Michaelmas 2012, NT III/IV, Solutions to Problem Sheet 3.

1 (i) Define $\phi : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}_2$, by $\phi : a + b\sqrt{-3} \mapsto (a+b) \pmod 2$. We will write, for $a \in \mathbb{Z}$, the class of a in $\mathbb{Z}_2$ by $\bar{a}$ (not to be confused with the "conjugation" in $\mathbb{Z}[\sqrt{-3}]$, which we don't use here).

Claim: ϕ is a ring homomorphism:

1) $\phi(1) = \phi(1 + 0\sqrt{-3}) = \bar{1}$. ⟦We can usually drop this check.⟧

2)

$$\begin{aligned} \phi((a+b\sqrt{-3}) + (a'+b'\sqrt{-3}) &= \phi((a+a') + (b+b')\sqrt{-3})) \\ = \overline{a+a'+b+b'} &= \overline{a+b} + [\overline{a'+b'} \\ &= \phi(a+b\sqrt{-3}) + \phi(a'+b'\sqrt{-3}). \end{aligned}$$

3)

$$\begin{aligned} \phi((a+b\sqrt{-3})(a'+b'\sqrt{-3})) &= \phi((aa'-3bb') + (a'b+ab')\sqrt{-3}) \\ = \overline{aa'-3bb'+a'b+ab'} &= \overline{aa'+bb'+a'b+ab'} \\ = \overline{(a+b)(a'+b')} &= \phi(a+b\sqrt{-3})\phi(a'+b'\sqrt{-3}). \end{aligned}$$

So ϕ is a ring homomorphism.

Claim: $\ker\phi = J$.

Now $\phi(2) = 0 = \phi(1+\sqrt{-3})$ whence 2 and $1+\sqrt{-3}$ and hence any R--linear combinations thereof lie in $\ker\phi$. So $J = (2, 1+\sqrt{-3})_R \subseteq \ker\phi$.

On the other hand, if $\alpha = a + b\sqrt{-3} \in \ker\phi$ then $a + b \equiv 0 \mod 2$, say $a = -b + 2t$, with $t \in \mathbb{Z}$.
So $\alpha = 2(t-b) + b(1+\sqrt{-3}) \in (2, 1+\sqrt{-3})_R = J$.

Hence $\ker\phi \subseteq J$ and so $\ker\phi = J$.

Now ϕ is clearly surjective with image $\mathbb{Z}_2$. So, by the first isomorphism theorem, $R/J \cong \mathbb{Z}_2$, a field. And hence J is maximal, as required.

(ii) Denote by g_i the i-th generator in a given presentation of an ideal.

$$\begin{aligned} J^2 &= (2, 1+\sqrt{-3})_R^2 = (4, 2(1+\sqrt{-3}), 2(1+\sqrt{-3}), (1+\sqrt{-3})^2) \\ &= (4, 2(1+\sqrt{-3}), -2+2\sqrt{-3}) \qquad \text{eliminate } \mathrm{g}_3 \ (= \ \mathrm{g}_2), \\ &= 2(2, 1+\sqrt{-3}, -1+\sqrt{-3})_R, \\ &= 2(2, 1+\sqrt{-3}, -2)_R \qquad \text{replace } \mathrm{g}_3 \text{ by } \mathrm{g}_3 - \mathrm{g}_2, \\ &= 2(2, 1+\sqrt{-3})_R \qquad \text{eliminate } \mathrm{g}_3 \ (= -\mathrm{g}_1) \\ &= 2J = (2)_R J. \end{aligned}$$

But $J \neq (2)_R$, otherwise $2 \mid (1+\sqrt{-3})$ and $(1+\sqrt{-3})/2 \in R$, which is not the case.

(iii) Suppose $\alpha = a + b\sqrt{-3} \in R$ and $\alpha J \subseteq (2)_R = 2R$.
Then, in particular, $\alpha(1+\sqrt{-3}) = a - 3b + (a+b)\sqrt{-3}$ lies in $2R$. So $2 \mid (a+b)$ and $\phi(\alpha) = 0$.

So $\alpha \in \ker\phi = J$.

