MATH 203301

ANSWERS: MATH 2033
(2011)

Rings, Polynomials and Fields

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

1. (i) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

This is a subset of $\mathbb{R}$ and arithmetic is taken from there, so need to check closure and identities and additive inverses.

(4 Marks)

(ii) Suppose $a + b\sqrt{2} = a' + b'\sqrt{2}$. Then $(a - a') = (b' - b)\sqrt{2}$. Thus either $a - a' = 0$ and $b - b' = 0$ or $\sqrt{2}$ is rational — a contradiction.

(4 Marks)

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

(3 Marks)

(iv) A unit in a ring is an element with a multiplicative inverse.

(1 Marks)

(v) For $\mathbb{Z}[\sqrt{-2}]$ we have $N(a+b\sqrt{-2}) = a^2+2b^2$. A unit has norm 1, so $b = 0$ and $a = \pm 1$. For $\mathbb{Z}[\sqrt{2}]$ we have $N(a + b\sqrt{2}) = a^2 - 2b^2$. A unit has norm 1, so require solutions to $a^2 = 1 + 2b^2$. For example $a = 3$, $b = 2$ gives a unit $u_1 = 3 + 2\sqrt{2}$. Evidently this has magnitude greater than 1, so all positive powers of u_1 are distinct. But if u is a unit then so is u^2. DONE.

(3 Marks)

(vi)

(a) ANSWER: $1 + 1 = 2$, 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: Closed under addition. Closed under multiplication. Indentity matrices are of this form. Additive inverses are of this form. Thus U is a subring.

(4 Marks)

(d) ANSWER: Not closed under multiplication, so NO.

(2 Marks)

(continued. . .)

2. (i) Answer: Let $H, H' \subseteq G$ be groups. If $g, f \in H \cap H'$ then $g, f \in H, H'$ so $gf \in H, H'$, so $gf \in H \cap H'$. Thus multiplication closes in $H \cap H'$. Evidently the identity element e of G lies in H and H' and hence in $H \cap H'$. Finally if $g \in H, H'$ then $g^{-1} \in H, H'$ so $H \cap H'$ also has inverses. DONE.

(4 Marks)

(ii) $2\mathbb{Z}$ is even numbers; $3\mathbb{Z}$ is numbers congruent to 0 mod. 3.
Check closure; identity (0 in both cases); inverses (negations in both cases).
$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

(4 Marks)

(iii) Write $\{G_i\}_i$ for the set of subgroups containing S.
(a) the indentity element is in every subgroup, so it is in the intersection.
(b) since S is a subset of every subgroup concerned, and these are groups, they also each contain the inverses.
(c) suppose for a contradiction that some sum x is not in. Then it is not in some G_i. But then G_i is not closed under addition — a contradiction. (Other formulations are acceptable.)

(3 Marks)

(iv) Let I, I' be ideals. Note from above that $I \cap I'$ is an abelian group. So RTS $x \in I, I'$ implies $rxr' \in I, I'$. But this is true for I and I' separately. DONE.

(3 Marks)

(v) First note that (S) contains the abelian group closure of any subset. Next note that every ideal containing S contains the argument of the closure on the right by the definition of ideal, hence this is a subset of the intersection (S). Thus the RHS is contained in the left. Finally note that the RHS is an ideal, by considering the action of $r \in R$ on the right (resp. left) on a representative element. (Or otherwise.)

(4 Marks)

(vi) $ar + ar' = a(r + r') \in aR$; $(ar)s = a(rs) \in aR$.

(2 Marks)

(vii) (1) $d \in I$ implies $dn \in I$ by closure under repeated addition (say).
(2) suppose there is such an element. Then there is a positive one WLOG. Then $d' - d$ is smaller positive in $I \setminus d\mathbb{Z}$. Iterating this subtraction eventually results in an element in $[1, d-1]$ and hence contradiction of 'smallest'.

Every proper ideal I in $\mathbb{Z}$ has a smallest positive element. If this element is a, say, then we have shown $I = a\mathbb{Z}$. DONE.

(5 Marks)

(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) $-a$ is additive inverse of a, i.e. $a + (-a) = 0$. $-\theta(a)$ is additive inverse of $\theta(a)$. Apply θ: $\theta(a) + \theta(-a) = 0$, so $\theta(-a) = -\theta(a)$.

(3 Marks)

(iii)

(1) $\theta : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{3}]$ defined by $\theta(a + b\sqrt{3}) = a - b\sqrt{3}$ for $a, b \in \mathbb{Z}$.

ANSWER: YES. (Arithmetic on either side requires $\sqrt{3}^2 = 3$ but only an internally consistent choice of sign for $\sqrt{3}$, so operations are preserved by the map.)

(2) $\psi : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]$ defined by $\phi(a) = a\sqrt{7}$ for $a \in \mathbb{Z}$.

ANSWER: NO. ($1.1 = 1$, $\psi(1).\psi(1) = 7 \neq \psi(1)$.)

