Assignment 2 – Solutions

Because of the length of the assignment we mainly give ideas of the proofs and leave out many computations that we've done earlier before in the same or a similar way. Of course no proof is unique, there are always many ways to prove a claim. Therefore all the solutions are only suggestions.

Chapter 3

3)a) Consider $u = a + \sqrt{10}b$ and $v = c + \sqrt{10}d$. Then verify by computation that

$$N(uv) = N\left(ac + 10bd + \sqrt{10}(ad + bc)\right) = \ldots = N(u) \cdot N(v).$$

If $u = 0$ then clearly $N(u) = 0$. So suppose now $N(u) = 0$.

$$N(u) = 0 \Rightarrow a^2 - 10b^2 = 0 \Rightarrow a^2 = 10b^2 \tag{1}$$

We know that for all $w \in R$ we have

$$N(u) \cdot N(w) = 0.$$

So verify for $w = 1 + \sqrt{10}$:

$$N(uw) = -18b(10b - a),$$

using (1).

If $u \neq 0$, then clearly $b \neq 0$, so we know that the second factor has to equal zero and we can conclude:

$$\begin{aligned} 10b - a = 0 \quad &\Rightarrow \quad a = 10b \\ &\Rightarrow \quad a^2 = 100b^2 \\ &\Rightarrow \quad 10b^2 = 100b^2 \\ &\Rightarrow \quad b = 0, \end{aligned}$$

again using (1). But this is a contradiction, so $u = 0$.

b) Claim: u unit in $R \Leftrightarrow N(u) = \pm 1$.
proof:

"$\Rightarrow$" : Let u be unit in R. Then there exists a $v \in R$ such that $uv = 1$. Because of the multiplicity of N we have

$$1 = N(1)\,N(uv) = N(u)\,N(v).$$

So $N(u)$ is a unit in $\mathbb{Z}$ and therefore the claim holds, as the only units in $\mathbb{Z}$ are 1 and -1.

"$\Leftarrow$" : Suppose $N(u) = \pm 1$. We need to find a $v \in R$ with $uv = 1$.
Claim: $v = N(u) \cdot \left(a - \sqrt{10}b\right)$ does it.
Proof: $v \in R$, as $N(u) = \pm 1$ and $a, b \in \mathbb{Z}$. Furthermore we have

$$\begin{aligned} u \cdot v &= \left(a + b\sqrt{10}\right) \cdot N(u) \cdot \left(a - b\sqrt{10}\right) \\ &= N(u) \cdot N(u) = 1. \end{aligned}$$

□

c) Suppose $u = a \cdot b$. Then clearly $N(u) = N(a) \cdot N(b)$.

$\underline{u = 2}$: We have $N(u) = 4$. So $N(a)$ is either $-1, 1, -2$ or 2. We have to show that ± 2 is impossible.
Consider $a = x + y\sqrt{10}$ and suppose

$$N(a) = x^2 - 10y^2 = \pm 2.$$

If we find a solution in $\mathbb{Z}$, then we have a solution in any $\mathbb{Z}_n$, because we have the natural ring-homomorphism between both rings.

Consider $\mathbb{Z}_5$. The equation simplifies to $x^2 = \pm 2$, which means $x^2 = 2$ or $x^2 = 3$. A quick check verifies that there are no elements in $\mathbb{Z}_5$ that satisfy either of the equations. So we know that there is no $a \in R$ with $N(a) = \pm 2$. Therefore any a in a factorisation of 2 has an N–value of ± 1 and thus is a unit. So 2 is irreducible in R.

$\underline{u = 3}$: Same proof. Observe that ± 3 in $\mathbb{Z}_n$ is 3 or 2.

$\underline{u = 4 + \sqrt{10}}$: In this case $N(u) = 6$. So any a in a non–trivial factorisation of u has an N–value of ± 2 or ± 3. But as shown above this is not possible. So $4 + \sqrt{10}$ is irreducible.