(iv) Certainly, $J = (2, 1+\sqrt{-3})_R \supseteq (2)_R$.
But suppose $J \mid (2)_R$, which should be interpreted as saying that there is an ideal I in R such that $IJ = (2)_R$. ⟦Note that I need not necessarily be principal. ⟧
But then, for all $\alpha \in I$, we would have $\alpha J \in (2)_R$, and so, by (iii), $\alpha \in J$.
Thus $I \subseteq J$ and so $2R = IJ \subseteq J^2 = 2J$ ($\subseteq 2R$).

Now $2 \in 2R = 2J$. So $2 = 2\beta$ for some $\beta \in J$. But then $1 = \beta \in J$ and hence $J = R$.
But $J \neq R$ since, by (i), R/J is non-trivial.
So J does not divide $(2)_R$.

2 (a) It is clear that $\varphi : R \to \mathbb{Z}^{\geq 0}$. So it remains to show that, for $\alpha, \beta \in R$,

(i) $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$;
(ii) $\varphi(\alpha) = 0 \implies \alpha = 0$;
(iii) $\varphi(\alpha) = 1 \implies \alpha \in R^*$.

So let $\alpha = r + s\sqrt{d}$ and $\beta = t + u\sqrt{d}$ (with $r, s, t, u \in \mathbb{Z}$). Then
$\varphi(\alpha\beta) = \varphi(rt + sud + (ru + st)\sqrt{d}) = |(rt + sud)^2 - (ru + st)^2 d|$
$= |r^2t^2 + s^2u^2d^2 - r^2u^2d - s^2t^2d|$, the cross terms cancelling.
And so $\varphi(\alpha)\varphi(\beta) = |(r^2 - ds^2)(t^2 - du^2)| = |r^2t^2 + s^2u^2d^2 - r^2u^2d - s^2t^2d| = \varphi(\alpha\beta)$.
And we have (i).

Again, suppose that $\varphi(\alpha) = 0$. Then $r^2 = ds^2$.
If $s \neq 0$ then $d = r^2/s^2$ and $\sqrt{d} = \pm r/s \in \mathbb{Q}$, a contradiction.
So $s = 0$ whence $r = 0$ and $\alpha = 0$. And we have (ii).

Finally, if $\varphi(\alpha) = 1$ then $1 = \pm(r^2 - ds^2) = \pm(r - s\sqrt{d})\alpha$. So $\alpha \in R^*$.

(b) For $\beta \notin R^\times$, $\beta \neq 0$ we have $\varphi(\beta) > 1$. Now multiply both sides by $\varphi(\gamma)$.

(c) We can ignore the "stupid" case $\alpha = 0$.
Moreover, any $\alpha \in \mathbb{R}^\times$ (i.e. a unit) is indeed an *empty* (hence certainly finite) product of irreducibles, multiplied by a unit.
For any other $\alpha \notin R^\times$, we have $\varphi(\alpha) > 1$, and so we can use induction on $\varphi(\alpha)$, reducing it to smaller factors. (We had a similar argument in the lectures.)

3 (i) $R = \mathbb{Q}[X]$:

(a) Define $\varphi : R \to \mathbb{Z}^{\geq 0}$ by $\varphi(0) = 0$ and $\varphi(\gamma) = \deg(\gamma) + 1$, if $\gamma \neq 0$.

Given α, $\beta \in R$ with $\alpha \neq 0$ we must show that there is a $\gamma \in R$ such that

$$\varphi(\beta - \alpha\gamma) < \varphi(\alpha).$$

If $\alpha \in \mathbb{Q}$ then we need only take $\gamma = \beta\alpha^{-1}$ (since $\alpha \neq 0$).

If $\alpha \notin \mathbb{Q}$ then, by long division of polynomials, we can find $\gamma \in R$ such that

$$\deg(\beta - \alpha\gamma) < \deg(\alpha)$$

and then $\varphi(\beta - \alpha\gamma) < \varphi(\alpha)$, as required.

So φ is Euclidean and R is a Euclidean ring.

(b) (Take $\gamma = X$).

(ii) $R = \mathbb{Z}[i]$:

(a) Define $\varphi : R \to \mathbb{Z}^{\geq 0}$ by $\varphi(\gamma) = \gamma\bar{\gamma} = |\gamma|^2$.

