MATH 203301

ANSWERS: MATH 2033
(May/June 2010)

Rings, Polynomials and Fields

Non-bookwork questions are similar to seen unless otherwise stated.

1. (i) Let $a, b \in \mathbb{Z}$ be such that $\alpha = a + b\sqrt{d}$. Then $N(\alpha) = |a^2 - db^2|$.

(3 Marks)

(ii) $(a + b\sqrt{d})(e + f\sqrt{d}) = (ae + dbf) + (af + be)\sqrt{d}$

$N((ae+dbf)+(af+be)\sqrt{d}) = |(ae+dbf)^2-d(af+be)^2| = |a^2e^2+d^2b^2f^2-d(a^2f^2+b^2e^2)|$

$\square$

(5 Marks)

(iii)

$$\frac{20 + 4\sqrt{3}}{1 + 3\sqrt{3}} = \frac{(20 + 4\sqrt{3})(1 - 3\sqrt{3})}{(1 + 3\sqrt{3})(1 - 3\sqrt{3})} = \frac{-16 - 56\sqrt{3}}{-26}$$

so $q = 1 + 2\sqrt{3}$ and

$$r = -(1 + 2\sqrt{3})(1 + 3\sqrt{3}) + 20 + 4\sqrt{3} = 1 - \sqrt{3}$$

(Optional check: $N(r) = 1 + 12 < N(1 + 3\sqrt{3}) = |1 - 27|$.)

(9 Marks)

(iv)

(a) ANSWER: $1 + 1 = 2$ even, so not closed under addition, so NO.

(2 Marks)

(b) ANSWER: $\frac{1}{6} \in T$ but $(\frac{1}{6})^2 = \frac{1}{36} \notin T$ so NO.

(2 Marks)

(c) ANSWER: Sum of diagonal matrices is diagonal; product of diagonal matrices is diagonal; identity matrices are diagonal; additive inverse of diagonal matrix is diagonal. Thus U is a subring.

(4 Marks)

(continued. . .)

2. See paper version for now.

(continued. . .)

3. (i) Let R and S be rings. A *(ring) homomorphism* $\theta : R \to S$ is a map such that for all $r, r' \in R$,

$$\theta(rr') = \theta(r)\theta(r')$$

and $\theta(r + r') = \theta(r) + \theta(r')$ and $\theta(1) = 1$ (where we denote the multiplicative identity of any ring by 1).

(6 Marks)

(ii) $a + 0 = a$ implies $\theta(a) + \theta(0) = \theta(a)$.

(3 Marks)

(iii)

(1) $\theta : \mathbb{Z}[\sqrt{23}] \to \mathbb{Z}[\sqrt{23}]$ defined by $\theta(a + b\sqrt{23}) = a - b\sqrt{23}$ for $a, b \in \mathbb{Z}$.

ANSWER: YES. (Arithmetic on either side requires $\sqrt{23}^2 = 23$ but only an internally consistent choice of sign for $\sqrt{23}$, so operations are preserved by the map.)

(2) $\psi : \mathbb{Z} \to \mathbb{Z}[\sqrt{2}]$ defined by $\phi(a) = a\sqrt{2}$ for $a \in \mathbb{Z}$.

ANSWER: NO. ($1.1 = 1$, $\psi(1).\psi(1) = 2 \neq \psi(1)$.)

(3) $\phi : \mathbb{Z}[\sqrt{2}] \to M_2(\mathbb{Z}[\sqrt{2}])$ defined by $\phi(a + b\sqrt{2}) = (b + a\sqrt{2})1_2$ for $a, b \in \mathbb{Z}$ (recall that $M_2(R)$ is the ring of 2×2 matrices over a ring R, and

$$1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is the unit matrix).

ANSWER: NO. (As above, essentially.)

(6 Marks)

(iv) Let I be an ideal in a ring R. Explain what is meant by the *factor ring* R/I.

For r in R define $[r] = \{r + i \mid i \in I\}$. The ring R/I has these as elements, and operations induced from those on representatives in R:

$$[r] + [r'] = [r + r']$$

and $[r].[r'] = [rr']$. (Noting that such rules turn out to be well-defined.)

(6 Marks)

(v) Give the multiplication table for the ring $\mathbb{Z}/2\mathbb{Z}$.

Setting $[0] = \{\textit{even numbers}\}$; $[1] = \{\textit{odd numbers}\}$:

	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

(4 Marks)

(continued...)

4. See paper version for now.

(continued...)

5.

(i) $\omega^2 = \sqrt{7} - 1$ so $\omega^4 = (\sqrt{7} - 1)(\sqrt{7} - 1) = 8 - 2\sqrt{7}$ so $\omega^4 + 2\omega^2 = 6$

(2 Marks)

(ii) $\tau^2 = 5 - \sqrt{5}$. Now for $a, b \in \mathbb{Q}$, $a + b\sqrt{5} = a - (\tau^2 - 5)b \in \mathbb{Q}(\tau)$ $\square$

(4 Marks)

(iii) $\alpha \in K$ is said to be *algebraic* over F if there exists $f \in F[x]$ such that $f(\alpha) = 0$ in K.

(4 Marks)

(iv) $\sqrt{2}$ (or other), *algebraic* with polynomial $x^2 - 2$ and irrational (else there exist p, q coprime with $p/q = \sqrt{2}$, giving $p^2 = 2q^2$ whereupon primeness of 2 contradicts coprimality).

(2 Marks)

(v) Let $m = \sum_{i=0}^{n} m_i x^i$ with degree n minimal among those polynomials with root α. Then m/m_n monic. So consider m monic WLOG. If m' is another such, $m - m'$ has root α and lower degree, hence must vanish. Finally, m cannot factorise, else again one factor has lower degree and root α. $\square$

(5 Marks)

(vi) $\tau^2 = 5 - \sqrt{5}$, $5 - \tau^2 = \sqrt{5}$, $(5 - \tau^2)^2 = 5$ so $\tau^4 - 10\tau^2 + 20 = 0$ monic, and irreducible (e.g. by Eisenstein).

(4 Marks)

(vii) $\{1, \tau, \tau^2, \tau^3\}$ a basis of $\mathbb{Q}(\tau)$ over $\mathbb{Q}$ by the last result, so $[\mathbb{Q}(\tau) : \mathbb{Q}] = 4$. Clearly $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Thus $[\mathbb{Q}(\tau) : \mathbb{Q}(\sqrt{5})] = 2$ by the Tower Theorem.

(6 Marks)

END