$\underline{u = 4 - \sqrt{10}}$: The same.

d) Just compare the N–values of the four elements:

$$\begin{aligned} N(2) &= 4 & N\left(4 + \sqrt{10}\right) &= 6 \\ N(3) &= 9 & N\left(4 - \sqrt{10}\right) &= 6 \end{aligned}$$

As no N–value on the let hand side divides any on the right hand side (and vice versa), none of the four elements in R divides another. Therefore none of these elements are prime elements.

4) Consider $u \neq 0$ and suppose we cannot factorise it into irreducibles. That means that in any factorisation $u = v_1 \cdot v_2$ both the factors are reducible. We can therefore factorise both of them, and again every factor is reducible. We can do this as often as we want. Let us do this until we have $k \geq |N(u)|$ factors. So

$$u = \prod_{i=1}^{k} v_i.$$

As each of the factors is reducible and thus not a unit, its N–value is greater than 1 or smaller than -1. Therefore we have

$$|N(u)| = \prod_{i=1}^{k} \underbrace{|N(v_i)|}_{>1} > |N(u)|.$$

This is of course a contradiction, and therefore we cannot factorise u into as many reducible factors as we want. So u must have a factorisation into (finitely many) irreducibles.

This factorisation need not be unique, as seen in problem 3)d). The element 6 has two factorisations, where the factors are not associates of each other.

5)a) Let $P = (a)$ and a uniquely factorised into $a = p_1 \cdots p_n$. (Theorem 3.7)
Claim: $(a) = (p_1)(p_2) \cdots (p_n) =: P'$
Proof: Clearly $(a) \subseteq P'$ as $a \in P'$.
"$\supseteq$": Let $b \in P'$. Then (for some $m \in \mathbb{N}$):

$$\begin{aligned} b &= \sum_{j=1} m x_{1j} p_1 \cdot x_{2j} p_2 \cdots x_{nj} p_n \\ &= \left(\sum_{j=1}^{m} x_{1j} \cdots x_{nj} \right) p_1 \cdots p_n \\ &= \left(\sum_{j=1}^{m} x_{1j} \cdots x_{nj} \right) a \qquad \in (a). \end{aligned}$$

As p_i are irreducible, all (p_i) are maximal ideals.

b) P primary $\Leftrightarrow$ $P = (p^n)$ for some $p \in R$, p prime or $p = 0$, and some n.

"$\Rightarrow$" : Let $P = (q)$ be primary. So if $ab \in P$ and $a \notin P$, then $b^m \in P$ for some m.

Case 1: $q \neq 0$. Suppose $q \neq p^n$ for all p, p prime. So we have a factorisation of q into at least two prime factors:

$$q = \prod_{i=1}^{k} p_i^{j_i},$$

p_i prime, $p_i \neq p_j$ for $i \neq j$.
Let $a = p_1^{j_1}$ and $b = \prod_{i=2}^{k} p_i^{j_i}$. Then $q = ab$, so $ab \in P$. But $a \notin P$, so $b^m \in P$ for some m. But this is impossible, as p_1 is not a factor of b^m. So we have a contradiction and $q = p^n$ for some prime element p and some integer n.
Case 2: $q = 0$. If $ab \in (q)$, $a \notin (q)$, then $b = 0$. So $b^1 \in (q)$.

"$\Leftarrow$" : Let $p = 0$. Then $P = (0)$ and P is primary (see Case 2 of above).
Let $P = (p^n)$, $p \neq 0$, p irreducible. Suppose $ab \in P$, $a \notin P$.
Then $ab = rp^n$ for some $r \in R$. So $p^n | ab$. But $p^n \not| a$, so $p|b$ and $p|b^n$.

c) "$\subseteq$" : Suppose $q \in P_1 \cdots P_n$. Then $q = r \cdot p_1^{n_1} \cdots p_n^{n_n}$.
Clearly $p_i^{n_i} | q \ \forall\, i$, so $q \in P_i \ \forall\, i$ and thus $q \in P_1 \cap \ldots \cap P_n$.

