MATH7421 Solutions Week 4

Primes, Irreducibles and Unique Factoristion

1. If $p|a$ then we are finished. Assume that $p \nmid a$. Then $\gcd(p,a) = 1$ (since p is prime). By Euclid's Algorithm we may find $s, t \in \mathbb{Z}$ such that $sp + ta = \gcd(p,a) = 1$. Multiplying by b gives $spb + tab = b$. Since $p|ab$ we have that the LHS is divisible by p, so that $p|b$ follows.

2. Suppose that π is reducible. Then there exists a non-trivial factorisation $\pi = \alpha\beta$, for two non-zero non-units. Since π is prime we must have that $\pi|\alpha$ or $\pi|\beta$. We can swap α and β so that $\pi|\alpha$ is true.

   We now have that $\alpha = \gamma\pi$ for some $\gamma \in R$. We now learn that $\pi = (\gamma\pi)\beta$, so that $\pi(1-\gamma\beta) = 0$. Since R is an integral domain we either have that $\pi = 0$ or $\gamma\beta = 1$. The first possibility cannot happen (since $\pi \neq 0$ by assumption) and the second gives the contradiction $\beta \in R^\times$ (i.e. it would give a trivial factorisation of π). This proves that π must be irreducible.

3. Suppose that $\alpha = \beta\gamma$ for two non-zero non-units $\beta \in \mathcal{O}_K$ and $\gamma \in \mathcal{O}_K$. Taking norms gives $p = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Since $N(\beta) \in \mathbb{Z}$ and $N(\gamma) \in \mathbb{Z}$ and p is prime, we must have that $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$. We can swap β and γ so that $N(\beta) = \pm 1$.

   Let $\sigma_1, \sigma_2, ..., \sigma_d$ be the embeddings $K \hookrightarrow \mathbb{C}$. By a similar argument to Exercise 12 of Week 3 we have that $N(\beta) = \prod_i \sigma_i(\beta) = \beta x = \pm 1$ with $x = \sigma_2(\beta)\sigma_3(\beta)...\sigma_d(\beta) \in \mathcal{O}_K$. This implies that $\beta \in \mathcal{O}_K^\times$ is a unit, since it has multiplicative inverse $\pm x$. This contradicts the above assumption (that the factorisation of α is non-trivial).

4. We have that $14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$ are two inequivalent factorisations of 14. This will follow if we can prove that each factor is irreducible (since the units of this ring are $\mathbb{Z}[\sqrt{-10}]^\times = \{\pm 1\}$, and clearly there is no way to reorder the terms in the second factorisation to be unit multiples of the terms in the first factorisation).

   Note that 2 is irreducible since if $2 = \alpha\beta$ is a non-trivial factorisation then $4 = N(2) = N(\alpha)N(\beta)$. If $N(\alpha) = 1$ or $N(\beta) = 1$ then one of α or β is a unit (since the solutions to $N(x + y\sqrt{-10}) = x^2 + 10y^2 = 1$ are $(x, y) = (\pm 1, 0)$, which correspond to the units ± 1). So we must have that $N(\alpha) = N(\beta) = 2$. However, such elements don't exist, as there are no integer solutions to $x^2 + 10y^2 = 2$.

   Note that 7 is irreducible since if $7 = \alpha\beta$ is a non-trivial factorisation then $49 = N(7) = N(\alpha)N(\beta)$. Again, we cannot have that $N(\alpha) = 1$ or $N(\beta) = 1$, so we must have $N(\alpha) = N(\beta) = 7$. Such elements do not exist since there are no integer solutions to $x^2 + 10y^2 = 7$.

Note that $2 \pm \sqrt{-10}$ are both irreducible, since if $2 \pm \sqrt{-10} = \alpha\beta$ then $14 = N(\alpha)N(\beta)$. Again, we cannot have that $N(\alpha) = 1$ or $N(\beta) = 1$ and so we must have $N(\alpha) \in \{2, 7\}$. We have shown that both are impossible above.

This shows that all of the factors are irreducible, so that both factorisations are inequivalent. Hence $\mathbb{Z}[\sqrt{-10}]$ is not a UFD.

