

### Question 2

- (i) What do I have to do ... follow basic strategy for ideals. Closure under +, closure under additive inverses, possessing zero, closure under arbitrary multiplication. Slight difficulty over elements. Element of  $R/N$  is  $r + N$  for  $r \in R$ . Element of  $I/N$  is  $x + N$  for  $x \in I$ . Each step needs the definition of  $I/N$ , properties of the ideal  $I$ .

- (ii) What have fields to do with ideals? Fields have only trivial ideals so there's the germ of a contradiction argument here.

*Closure under +* Suppose  $x + N, y + N \in I/N$ ; then

$$(x + N) + (y + N) = (x + y) + N$$

(by definition of coset addition).

But  $x, y \in I$  so  $(x + y) \in I$  since  $I$  is an ideal. Hence  $(x + y) + N \in I/N$ .

*Additive inverses* Suppose  $x + N \in I/N$ ; then

$$-(x + N) = (-x) + N.$$

But  $x \in I$ , so  $-x \in I$ , so  $(-x) + N \in I/N$ .

*Zero* Since  $I$  is an ideal,  $0 \in I$ . Hence  $0 + N = N \in I/N$ . So  $N$  is the zero of  $R/N$ , and  $I/N$  does contain the zero of  $R/N$ .

*Arbitrary multiplication* Suppose  $x + N \in I/N$  and  $r + N \in R/N$ . Then  $(x + N)(r + N) = (xr) + N$ . But  $x \in I, r \in R$  so  $xr \in I$  because  $I$  is an ideal. Thus  $(xr) + N \in I/N$ . Since  $R$  is commutative, so is  $R/N$ , and hence  $(r + N)(x + N) \in I/N$ .

Suppose not: that is, suppose  $I \neq R, I \neq N$ . Then  $I/N$  is an ideal of  $R/N$ .

Because  $I \neq R$ , there is some coset  $r + N$  not in  $I/N$ , so  $I/N \neq R/N$ . Because  $I \neq N$ , there is a coset  $x + N \neq N$  in  $I/N$ . Hence  $I/N$  is non-trivial and not the whole ring  $R/N$ . But this contradicts Theorem 2.4.3, that the only ideals of the field  $R/N$  are  $R/N$  and the zero ideal. Thus either  $I = N$  or  $I = R$ .

### Question 3

- (i) Basic strategy called for: closure under +, zero, closure under scalar multiplication. Nearly forgot the subset requirement ... bad trap to fall into.

- (ii) Need to prove spanning and linear independence.

- (iii) Need to prove spanning and linear independence. Spanning is OK because of definition of  $W$ , but independence looks harder. Try a 'first principles' approach. On the face of it we have  $i = c^{-1}(-a - b\sqrt{2})$  which would make  $i$  real ... but we'd better look at the possibility  $c = 0$ . Deal with  $c \neq 0, c = 0$  separately.

Since the elements of  $W$  are of the form of those in  $K$  with  $d = 0$ , we have  $W \subseteq K$ .

If  $a + b\sqrt{2} + ci, a' + b'\sqrt{2} + c'i \in W$ , then

$$(a + b\sqrt{2} + ci) + (a' + b'\sqrt{2} + c'i) \\ = (a + a') + (b + b')\sqrt{2} + (c + c')i \in W$$

because  $\mathbf{Q}$  is closed under addition, so

$$a + a', b + b', c + c' \in \mathbf{Q}.$$

Since  $0 \in \mathbf{Q}, 0 + 0\sqrt{2} + 0i = 0 \in W$ , so  $W$  contains the zero of  $K$ . If  $a + b\sqrt{2} + ci \in W$  and  $\lambda \in \mathbf{Q}$ , then

$$\lambda(a + b\sqrt{2} + ci) = (\lambda a) + (\lambda b)\sqrt{2} + (\lambda c)i \in W$$

because  $\mathbf{Q}$  is closed under multiplication. Hence  $W$  is a vector subspace of  $K$ .

$\{1, \sqrt{2}\}$  spans  $V$  by the definition of the elements of  $V$  as linear combinations of  $1, \sqrt{2}$  over  $\mathbf{Q}$ .

Suppose  $a + b\sqrt{2} = 0$ . This means that  $\sqrt{2}$  is rational unless  $a = b = 0$ . Since  $\sqrt{2}$  is irrational, we obtain  $a = b = 0$ . Thus  $\{1, \sqrt{2}\}$  is a linearly independent spanning set, hence a basis for  $V$ .

$\{1, \sqrt{2}, i\}$  spans  $W$  by the definition of the elements of  $W$  as linear combinations of  $1, \sqrt{2}, i$  over  $\mathbf{Q}$ .

Suppose  $a + b\sqrt{2} + ci = 0$  for  $a, b, c \in \mathbf{Q}$ . If  $c \neq 0$  then

$$i = c^{-1}(-a - b\sqrt{2})$$

which forces  $i \in \mathbf{R}$ ; contradiction.

Thus  $c = 0$ .

Then  $a + b\sqrt{2} = 0$ . In part (ii) we showed that this implies that  $a = b = 0$ . Thus  $\{1, \sqrt{2}, i\}$  is a linearly independent spanning set, hence a basis.