(3) $\phi : \mathbb{Z}[\sqrt{2}] \to M_2(\mathbb{Z}[\sqrt{2}])$ defined by $\phi(a + b\sqrt{2}) = (b + a\sqrt{2})T$ 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 (since, for example, the identity is not taken to the identity).

(6 Marks)

(iv) REFLEXIVE: $r - r = 0 \in I$

SYMMETRIC: $r - r' = -(r' - r)$

TRANSITIVE: $r - s, s - t \in I$ implies $(r - s) + (s - t) = r - t \in I$.

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 $\mathbb{Z}/3\mathbb{Z}$.

Setting $[0] = \{0, 3, 6, ...\}$; $[1] = \{1, 4, 7, ...\}$ and so on:

	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

(4 Marks)

(continued. . .)

4. (i) $A = \{f \in \mathbb{Q}[x] \ : \ f(3) = 1\}$ is an ideal in $\mathbb{Q}[x]$ if
(I) $(A, +)$ is a subgroup;
(II) $ar, ra \in A$ for all $a \in A$, $r \in R$.
Check: (I) $(f+g)(3) = f(3) + g(3) = 1 + 1 = 2$ so we do NOT have closure. DONE.

(5 Marks)

(ii) There is more than one way to do this. One strategy is to answer the last part first. Let a be the primitive fourth root of 5, and note that $a \in \mathbb{R}$, but not in $\mathbb{Q}$ (by a Theorem, say). Then

$$x^4 - 5 = (x-a)(x+a)(x-ia)(x+ia)$$

as a product of irreducible polynomials in $\mathbb{C}[x]$.
Since $\mathbb{R} \subset \mathbb{C}$ the factorisation as a product of irreducibles in $\mathbb{R}[x]$ is given by taking suitable products from these factors, when they do not lie in $\mathbb{R}[x]$. By inspection we thus have

$$x^4 - 5 = (x-a)(x+a)(x^2 + a^2)$$

as a product of irreducible polynomials in $\mathbb{R}[x]$.
Similarly in $\mathbb{Q}[x]$ we see that there is no stopping point in the combination of factors, so $x^4 - 5$ is irreducible over $\mathbb{Q}$.

(5 Marks)

(iii) Determine, giving reasons, which of the following polynomials are irreducible over $\mathbb{Q}$. There is more than one way to do these.

(a) Any rational root r/s obeys $r|4$ and $s|1$. Possibilities are $r/s \in \{\pm 1, \pm 2, \pm 4\}$. Substitution eliminates all of them. Thus irreducible.

(b) Any rational root r/s obeys $r|7$ and $s|1$. Possibilities are $r/s \in \{\pm 1, \pm 7\}$. Substitution eliminates all of them. Thus irreducible.
(Alternatively note that this is irreducible over $\mathbb{R}$ since it is everywhere positive!)

(c) $6x^4 + 10x^3 + 30x^2 + 10x + 25$.
Irreducible by reverse Eisenstein with $p = 2$.

(d) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
Compute $f(x+1)$. Then irreducible by Eisenstein's criterion with $p = 7$.
(Or could use the rational root test directly.)

(8 Marks)

(iv) BOOKWORK: Definition: A *primitive polynomial* is a polynomial in $\mathbb{Z}[x]$ such that the GCD of the coefficients is 1.

(3 Marks)

(v) Suppose for a contradiction that $pp' + 1 = pq$. Then $pq - pp' = 1$ so $p(q - p') = 1$ so p a unit. This contradicts the irreducibility of p. The same argument works for p'.

(continued. . .)

(3 Marks)

(vi) The Maclaurin series has unboundedly many terms, but polynomials have only finitely many terms.

(1 Marks)

(continued. . .)

5.

(i) $\mathbb{Q}(\sqrt{d})$ is smallest subfield of $\mathbb{R}$ containing $\mathbb{Q} \cup \{\sqrt{d}\}$.

(1 Marks)

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

(2 Marks)

(iii) $\sqrt{2}$ (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)

(iv) 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)

(v) A basis is a linearly independent spanning set.

(2 Marks)

(vi) Since the minimal polynomial of τ is $\tau^4 - 10\tau^2 + 20 = 0$ — monic, and irreducible (e.g. by Eisenstein) — $\{1, \tau, \tau^2, \tau^3\}$ a basis of $\mathbb{Q}(\tau)$ over $\mathbb{Q}$.

(4 Marks)

(vii) Consider K as a vector space over F. Then $[K : F]$ is the dimension.

(2 Marks)

(viii) Since the minimal polynomial of τ is $\tau^4 - 10\tau^2 + 20 = 0$, $\{1, \tau, \tau^2, \tau^3\}$ is a basis of $\mathbb{Q}(\tau)$ over $\mathbb{Q}$, 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 (assuming, or checking, that $\mathbb{Q}(\tau) \supset \mathbb{Q}(\sqrt{5})$).

(5 Marks)

(ix) Since the polynomial is quadratic it is enough to evaluate at 0 and 1 and check neither is a root.

(2 Marks)

END