5. The point here is that $5 = (1 + 2i)(1 - 2i)$ and $13 = (3 + 2i)(3 - 2i)$ are not irreducible in $\mathbb{Z}[i]$. Multiplying the irreducibles in a different order gives the two different (but equivalent) factorisations:

$$\begin{aligned}65 = 5 \cdot 13 &= [(1 + 2i)(1 - 2i)][(3 + 2i)(3 - 2i)] \\ &= [(1 + 2i)(3 + 2i)][(1 - 2i)(3 - 2i)] = (-1 + 8i)(-1 - 8i).\end{aligned}$$

Euclidean Domains

6. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ and $\beta \neq 0$. We wish to find $q, r \in \mathbb{Z}[\sqrt{2}]$ with $\alpha = q\beta + r$ and $r = 0$ or $0 \leq |N(r)| \leq |N(\beta)|$.

   Consider $\frac{\alpha}{\beta} = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. We can round off the coefficients to produce $q = \lfloor a \rceil + \lfloor b \rceil \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and consider the remainder $r = \alpha - q\beta \in \mathbb{Z}[\sqrt{2}]$. We then have that $\alpha = q\beta + r$ by construction, and so it suffices to show that $r = 0$ or $0 \leq |N(r)| < |N(\beta)|$.

   If $r = 0$ then we are done. Otherwise:

$$\begin{aligned}\left|N\left(\frac{r}{\beta}\right)\right| = \left|N\left(\frac{\alpha - q\beta}{\beta}\right)\right| = \left|N\left(\frac{\alpha}{\beta} - q\right)\right| &= |N((a - \lfloor a \rceil) + (b - \lfloor b \rceil)\sqrt{2})| \\ &= |(a - \lfloor a \rceil)^2 - 2(b - \lfloor b \rceil)| \\ &\leq (a - \lfloor a \rceil)^2 + 2(b - \lfloor b \rceil)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 \\ &= \frac{3}{4}.\end{aligned}$$

   It follows that $0 \leq \left|N\left(\frac{r}{\beta}\right)\right| \leq \frac{3}{4}$, so that by multiplicativity of the norm we have $0 \leq |N(r)| \leq \frac{3}{4}|N(\beta)| < |N(\beta)|$, as required.

7. Let $\alpha, \beta \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $\beta \neq 0$. We wish to find $q, r \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ with $\alpha = q\beta + r$ and $r = 0$ or $0 \leq N(r) \leq N(\beta)$.

   Consider $\frac{\alpha}{\beta} = a + b\left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Q}(\sqrt{-3})$. We can round off the coefficients to produce $q = \lfloor a \rceil + \lfloor b \rceil \left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and consider the remainder $r = \alpha - q\beta \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. We then have that $\alpha = q\beta + r$ by construction, and so it suffices to show that $r = 0$ or $0 \leq |N(r)| < |N(\beta)|$.

If $r = 0$ then we are done. Otherwise:

$$\begin{aligned}
N\left(\frac{r}{\beta}\right) = N\left(\frac{\alpha - q\beta}{\beta}\right) = N\left(\frac{\alpha}{\beta} - q\right) &= N\left((a - \lfloor a \rceil) + (b - \lfloor b \rceil)\left(\frac{1+\sqrt{-3}}{2}\right)\right) \\
&= (a - \lfloor a \rceil)^2 + (a - \lfloor a \rceil)(b - \lfloor b \rceil) + (b - \lfloor b \rceil)^2 \\
&\le \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \\
&= \frac{3}{4}
\end{aligned}$$

It follows that $0 \le N\left(\frac{r}{\beta}\right) \le \frac{3}{4}$, so that by multiplicativity of the norm we have $0 \le N(r) \le \frac{3}{4}N(\beta) < N(\beta)$, as required.

8. Let $\alpha = 3$ and $\beta = 1+\sqrt{-5}$ and suppose that $q, r \in \mathbb{Z}[\sqrt{-5}]$ are such that $3 = q(1+\sqrt{-5})+r$. Letting $q = x + y\sqrt{-5}$ we see that:

$$\begin{aligned}
N(x, y) &:= N(3 - (x + y\sqrt{-5})(1 + \sqrt{-5})) \\
&= N((3 - x + 5y) - (x + y)\sqrt{-5}) \\
&= (3 - x + 5y)^2 + 5(x + y)^2.
\end{aligned}$$

If $|x + y| \ge 2$ then clearly $N(x, y) > 6$. If $x + y = 0$ then $N(x, y) = (3 + 6y)^2 \ge 9 > 6$. If $x + y = \pm 1$ then $N(x, y) = (3 \pm 1 + 6y)^2 + 5 \ge 9 > 6$.

