1. (DF7.5.2) Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).

Proof. Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication as given.

We check that the ring of fractions $D^{-1}R$ is a well defined ring, defining elements of this ring in the same way that the quotient field is defined, but with any D closed under multiplication.

If D contains $0 \in R$, then every element in $D^{-1}R$ is equal to the zero element, so that $D^{-1}R$ is the zero ring: For any fraction a/b and any nonzero $d \in D$, we have

$$\frac{a}{b} = \frac{0}{0} = \frac{0}{d},$$

since $a0 = b0 = 0d = 0$. Hence in this case we get the zero ring which is automatically a subring of the quotient field of R (also note that the zero ring is not an integral domain; perhaps the formulation of the problem was not meant to include this case). So suppose D does not contain zero (it also will not contain any zero divisors since R is an integral domain)

For fractions $a/b = a'/b'$ and $c/d = c'/d'$, we check that addition and multiplication is well defined. With $ab' = a'b$ and $cd' = c'd$, we have

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd'+b'c'}{b'd'} \qquad \frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{b'd'},$$

and we check that

$$adb'd' + bcb'd' = a'd'bd + b'c'bd \quad \text{and} \quad acb'd' = a'c'bd.$$

Observe that $adb'd' + bcb'd' = a'dbd' + bc'b'd = a'd'bd + b'c'bd$ and that $acb'd' = a'cbd' = a'c'bd$ as desired. Hence the operations of addition and multiplication are well defined.

Note the additive identity is $0/d$ for any $d \in D$ since $a/b + 0/d = ad/bd = a/b$, and the additive inverse of c/d is $-c/d$ since $c/d + -c/d = (cd-cd)/d^2 = 0/d$. We check that $D^{-1}R$ is closed under addition and closed under multiplication, and that these operations are commutative (since R is a commutative ring):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}, \text{ and } \frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in D^{-1}R,$$

and since $bd = db \in D$ as D is closed under multiplication, it follows that $D^{-1}R$ is closed under its operations. The multiplicative identity of $D^{-1}R$ is d/d for any $d \in D$, since $(a/b)(d/d) = ad/bd = a/b = da/db = (d/d)(a/b)$ (since $adb = bda$).

The multiplication and addition is associative because the multiplication in R is associative:

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$$

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+bde}{bdf}=\frac{a}{b}+\frac{cf+de}{df}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).$$

The multiplication also distributes:

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+de}{df}\right)=\frac{acf+ade}{bdf}=\frac{acfb+adeb}{b^2df}=\frac{ac}{bd}+\frac{ae}{bf}$$

$$\left(\frac{c}{d}+\frac{e}{f}\right)\frac{a}{b}=\left(\frac{cf+de}{df}\right)\frac{a}{b}=\frac{cfa+dea}{dfb}=\frac{cfab+deab}{dfb^2}=\frac{ca}{db}+\frac{ea}{fb}$$

It follows that $D^{-1}R$ is a commutative ring with identity.

To show that $D^{-1}R$ is isomorphic to a subring of the quotient field Q of R, we use the inclusion homomorphism $\iota\colon D^{-1}R \hookrightarrow Q$ which sends a/b to a/b, interpreting an element of D to also be an element of $R-\{0\}$ since we assumed in this case that D did not contain 0. This map is clearly injective, so by the first isomorphism theorem, $D^{-1}R$ is isomorphic to its image under ι, which is a subgroup of Q. □

2. (DF7.6.3) Let R and S be rings with identities. Prove that every ideal of $R\times S$ is of the form $I\times J$ where I is an ideal of R and J is an ideal of S.

Proof. Let A be an ideal of $R\times S$, and let I be the set of elements $r\in R$ such that for each $r\in I$ there exists an element $s\in S$ such that $(r,s)\in A$. Similarly, let J be the set of elements $s\in S$ such that for each $s\in J$, there exists an element $r\in R$ such that $(r,s)\in A$. Essentially, I and J are the sets which contain the elements which appear in the first and second components of elements of A, respectively. We show that these are ideals of R and S each, and show that A is isomorphic to $I\times J$.

Note since A is an ideal it contains an additive identity, which from the definition of the addition on $R\times S$ it follows that the additive identity is $(0_R,0_S)$, so that $0_R\in I$ and $0_S\in J$. Then let r,r' be elements of I. Then there exist $s,s'\in S$ such that $(r,s),(r',s')\in A$ and so since A is an ideal, we have for any $(a,b)\in R\times S$ (so $a\in R$ and $b\in S$) that

$$(r,s)-(r',s')=(r-r',s-s')\in A,\ \text{and}\ (r,s)(r',s')=(rr',ss')\in A$$

$$(a,b)(r,s)=(ar,bs)\in A,\ \text{and}\ (r,s)(a,b)=(ra,sb)\in A$$

so that I is closed under subtraction and multiplication and is a nonempty subset of R, and multiplication by elements of R on the right and left. It follows that I is an ideal of R. Similarly, let s,s' be elements of J, so that there exist $r,r'\in R$ such that $(r,s),(r',s')\in A$. Then for any $(a,b)\in R\times S$ we have

$$(r,s)-(r',s')=(r-r',s-s')\in A,\ \text{and}\ (r,s)(r',s')=(rr',ss')\in A$$

$$(a,b)(r,s)=(ar,bs)\in A,\ \text{and}\ (r,s)(a,b)=(ra,sb)\in A,$$

and it follows similarly that J is an ideal of S.