Take α, $\beta \in R$ with $\alpha \neq 0$. We must show that there is a $\gamma \in R$ such that

$$\varphi(\beta - \alpha\gamma) < \varphi(\alpha).$$

Now $\dfrac{\beta}{\alpha} = \dfrac{\beta\widetilde{\alpha}}{\alpha\widetilde{\alpha}} = x + yi$ for some x and y in $\mathbb{Q}$ (since $\alpha\widetilde{\alpha} \in \mathbb{N}$).

Choose $\gamma = m + in \in R$ where $m = \lfloor x + \frac{1}{2} \rfloor$ and $n = \lfloor y + \frac{1}{2} \rfloor$. (Here $\lfloor x \rfloor$, for some $x \in \mathbb{R}$, denotes the largest integer smaller or equal to x.)
Then, with $r = x - m$ and $s = y - n$, we have $|r|$ and $|s| \leq \frac{1}{2}$.

So

$$\begin{aligned}
\varphi(\beta - \alpha\gamma) &= \varphi((\beta/\alpha - \gamma)\alpha) = \varphi(\beta/\alpha - \gamma)\varphi(\alpha) \\
&= \varphi(r + si)\varphi(\alpha) = (r^2 + s^2)\varphi(\alpha) \\
&\leq (\frac{1}{4} + \frac{1}{4})\varphi(\alpha) \\
&< \varphi(\alpha),
\end{aligned}$$

as required.

Hence φ is Euclidean and R is a Euclidean ring.

(b) With $\alpha = 4 + 5i$ and $\beta = 15 + 8i$,

$$\frac{\beta}{\alpha} = \frac{(15 + 8i)(4 - 5i)}{4^2 + 5^2} = \frac{100 - 43i}{41}.$$

Choosing γ as above we find $\gamma = 2 - i$.

Checking: $(\beta - \alpha\gamma) = 15 + 8i - (4 + 5i)(2 - i) = 2 + 2i$.
And so $\varphi(\beta - \alpha\gamma) = 4 + 4 = 8 < 41 = \varphi(\alpha)$, as required.

(iii) $R = \mathbb{Z}[\sqrt{3}]$:

(a) Define $\varphi : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}$ by $\varphi(a + b\sqrt{3}) = |a^2 - 3b^2|$ (for $a, b \in \mathbb{Q}$).

If $\alpha = a + b\sqrt{3} \in R$ then a and $b \in \mathbb{Z}$, and so

$$\varphi(\alpha) = |a^2 - 3b^2| \in \mathbb{Z}^{\geq 0}.$$

Moreover, $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.
Take α, $\beta \in R$ with $\alpha \neq 0$. We must show that there is a $\gamma \in R$ such that

$$\varphi(\beta - \alpha\gamma) < \varphi(\alpha).$$

Now $\alpha\widetilde{a} \in \mathbb{Z}$ and $\widetilde{a} \neq 0$ (since $\widetilde{\ } : R \to R$, $a + b\sqrt{3} \mapsto a - b\sqrt{3}$ is injective).
So $\dfrac{\beta}{\alpha} = \dfrac{\beta\widetilde{a}}{\alpha\widetilde{a}} = x + y\sqrt{3}$ for some x and y in $\mathbb{Q}$.

Choose $\gamma = m + n\sqrt{3} \in R$ where $m = [x + \frac{1}{2}]$ and $n = [y + \frac{1}{2}]$.
Then, with $r = x - m$ and $s = y - n$, we have $|r|$ and $|s| \leq \frac{1}{2}$.

So

$$\begin{aligned}
\varphi(\beta - \alpha\gamma) &= \varphi((\beta/\alpha - \gamma)\alpha) = \varphi(\beta/\alpha - \gamma)\varphi(\alpha) \\
&= \varphi(r + s\sqrt{3})\varphi(\alpha) = |r^2 - 3s^2|\varphi(\alpha) \leq \max(r^2, 3s^2)\varphi(\alpha) \\
&\leq \frac{3}{4}\varphi(\alpha) \\
&< \varphi(\alpha),
\end{aligned}$$

as required.

Hence φ is Euclidean and R is a Euclidean ring.

