{-2}) = 1 + 2\sqrt{-2}$, division with remainder in the ring $\mathbb{Z}[\sqrt{-2}]$ gives $1 + 2\sqrt{-2} = (1 - \sqrt{-2})(-1 + \sqrt{-2}) + (0)$. Thus, the Euclidean Algorithm establishes that $1 - \sqrt{-2}$ is a greatest common divisor for 12 and $1 + 2\sqrt{-2}$ in the ring $\mathbb{Z}[\sqrt{-2}]$. □

Remark. The units in the ring $\mathbb{Z}[\sqrt{-2}]$ are ± 1, so the only other greatest common divisor for 12 and $1 + 2\sqrt{-2}$ is $-1 + \sqrt{-2}$.

P10.3. Let $\mathbb{F}_2 := \mathbb{Z}/\langle 2\rangle$ be the field with two elements. Find the lowest-degree polynomial f in the ring $\mathbb{F}_2[x]$ such that

$$f \equiv 1 \bmod x+1 \qquad\qquad f \equiv x^2+x \bmod x^3+x^2+1$$
$$f \equiv 0 \bmod x^2+x+1 \qquad\qquad f \equiv x^2+x+1 \bmod x^4+x+1$$

Solution. The Extended Euclidean algorithm applied to $g_1 := x+1$ and $g_2 := x^2+x+1$ gives $g_2 + x\,g_1 = (1)(x^2+x+1) + (x)(x+1) = 1$.

Table 1. Local variables when computing $\gcd(g_2, g_1)$

d_0	d_1	s_0	s_1	t_0	t_1	q
x^2+x+1	$x+1$	1	0	0	1	x
$x+1$	1	0	1	1	x	$x+1$
1	0	1		x		

Hence, the first iteration of the loop in the Effective Remainder Algorithm yields

$$(1)(x^2+x+1)(1) + (x)(x+1)(0) = x^2+x+1 = (0)(x^3+1) + (x^2+x+1)\,.$$

We verify that $x^2+x+1 = (x+1)(x+1)+1 = (x^2+x+1)+0$.

The Extended Euclidean algorithm applied to $g_3 = x^3+x^2+1$ and $g_1\,g_2 = x^3+1$ gives $x\,g_3 + (x+1)\,g_1\,g_2 = (x)(x^3+x^2+1) + (x+1)(x^3+1) = 1$.

Table 2. Local variables when computing $\gcd(g_2, g_1\,g_2)$

d_0	d_1	s_0	s_1	t_0	t_1	q
x^3+x^2+1	x^3+1	1	0	0	1	1
x^3+1	x^2	0	1	1	1	x
x^2	1	1	x	1	$x+1$	x^2
1	0	x		$x+1$		

Hence, the second iteration of the loop in the Effective Remainder Algorithm yields

$$\begin{aligned} &(x)(x^3+x^2+1)(x^2+x+1) + (x+1)(x^3+1)(x^2+x) \\ &= x^4+x^3+x^2 \\ &= (0)(x^6+x^5+x^2+1) + (x^4+x^3+x^2)\,. \end{aligned}$$

We verify that $x^4+x^3+x^2 = (x^3+x+1)(x+1)+1 = (x^2)(x^2+x+1)+0$ and $x^4+x^3+x^2 = (x)(x^3+x^2+1)+(x^2+x)$.

Next, the Extended Euclidean algorithm applied to $g_1\,g_2\,g_3 = x^6+x^5+x^2+1$ and $g_4 := x^4+x+1$ gives $(x^3)(x^6+x^5+x^2+1) + (x^5+x^4+x^2+x+1)(x^4+x+1) = 1$.

Table 3. Local variables when computing $\gcd(g_1\,g_2\,g_3, g_4)$

d_0	d_1	s_0	s_1	t_0	t_1	q
$x^6+x^5+x^2+1$	x^4+x+1	1	0	0	1	x^2+x
x^4+x+1	x^3+x^2+x+1	0	1	1	x^2+x	$x+1$
x^3+x^2+x+1	x	1	$x+1$	x^2+x	x^3+x+1	x^2+x+1
x	1	$x+1$	x^3	x^3+x+1	$x^5+x^4+x^2+x+1$	x
1	0	x^3		$x^5+x^4+x^2+x+1$		

Thus, the third iteration of the loop in the Effective Remainder Algorithm yields

$$
\begin{aligned}
&(x^3)(x^6+x^5+x^2+1)(x^2+x+1)+(x^5+x^4+x^2+x+1)(x^4+x+1)(x^4+x^3+x^2) \\
&= x^{13}+x^{11}+x^{10}+x^9+x^7+x^5+x^2 \\
&= (x^3+x^2)(x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2+x+1)+(x^9+x^7+x^5)\,.
\end{aligned}
$$

We verify that

$$
\begin{aligned}
x^9+x^7+x^5 &= (x^8+x^7+x^4+x^3+x^2+x+1)(x+1)+1 \\
&= (x^7+x^6+x^5)(x^2+x+1)+0 \\
&= (x^6+x^5+x^3+x^2+x)(x^3+x^2+1)+(x^2+x) \\
&= (x^5+x^3+x^2+1)(x^4+x+1)+(x^2+x+1)\,.
\end{aligned}
$$

□

Therefore, the desired polynomial in $\mathbb{F}_2[x]$ is $x^9+x^7+x^5$.