We show that $I\times J$ is an ideal of $R\times S$. It is clear that $I\times J$ is a subring of $R\times S$ since I,J are subrings of R,S respectively. Then for any $(r,s)\in R\times S$ and $(a,b)\in I\times J$ we have that $(r,s)(a,b)=(ra+sb)\in I\times J$

and $(a, b)(r, s) = (ar, bs) \in I \times J$ since I, J are ideals. Hence $I \times J$ is an ideal of $R \times S$. What remains is to show that $I \times J = S$.

An element of A is of the form (a, b), and automatically $a \in I$ and $b \in J$ since for $a \in R$, we have that b is an element of S such that $(a, b) \in A$, and similarly for $b \in S$, we have that a is an element of R such that $(a, b) \in A$. Hence $(a, b) \in I \times J$ so that $A \subseteq I \times J$. Then any element (r, s) of $I \times J$ can be decomposed into $(r, 0_S) + (0_R, s)$, and since there are elements $s' \in S$ and $r' \in R$ such that $(r, s'), (r', s) \in A$. But since R, S have identities, we can write (r, s) as $(1_r, 0_S)(r, s') + (0_R, 1_S)(r', s)$, and this combination is in A since A is an ideal of $R \times S$. Hence $I \times J \subseteq A$, so that $A = I \times J$.

Since A was an arbitrary ideal of $R \times S$, it follows that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S. $\square$

3. (DF8.1.7) Find a generator for the ideal $(85, 1 + 13i)$ in $\mathbb{Z}[i]$, i.e., a greatest common divisor for 85 and $1 + 13i$, by the Euclidean Algorithm. Do the same for the ideal $(47 - 13i, 53 + 56i)$.

Generators of these ideals are greatest common divisors of the two numbers which generate the ideal. To find a greatest common divisor, we use the Euclidean algorithm. In each division we will choose the quotient to be any closest (with respect to the standard $\mathbb{C}$ Euclidean metric) element of $\mathbb{Z}[i]$ viewed as an element of $\mathbb{C}$ to the quotient computed in $\mathbb{Q}[i]$ viewed as an element of $\mathbb{C}$. That is, given elements $a, b \in \mathbb{Z}[i]$, we compute the quotient $q = a + bi$ in $\mathbb{Q}[i]$, and round a, b to the nearest integer to obtain a quotient q' in $\mathbb{Z}[i]$ (this is the algorithm suggested by the text). Starting with $N(85) = 85^2 > N(1 + 13i) = 1^2 + 13^2$ and $N(53 + 56i) = 53^2 + 56^2 > N(47 - 13i) = 47^2 + 13^2$, we have:

$$(85) = (1 - 7i)(1 + 13i) + \boxed{(-7 - 6i)} \qquad \begin{cases} \frac{85}{1+13i} = \frac{1}{2} + \frac{-13}{2}i \approx 1 - 7i \\ (85) - (1 - 7i)(1 + 13i) = (-7 - 6i) \end{cases}$$

$$(1 + 13i) = (-1 - i)(-7 - 6i) + (0) \qquad \begin{cases} \frac{1+13i}{-7-6i} = -1 - i \\ \text{no remainder} \end{cases}$$

and

$$(53 + 56i) = (1 + 1i)(47 - 13i) + (-7 + 22i) \qquad \begin{cases} \frac{53+56i}{47-13i} = \frac{43}{58} + \frac{81}{58}i \approx 1 + 1i \\ (53 + 56i) - (1 + 1i)(47 - 13i) = (-7 + 22i) \end{cases}$$

$$(47 - 13i) = (-1 - 2i)(-7 + 22i) + \boxed{(-4 - 5i)} \qquad \begin{cases} \frac{47-13i}{-7+22i} = \frac{-15}{13} + \frac{-23}{13}i \approx -1 - 2i \\ (47 - 13i) - (-1 - 2i)(-7 + 22i) = (-4 - 5i) \end{cases}$$

$$(-7 + 22i) = (-2 - 3i)(-4 - 5i) + (0) \qquad \begin{cases} \frac{-7+22i}{-4-5i} = -2 - 3i \\ \text{no remainder.} \end{cases}$$

A greatest common factor can be multiplied by a unit to obtain another greatest common factor, so multiply the remainders $-7-6i$ and $-4-5i$ by -1 to find that $(85, 1+13i) = (7+6i)$ and $(47-13i, 53+56i) = (4+5i)$.