"$\supseteq$" : Suppose $q \in P_1 \cap \ldots \cap P_n$. Then $q \in P_i \ \forall\, i$. Therefore $p_i^{n_i} | q \ \forall\, i$. As the p_i are distinct, we have

$$q = r \cdot p_1^{n_1} \cdots p_n^{n_n} \in P_1 \cdots P_n.$$

d) Let $P = (q)$. We know q has a unique factorisation (up to order and associativity). Let

$$q = \prod_{i=1}^{n} p_i^{n_i}.$$

Then $(p_i^{n_i})$ are primary. We therefore have because of c):

$$P = (p_1^{n_1}) \cdots (p_n^{n_n}) = (p_1^{n_1}) \cap \ldots \cap (p_n^{n_n}).$$

Note that associated elements in two factorisations generate the same ideal. So we have uniqueness up to order.

6)a) We know $\mathbb{Z}$ is Euclidean, so we have $a = qn + r$ for some $q, r \in \mathbb{Z}$. Let $r > \left|\frac{n}{2}\right|$.
Case 1: $r > 0$, $n > 0$. Consider $q' := q + 1$, $r' := r - n$. Then

$$q'n + r' = (q+1)\, n + r - n = qn + r = a.$$

and $|r'| \leq \frac{n}{2}$.

Cases 2,3 and 4 similarly.

b) To show that the Gaussian Integers form a Euclidean Domain we show that Definition 3.8 holds.

3.8(i) : Let $x, y \in \mathbb{Z}[i] =: R$, and $x = a + bi$, $y = c + di$. Then

$$\begin{aligned}
\varphi(xy) &= \varphi(ac - bd + i(ad + bc)) \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\
&= a^2\left(c^2 + d^2\right) + b^2\left(c^2 + d^2\right) \\
&= \left(a^2 + b^2\right)\left(c^2 + d^2\right) \\
&= \varphi(x)\underbrace{\varphi(y)}_{\geq 1} \quad \geq \quad \varphi(x).
\end{aligned}$$

3.8(ii) : To prove this part of the definiton we just follow the hint given in the book. There is nothing more to be done.
Let $x, y \in R$, $x \neq 0$. Show: There exist $q, r \in R$, such that $y = qx + r$ with $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(x)$. Case 1: $x \in \mathbb{N}$. Suppose $y = a + bi$.
From part a) we know that there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $a = q_1x + r_1$, $b = q_2x + r_2$ and $|r_1| \leq \frac{x}{2}$, $|r_2| \leq \frac{x}{2}$.
Put $q := q_1 + q_2i$ and $r := r_1 + r_2i$.
Claim: y = qx+r.
Proof:

$$\begin{aligned}
qx + r &= (q_1 + q_2i)x + r_1 + r_2i \\
&= q_1x + r_1 + (q_2x + r_2)i \\
&= a + bi = y.
\end{aligned}$$

Furthermore either $r = 0$ or

$$\begin{aligned}
\varphi(r) &= \varphi(r_1 + r_2i) = r_1^2 + r_2^2 \\
&\leq \left(\frac{x}{2}\right)^2 + \left(\frac{x}{2}\right)^2 = \frac{x^2}{2} < \varphi(x) = x^2.
\end{aligned}$$

Case 2: $x \in \mathbb{Z}[i]$. Let $x = c + di$.
Then $x\bar{x} > 0$, with $\bar{x} = c - di$, so $x\bar{x} = c^2 + d^2$.
There are $q, r_0 \in \mathbb{Z}$ such that $y\bar{x} = q(x\bar{x}) + r_0$. This is a direct application of Case 1.
Put $r = y - qx$.
Claim: y = qx +r.
Proof: $qx + r = qx + r = qx + y - qx = y$.

Claim: $r = 0$ or $\varphi(r) < \varphi(x)$.
Proof: Let $r \neq 0$. Then $y - qx \neq 0$.
$\varphi(r) = \varphi(y - qx)$.

$$\begin{aligned} \varphi(r)\,\varphi(\bar{x}) &= \varphi(r\bar{x}) = \varphi((y - qx)\,\bar{x}) \\ &= \varphi(y\bar{x} - q(x\bar{x})) = \varphi(r_0) < \varphi(x\bar{x}) = \varphi(x)\,\varphi(\bar{x}). \end{aligned}$$

So $\varphi(r) < \varphi(x)$.

8) This solution is rather long and can be looked up in
Dumit & Foote, "Abstract Algebra", pages 282f for PID and pages 277f for not Euclidean.