(b) With $\alpha = 1 + 3\sqrt{3}$ and $\beta = 5 - 9\sqrt{3}$,

$$\frac{\beta}{\alpha} = \frac{(5 - 9\sqrt{3})(1 - 3\sqrt{3})}{1 - 27} = \frac{86 - 24\sqrt{3}}{-26} = \frac{-43 + 12\sqrt{3}}{13}$$

Choosing γ as above we find $\gamma = -3 + \sqrt{3}$.

Checking: $(\beta - \alpha\gamma) = 5 - 9\sqrt{3} - (1 + 3\sqrt{3})(-3 + \sqrt{3}) = -1 - \sqrt{3}$.
And so $\varphi(\beta - \alpha\gamma) = |1 - 3| = 2 < 26 = \varphi(\alpha)$, as required.

4 (i) It is clear that P is an *additive* subgroup of R. Moreover, multiplying two monomials $a \cdot 2^r$ and $b \cdot 2^t$ in P, i.e., with $a, b \in \mathbb{Z}$ and $r, t \in \mathbb{Q}^{>0}$ produces another such monomial $ab \cdot 2^{r+t}$. Hence, multiplying *sums of* such monomials gives us also sums of the same type, which shows that $P^2 \subseteq P$.

On the other hand, each element $\pi = \sum_{j=1}^{s} a_j 2^{r_j}$ in P can be written as a product of other elements in P: take $r \in \mathbb{Q}$ such that $0 < r < r_j$ for all $r = 1, \dots, s$. Then 2^r and $\sum_{j=1}^{s} a_j 2^{r_j - r}$ are both in P and their product is simply π. Hence $P \subseteq P^2$.

(ii) Use that any element in R can be written—after combining terms in the form $\sum_{j=1}^{s} a_j 2^{r_j}$ with a_j *odd* for all j, where the r_j are mutually different. In fact, we can order the terms with respect to their exponents, i.e., such that $r_1 < r_2 < \cdots < r_s$, where r_1 can attain the value 0.

Similarly any element in P can be written in that form, with the extra condition that $r_1 > 0$, since all the exponents have to be *strictly greater* than 0.

Now multiplying $\pi \in P$ and $\rho \in R$ gives $\pi\rho$ with all exponents > 0, i.e. lying in P, whence P is an *ideal* in R.

Hence an element $\rho \in R$ can be written as $\rho =$ odd integer$\cdot 2^0 +$something in P, so $R \setminus P$ consists of the odd integers. But the ideal generated by P and any odd integer generates $1 \in R$ (since the even integers are in P), and hence generates R itself.

Therefore P is maximal.

(iii) Follows from the considerations in (ii), since all even integers are in P and $1 + P \supseteq 1 + 2\mathbb{Z}$, which contains (in fact equals) $R \setminus P$.

5 (Straightforward from Algebra II, intended as a reminder only.)

6 Suppose $\sum_{j=1}^{n} l_j \gamma\gamma_j = 0$, for some $l_1, \dots, l_n \in K$.
Then $\sum_{j=1}^{n} l_j \gamma_j = \gamma^{-1} \sum_{j=1}^{n} l_j \gamma\gamma_j = 0$, since $\gamma \in F^*$.
So $l_j = 0$ for every j (since $\{\gamma_1, \dots, \gamma_n\}$ is linearly independent over K).

Thus $\{\gamma\gamma_1, \dots, \gamma\gamma_n\}$ is linearly independent over K.

So, since $\{\gamma\gamma_1, \dots, \gamma\gamma_n\} \subset F$ and $|F : K| = n$,

$\{\gamma\gamma_1, \dots, \gamma\gamma_n\}$ is a basis for F over K.

7 Put $l = (a\alpha + b)/(c\alpha + d)$. Clearly we have $\mathbb{Q}[l] = \mathbb{Q}[(a\alpha + b)/(c\alpha + d)] \subseteq \mathbb{Q}[\alpha]$.

(Here we've used that $\mathbb{Q}[\alpha]$ is a field, since α is an algebraic number.)

We must show that $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[l]$.
Now $l(c\alpha + d) = (a\alpha + b)$; so $\alpha(cl - a) = (-dl + b)$.
But $cl - a = c(a\alpha + b)/(c\alpha + d) - a = (cb - ad)/(c\alpha + d) \neq 0$.
Thus $\alpha = (-dl + b)/(cl - a) \in \mathbb{Q}[l]$.

Thus $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[l]$.