4. (DF8.1.8) Let $F = \mathbb{Q}[\sqrt{D}]$ be a quadratic field with associated quadratic integer ring $\mathcal{O}$ and field norm N as in section 7.1.

   (a) Suppose D is $-1, -2, -3, -7$, or -11. Prove that $\mathcal{O}$ is a Euclidean Domain with respect to N. [Modify the proof for $\mathbb{Z}[i]$ $(D = -1)$ in the text. For $D = -3, -7, -11$ prove that every element of F differs from an element in $\mathcal{O}$ by an element whose norm is at most $(1 + |D|)^2/(16|D|)$, which is less than 1 for these values of D. Plotting the points of $\mathcal{O}$ in $\mathbb{C}$ may be helpful.]

   Proof. Note the field norm on F is a norm when $D < 0$, so we omit taking the absolute value of the field norms henceforth.

   For $D = -1, -2$ ($D \not\equiv 1 \mod 4$): Let $A = a + b\sqrt{D}$ and $B = c + d\sqrt{D}$ be any two elements of $\mathbb{Z}[\sqrt{D}]$ with $B \neq 0$. Then in $\mathbb{Q}[\sqrt{D}]$, the quotient A/B is given by $r + s\sqrt{D}$ for some rational numbers r, s; in particular $r = (ac - bdD)/(c^2 - d^2D)$ and $s = (bc - ad)/(c^2 - d^2D)$. Then round r to the nearest integer p and round s to the nearest integer q so that $|r - p|, |s - q|$ are at most $1/2$.

   We take the quotient A/B in $\mathbb{Z}[\sqrt{D}]$ to be $p + q\sqrt{D}$. The remainder we choose is given by $A - (p + q\sqrt{D})B = \theta B$ (and θB is computed in $\mathbb{Q}[\sqrt{D}]$), where $\theta = (r - p) + (s - q)\sqrt{D}$. This ensures that the remainder θB is also an element of $\mathbb{Z}[\sqrt{D}]$, and since D is equal to -1 or -2, it follows that

$$N(\theta B) = N(\theta)N(B) = [(r-p)^2 - (s-q)^2 D]N(B) \leq [1/4 + 2/4]N(B) = (3/4)N(B).$$

   Hence there is a division algorithm for $\mathbb{Z}[\sqrt{D}]$, meaning it is a Euclidean Domain.

   For $D = -3, -7, -11$ ($D \equiv 1 \mod 4$): Let $A = a + b[(1+\sqrt{D})/2]$ and $B = c + d[(1+\sqrt{D})/2]$ be any two elements of $\mathbb{Z}[(1+\sqrt{D})/2]$ with $B \neq 0$. Then in $\mathbb{Q}[\sqrt{D}]$, the quotient A/B is given by $r + s\sqrt{D}$ for some rational numbers r, s; in particular $r = [(a + b/2)(c + d/2) - (b/2)(d/2)D]/[(c + d/2)^2 - (d/2)^2 D]$ and $s = [(b/2)(c + d/2) - (a + b/2)(d/2)]/[(c + d/2)^2 - (d/2)^2 D]$. We first rewrite $r + s\sqrt{D}$ into its "cartesian" form (we are changing coordinates in $\mathbb{C}$). There exist rational numbers n, m such that $r + s\sqrt{D} = (n + m/2) + (m/2)\sqrt{D}$; that is, $m = 2s$ and $n = r - s$.

   We round in a particular order: First round $m = 2s$ to the nearest integer q, so that $|2s - q| \leq 1/2$. Then round the rational number $r - q/2$ to the nearest integer p so that $|r - p - q/2| \leq 1/2$. The motivation for this rounding comes from finding the closest element of $\mathbb{Z}[(1+\sqrt{D})/2]$ to any element u of $\mathbb{Q}[\sqrt{D}]$ by geometric means. Embedding $\mathbb{Z}[(1+\sqrt{D})/2]$ in $\mathbb{C}$ yields a lattice of points arranged in a manner such that $\mathbb{C}$ is tiled by parallelograms whose vertices are elements of $\mathbb{Z}[(1+\sqrt{D})/2]$. The parallelograms give a change of basis for $\mathbb{C}$ which is essentially given by basis vectors parallel to the sides of the parallelograms tiling $\mathbb{C}$. Slide u "vertically" along a line parallel to the slanted edge of the parallelograms until it hits the closest horizontal side edge of the parallelogram u was found in. This represents the first rounding to obtain q. Then slide the point horizontally to the closest element of $\mathbb{Z}[(1+\sqrt{D})/2]$ lying on the same line as it; this corresponds to the rounding used to obtain p. Graphically this might look like:

Then take the quotient to be $p+q[(1+\sqrt{D})/2]$, and the remainder to be $A-(p+q[(1+\sqrt{D})/2])B = \theta B$ (note that it follows that this remainder is in $\mathbb{Z}[(1+\sqrt{D})/2]$), where $\theta = (r-p-q/2)+(s-q/2)\sqrt{D}$. Then we have

$$\begin{aligned} N(\theta B) = N(\theta)N(B) &= [(r-p-q/2)^2 - (s-q/2)^2 D]N(B) \\ &= [(r-p-q/2)^2 - (2s-q)^2 D/4]N(B) \\ &\leq [1/4 - D/16]N(B) \\ &= [(4-D)/16]N(B) \\ &\leq (15/16)N(B) < N(B), \end{aligned}$$

and the final inequalities follow since D takes on the values $-3,-7,-11$. Thus we have chosen an appropriate quotient and remainder such that $\mathbb{Z}[(1+\sqrt{D})/2]$ has a division algorithm; that is, it is a Euclidean Domain.

Thus for $D=-1,-2,-3,-7$, or -11, the associated quadratic integer ring $\mathcal{O}$ of the quadratic field $F=\mathbb{Q}[\sqrt{D}]$ is a Euclidean Domain with respect to the field norm N. $\square$

(b) Suppose that $D=-43,-67$, or -163. Prove that $\mathcal{O}$ is not a Euclidean Domain with respect to any norm. [Apply the same proof as for $D=-19$ in the text.]

Proof. Let $\omega = [(1+\sqrt{D})]/2$. Previously in the text it was determined that the only units of $\mathcal{O}$ for $D<-3$ were ± 1 (since if the field norm of $a+b\omega$ was 1, then we sought to choose integers a,b satisfying $(2a+b)^2+|D|b^2=4$; it follows that $b=0$, so that $a=\pm 1$, so that the units are ± 1.) Hence $\widetilde{\mathcal{O}} = \{0,\pm 1\}$. Suppose that u is a universal side divisor in $\mathcal{O}$. Observe that for any element $a+b\omega$, its field norm $a^2+ab+[(1-D)/4]b^2 = (a+b/2)^2+(|D|/4)b^2 \geq (1-D)/4$ whenever $b\neq 0$. So the smallest values for the field norm on $\mathcal{O}$ are attained whenever $b=0$. They are, in cases:

$D=-43$, so $(1-D)/4=11$: Smallest norms are $1,4,9$.

$D=-67$, so $(1-D)/4=17$: Smallest norms are $1,4,9,16$.

$D=-163$, so $(1-D)/4=41$: Smallest norms are $1,4,9,16,25,36$.

For the first case when $D = -43$, let x take on $2, 3$ (x need not take on 1 since 1 is a unit). It follows that u should divide one of 2 or 3, and that u should divide one of 3 or 4 (the value $3 - 1 = 2$ will be handled in the first computation anyways). But observe that if $2 = ab$, then $N(2) = 4 = N(a)N(b)$ so that the only non-unit divisors of 2 are $\{\pm 2\}$. Similarly, if $3 = ab$, since 3 is not a possible norm value, we have that $N(3) = 9 = N(a)N(b)$. Hence the only non-unit divisors of 3 are $\{\pm 3\}$. Again in a similar fashion, observing that 2 and 8 are not possible values the norm takes on, the only non-unit factors of 4 are $\{\pm 2, \pm 4\}$. So u can only take on values in $\{\pm 2, \pm 3, \pm 4\}$. But observe that if $x = \omega = (1 + \sqrt{-43})/2$, none of the possible values for u divide $\omega, \omega \pm 1$ since the quotient computed in the quadratic field would not contain integer coefficents anyways.

For the second case when $D = -67$, repeat the above argument for $x = 2, 3$, and additionally for $x = 4$. So u has to either divide 4 or 5; if $5 = ab$ then $N(5) = 25 = N(a)N(b)$ yields that only ± 5 are the only non-unit divisors of 5. Still we find that any values in $\{\pm 2. \pm 3, \pm 4, \pm 5\}$ do not divide ω in this case.

For the last case when $D = -163$ an additional two more values of x must be considered: $x = 5, 6$ so that we must find non-unit factors of $6, 7$: if $6 = ab$ then $36 = N(a)N(b)$, and note that $2, 3, 12, 18$ are not norms so that the only additional values that u may take on is ± 6. Similarly, 49 is a square of a prime so that the only additional values that u may take on is ± 7. And once again with $x = \omega$, none of the values in $\{\pm n \mid 2 \leq n \leq 7\}$ divide ω.

In all cases, any of the restrictions to the values that any universal divisor could take on were all nullified by the incapability of dividing ω, so there are no universal side divisors in each case. Hence ω is not a Euclidean Domain. $\square$