Chapter 4

6) We know: $\forall\, I \lhd R : S^{-1}I \lhd S^{-1}R$.
And $\forall\, I \lhd S^{-1}R$ and $J = \varphi_S^{-1}(I) : J \lhd R$ and $I = S^{-1}J$.
So let $J \lhd S^{-1}R$ be an ideal and $I = \varphi_S^{-1}(J)$.
Then of course $I = (a)$ for some $a \in R$.

$$\begin{aligned} \Rightarrow J &= S^{-1}I = \left\{ \frac{ra}{s} \;\middle|\; r \in R, s \in S \right\} \\ &= \left\{ \frac{r}{a} \cdot a \;\middle|\; r \in R, s \in S \right\} \\ &= \left\{ ta \;\middle|\; t \in S^{-1}R \right\} \\ &= (a) \quad (\text{in } S^{-1}R). \end{aligned}$$

9) S be a multiplicative subset of the commutative ring R with identity. Recall:

$$\operatorname{Rad} I = \left\{ r \in R \;\middle|\; r^n \in I \text{ for some } n \right\}$$

So accordingly

$$\operatorname{Rad}\left(S^{-1}I\right) = \left\{ \frac{r}{s} \in S^{-1}R \;\middle|\; \left(\frac{r}{s}\right)^n = \frac{r^n}{s^n} \in S^{-1}I \text{ for some } n \right\}.$$

"$\subseteq$": Let $\frac{r}{s} \in S^{-1}(\operatorname{Rad} I)$. So we have $r \in \operatorname{Rad} I$ and $r^n \in I$. Then we have immediately that

$$\left(\frac{r}{s}\right)^n = \frac{r^n}{s^n} \in S^{-1}I,$$

because $r^n \in I$ and $s^n \in S$. Therefore $\frac{r}{s} \in \operatorname{Rad}(S^{-1}I)$ and thus

$$S^{-1}(\operatorname{Rad} I) \subseteq \operatorname{Rad}\left(S^{-1}I\right).$$

"$\supseteq$": Let $\frac{r}{s} \in \operatorname{Rad}(S^{-1}I)$. Then there exists an n such that $\left(\frac{r}{s}\right) = \frac{r^n}{s^n} \in S^{-1}I$.
Let $\frac{r^n}{s^n} = \frac{q}{t}$ with $q \in I$ and $t \in S$. So there exists an $u \in S$ such that

$$u\left(r^n t - q s^n\right) = 0_R.$$

Then we have

$$u r^n t = u q s^n \Rightarrow u^n r^n t^n = u^n q s^n t^{n-1} \in I,$$

as $a \in I$ and $I \lhd R$. The left hand side of the last equation equals $(urt)^n$ and so we have that $urt \in \operatorname{Rad} I$. As $u, t \in S$ we also have that $ut \in S$ and because of the commutativity:

$$\frac{r}{s} = \frac{urt}{ust} \in S^{-1}\left(\operatorname{Rad} I\right),$$

because $urt \in \operatorname{Rad} I$ and $ust \in S$. This proves the other inclusion and thus the two sets are equal.

15) We denote the set of all nilpotent elements in R with $\mathcal{N}(R)$. Observe that $\mathcal{N}(R)$ is an ideal in R.

"i) $\Rightarrow$ ii)": Clearly if R has a unique prime ideal then this ideal is exactly $\mathcal{N}(R)$.
Let $x \in R$ be a non–unit. Then there exists a maximal ideal M such that $x \in M$. As any maximal ideal is prime we have that $M = \mathcal{N}(R)$. This implies that x is nilpotent.

"ii) $\Rightarrow$ iii)": As $\mathcal{N}(R)$ contains all non–units it is maximal and thus prime. Note that every element of $\mathcal{N}(R)$ is a zero–divisor and that all units are not. So $\mathcal{N}(R)$ contains all zero–divisors and all non–units.

"iii) $\Rightarrow$ i)": Let P the minimal prime ideal that contains all non–units. Then it is of course maximal, as every element that could be added is a unit, and thus the larger ideal would be equal to R. So R has a unique prime ideal.

□