In either case we are unable to find $(x, y) \in \mathbb{Z}^2$ such that $N(x, y) < N(\beta) = 6$. Thus $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Domain with respect to the norm function.

9. Let $\alpha = \frac{1+\sqrt{-19}}{2}$ and $\beta = 2$ and suppose that $q, r \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ are such that $\frac{1+\sqrt{-19}}{2} = 2q+r$. Letting $q = x + y\left(\frac{1+\sqrt{-19}}{2}\right)$ we see that:

$$\begin{aligned}
N(x, y) &:= N\left(\left(\frac{1+\sqrt{-19}}{2}\right) - 2\left(x + y\left(\frac{1+\sqrt{-19}}{2}\right)\right)\right) \\
&= N\left(\left(\frac{1 - 4x - 2y}{2}\right) + \left(\frac{1 - 2y}{2}\right)\sqrt{-19}\right) \\
&= \frac{(1 - 4x - 2y)^2 + 19(1 - 2y)^2}{4} \\
&\ge \frac{19}{4} \\
&> 4
\end{aligned}$$

We are unable to find $(x, y) \in \mathbb{Z}^2$ such that $N(x, y) < N(\beta) = 4$. Thus $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is not a Euclidean Domain with respect to the norm function.

10. Computing the product gives:

$$\begin{aligned}
&1 + \zeta_{23} + \zeta_{23}^2 + \zeta_{23}^3 + \zeta_{23}^4 + 3\zeta_{23}^5 + 3\zeta_{23}^6 + 3\zeta_{23}^7 + \zeta_{23}^8 + 3\zeta_{23}^9 + 3\zeta_{23}^{10} + 7\zeta_{23}^{11} \\
&+ 3\zeta_{23}^{12} + 3\zeta_{23}^{13} + \zeta_{23}^{14} + 3\zeta_{23}^{15} + 3\zeta_{23}^{16} + 3\zeta_{23}^{17} + \zeta_{23}^{18} + \zeta_{23}^{19} + \zeta_{23}^{20} + \zeta_{23}^{21} + \zeta_{23}^{22}
\end{aligned}$$

Note that $\zeta_{23}^{23} = 1$, so that ζ_{23} is a root of $x^{23} - 1$. However, this polynomial has a factor of $x - 1$ and so ζ_{23} is a root of $x^{22} + x^{21} + ... + x + 1$ (which is irreducible by Exercise 6 of Week 1). Thus

$$1 + \zeta_{23} + \zeta_{23}^2 + ... + \zeta_{23}^{22} = 0.$$

Hence the product reduces to:

$$\begin{aligned} &2\zeta_{23}^5 + 2\zeta_{23}^6 + 2\zeta_{23}^7 + 2\zeta_{23}^9 + 2\zeta_{23}^{10} + 6\zeta_{23}^{11} + 2\zeta_{23}^{12} + 2\zeta_{23}^{13} + 2\zeta_{23}^{15} + 2\zeta_{23}^{16} + 2\zeta_{23}^{17} \\ &= 2(\zeta_{23}^5 + \zeta_{23}^6 + \zeta_{23}^7 + \zeta_{23}^9 + \zeta_{23}^{10} + 3\zeta_{23}^{11} + \zeta_{23}^{12} + \zeta_{23}^{13} + \zeta_{23}^{15} + \zeta_{23}^{16} + \zeta_{23}^{17}) \end{aligned}$$

which is clearly a multiple of 2 in $\mathbb{Z}[\zeta_{23}]$.

It follows that 2 divides the product, but it divides neither factor, so that 2 is not a prime element in $\mathbb{Z}[\zeta_{23}]$. Given that 2 is irreducible in $\mathbb{Z}[\zeta_{23}]$ we now conclude that $\mathbb{Z}[\zeta_{23}]$ is not a UFD, since $\mathbb{Z}[\zeta_{23}]$ is the ring of integers of $\mathbb{Q}(\zeta_{23})$ and we proved in the notes that such rings are integral domains that admitting factorisation into irreducibles (we also proved in the notes that such a ring is a UFD if and only if every irreducible is prime).