8 Now $K \supseteq \mathbb{Q}[\alpha] \supseteq \mathbb{Q}$.
We have $|\mathbb{Q}[\alpha] : \mathbb{Q}|$ divides $|K : \mathbb{Q}[\alpha]| \cdot |\mathbb{Q}[\alpha] : \mathbb{Q}| = |K : \mathbb{Q}| = p$ by the Tower Theorem,.
So $|\mathbb{Q}[\alpha] : \mathbb{Q}| = 1$ or p. But $|\mathbb{Q}[\alpha] : \mathbb{Q}| \neq 1$ (else $\alpha \in \mathbb{Q}$).

So $|\mathbb{Q}[\alpha] : \mathbb{Q}| = p$.

9 (i) Put $q(X) = X^2 - 7$. Then $q(X)$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein's Criterion with prime 7.
Since $q(\sqrt{7}) = 0$, $q(X)$ is the min. poly. of $\sqrt{7}$ in $\mathbb{Q}[X]$.

Thus, $|\mathbb{Q}[\sqrt{7}] : \mathbb{Q}| = \deg q(X) = 2$.

(ii) Note that $\sqrt[3]{5} \in \mathbb{Q}[\sqrt[3]{5} + 2]$ and that $\sqrt[3]{5} + 2 \in \mathbb{Q}[\sqrt[3]{5}]$.

So $\mathbb{Q}[\sqrt[3]{5}] \subseteq \mathbb{Q}[\sqrt[3]{5}+2]$, $\mathbb{Q}[\sqrt[3]{5}+2] \subseteq \mathbb{Q}[\sqrt[3]{5}]$ and $\mathbb{Q}[\sqrt[3]{5}+2] = \mathbb{Q}[\sqrt[3]{5}]$.

Now $q(X) = X^3 - 5$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein's Criterion with prime 5. Since $q(\sqrt[3]{5}) = 0$, $q(X)$ is the min. poly. of $\sqrt[3]{5}$ in $\mathbb{Q}[X]$.

Thus $|\mathbb{Q}[\sqrt[3]{5}+2] : \mathbb{Q}| = |\mathbb{Q}[\sqrt[3]{5}] : \mathbb{Q}| = \deg q(X) = 3$.

(iii) Let $\alpha = e^{2\pi i/5}$. Note that (cf. (ii)) $\mathbb{Q}[\alpha] = \mathbb{Q}[\alpha - 1]$.

Put $\beta = \alpha - 1\,(\neq 0)$. Then $1 = \alpha^5 = (\beta+1)^5 = \beta^5 + 5\beta^4 + 10\beta^3 + 10\beta^2 + 5\beta + 1$.

So $\beta^4 + 5\beta^3 + 10\beta^2 + 10\beta + 5 = (\beta^5 + 5\beta^4 + 10\beta^3 + 10\beta^2 + 5\beta)/\beta = 0$.

Thus $q(X) = X^4 + 5X^3 + 10X^2 + 10X + 5$ is the min. poly. of β over $\mathbb{Q}$ since it is irreducible in $\mathbb{Q}[X]$ by Eisenstein's Criterion with prime 5.

Thus $|\mathbb{Q}[\alpha] : \mathbb{Q}| = |\mathbb{Q}[\beta] : \mathbb{Q}| = \deg q(X) = 4$.

10 We illustrate the idea for $p = 7$, $q = 2$, leaving the general case as a minor transfer exercise (the case $ab = 0$ then needs a slightly different argument).

Put $K = \mathbb{Q}[\sqrt{2}]$. We claim that $\sqrt{7} \notin K$.

For suppose that $\sqrt{7} \in K$ then $\sqrt{7} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.

Then $7 = a^2 + 2b^2 + 2ab\sqrt{2}$.

If $ab \neq 0$ then $\sqrt{2} = (7 - a^2 - 2b^2)/2ab \in \mathbb{Q}$. Contradiction.

But if $ab = 0$ then $7 = a^2 + 2b^2$ and this has no integer solution. Contradiction.

Thus $\sqrt{7} \notin K$ and so $X^2 - 7$ has no roots in K.

Hence $X^2 - 7$ is irreducible in $K[X]$ and is therefore the min. poly. of $\sqrt{7}$ over K