Algebra III M3P8, M4P8

Solutions Sheet 5

1) (a) and (b) are easy, and (c) follows from (b).

(d) No, for example consider $f : \mathbb{Z} \to \mathbb{Q}$, $I = (0) \subset \mathbb{Q}$. But (0) is a maximal ideal of $\mathbb{Q}$ but not a maximal ideal of $\mathbb{Z}$.

2) (a) I is visibly principal, but not prime hence not maximal. Indeed, 2 and 5 are not in I, because if $2 = (a + b\sqrt{-10})\sqrt{-10}$, then 4 is a multiple of 10 which is absurd (and a similar argument works for 5). But their product, 10, is in I.

(b) If $I = (a+b\sqrt{-10})$, then a^2+10b^2 divides 4 and 10, hence divides 2. But then $a + b\sqrt{-10} = \pm 1$ implying that $1 = (m + n\sqrt{-10})2 + (p + q\sqrt{-10})\sqrt{-10}$ for some integers m, n, p, q. But the real part of the right hand side is even, a contradiction. Thus I is not principal. It is clear that $\mathbb{Z}[\sqrt{-10}]/I \cong \mathbb{Z}/2$ which is a field, hence I is maximal and thus prime.

(c) Since $x = -(x^3 - x) + x \cdot x^2 \in I$ we see that $I = (x)$, hence I is principal. Also, $\mathbb{R}[x]/I \cong \mathbb{R}$ is a field, so I is maximal, and thus prime.

(d) Note that $I = (x^2+2)$, so I is principal. Since $\mathbb{Z}[x]/I \cong \mathbb{Z}[\sqrt{-2}]$ is an integral domain but not a field, I is prime but not maximal.

(e) For contradiction assume that $(x, y) = (f(x, y))$ for some polynomial $f(x, y)$. We are given that $\mathbb{R}[x, y]$ is a UFD. Thus $x = f(x, y)g(x, y)$ and $y = f(x, y)g(x, y)$ for some $g(x, y)$, $h(x, y) \in \mathbb{R}[x, y]$. It follows that $f(x, y)$ has degree 0 as a polynomial in x with coefficients in $\mathbb{R}[y]$. Similarly, it has degree 0 as a polynomial in y over $\mathbb{R}[x]$. Therefore, $f(x, y)$ is a constant. But then I contains 1 which is impossible, because I contains only polynomials with zero constant term.

3) (a) An obvious check shows that R is closed under $+$, $-$ and $\times$.

(b) R^* consists of fractions with odd numerators and odd denominators. The only irreducible element is 2, up to multiplication by a unit.

(c) The natural inclusion $\mathbb{Z} \to R$ is a homomorphism of rings. By Question 1 (a), the inverse image of an ideal is an ideal. Hence $I \cap \mathbb{Z} = (n)$ for some $n \in \mathbb{Z}$. Write $n = a2^m$, where a is odd, and $m \geq 0$. Then $2^m \in I$ (and $a = \pm 1$). It is clear that I does not contain $2^{m-1}u$, where $u \in R^*$. Thus every non-zero ideal of R has the form $I = (2^m)$ for some $m \geq 0$.

(d) By part (c) the ring R is a PID, hence also a UFD.

4) In lectures we proved that the roots of $x^{p^n} - x = 0$ (in some big field that contains them all) constitute the field $\mathbb{F}_{p^n}$.

If $f(x)$ is a monic irreducible factor of $x^{p^n} - x$ over $\mathbb{F}_p$, then $\mathbb{F}_p[x]/(f(x))$ is isomorphic to a subfield of $\mathbb{F}_{p^n}$ (namely, to $\mathbb{F}_p(\alpha)$, where α is a root of $f(x) = 0$). The degree of this subfield is the degree of $f(x)$, so it equals p^m, where m divides n. (See Q6 of Sheet 4.)

Conversely, if m divides n, then $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$. (It consists of the roots of $x^{p^m} - x = 0$, which divides $x^{p^n} - x = 0$.) Let α be a generator of the multiplicative group of $\mathbb{F}_{p^m}$, which is cyclic by a result in lectures. Then $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$, so the degree of the minimal polynomial of α must be p^m.