MATD01 Fields and Groups

Assignment 4

Solutions

1. Statements (h), (i), (p), and (s) are false (Question 7 gives a counter-example for (h) and (i) and counter-examples for (p) and (s) are given in the hints). All other statements are true.

Simpler counter-example for (h): Take $R = \mathbb{Z}[x]$ and $a = x$. Then x is irreducible but (x) is not maximal (as $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$). Note that this is not a counter example for (i) (why?).

2. Since a and b are relatively prime, there are $r, s \in R$ such that $ar + bs = 1$. Then $car + cbs = c$. Now ab divides both car and cbs (why?), so it also divides c.

3. Consider

$$\Gamma : \mathrm{Hom}(R[x], S) \longrightarrow \mathrm{Hom}(R, S) \times S$$

defined by

$$\Gamma(\phi) = (\phi|_R, \phi(x))$$

(where $\phi|_R$ is the restriction of ϕ to R - see Statement (b) of Question 1). We claim that Γ is a bijection. Indeed, for injectivity note that if $\phi_1, \phi_2 \in \mathrm{Hom}(R[x], S)$ and $\Gamma(\phi_1) = \Gamma(\phi_2)$, then for every $\sum\limits_i r_i x^i \in R[x]$,

$$\phi_1(\sum_i r_i x^i) = \sum_i \phi_1(r_i)\phi_1(x)^i \overset{\text{why?}}{=} \sum_i \phi_2(r_i)\phi_2(x)^i = \phi_2(\sum_i r_i x^i),$$

so that $\phi_1 = \phi_2$. For surjectivity, given $\psi \in \mathrm{Hom}(R, S)$ and $\alpha \in S$ consider the map $\phi : R[x] \to S$ defined by

$$\phi(\sum_i r_i x^i) = \sum_i \psi(r_i)\alpha^i.$$

Then ϕ is a ring homomorphism (as it is the composition of the map $R[x] \to S[x]$ given by $\sum\limits_i r_i x^i \mapsto \sum\limits_i \psi(r_i) x^i$ and the evaluation map $S[x] \to S$ given by $f(x) \mapsto f(\alpha)$). Clearly $\Gamma(\phi) = (\psi, \alpha)$.

4. First we note that $I = \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\}$ consists of all polynomials in $\mathbb{Z}[x]$ whose constant term is even (verify this). Now suppose $I = (h(x))$ for some $h(x) \in \mathbb{Z}[x]$. Then $h(x) \mid 2$ (why?). Since $\mathbb{Z}$ is an integal domain, it follows that $h(x)$ and hence the quotient of 2 in division by $h(x)$ must be of degree zero. Thus $h(x) \in \{\pm 1, \pm 2\}$. If $f(x) = \pm 1$, then $I = \mathbb{Z}[x]$, which is false (as $3 \notin I$). If $f(x) = \pm 2$, then every element of $I = (2)$ must have all coefficients even, which is again false (as $x \in I$).

5. (a) $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. The two polynomials x^2+x+1 and $x^2 - x + 1$ are irreducible over $\mathbb{Q}$ since they don't have any rational roots.

(b) Since ω is a root of $x^6 - 1$, it must be a root of one of the irreducible factors of $x^6 - 1$. Since it is a primitive 6-th root, it cannot be a root of $x - 1, x + 1$, or $x^2 + x + 1$ (reason for the last one: $x^2 + x + 1$ is a factor of $x^3 - 1$). Thus ω must be a root of $x^2 - x + 1$. Being irreducible and monic, thus $x^2 - x + 1$ is the minimal polynomial of ω (over $\mathbb{Q}$)

(c) The kernel is the ideal $(x^2 - x + 1)$. (See last week's Question 3(b).)

(d) Note that $\omega^3 = -1$, as $(\omega^3)^2 = 1$ and $\omega^3 \neq 1$. Thus (by the hypotheses on m, n) we have $f(\omega) = \omega^2 - \omega + 1 = 0$. It follows that $x^2 - x + 1 \mid f(x)$ (why?). The hypotheses on m, n also imply that $f(x)$ must have degree larger than 2.

6. We will outline the procedure, leaving the calculations to the reader. Use Euclid's algorithm to find $h(x), k(x) \in \mathbb{Q}[x]$ such that

$$g(x)h(x) + f(x)k(x) = 1.$$

(Such $h(x)$ and $k(x)$ exist because $g(x)$ is nonzero with $\deg(g(x) < \deg(f(x))$, so that $f(x)$ cannot divide $g(x)$. Since $f(x)$ is irreducible, it follows that $\gcd(f(x), g(x)) = 1$.) Then in the quotient $\mathbb{Q}[x]/(f(x))$,

$$\overline{g(x)} \cdot \overline{h(x)} = 1$$

(why?), so that $\overline{h(x)} = \overline{g(x)}^{\,-1}$. Answer: $\overline{g(x)}^{\,-1} = \overline{x^5 + x^4 + x + 1}$.

7. (a) Let $S = \{a + b\sqrt{-D} : a, b \in \mathbb{Z}\}$. It is clear that $S \subset \mathbb{Z}[\sqrt{-D}]$, so that we need to show that $\mathbb{Z}[\sqrt{-D}] \subset S$. Note that S is closed under taking $\mathbb{Z}$-linear combinations (i.e. if $\alpha, \beta \in S$, then $a\alpha + b\beta \in S$ for every $a, b \in S$). Thus it is enough to show that $\sqrt{-D}^m \in S$ for every $m \geq 0$. We show this by induction on m. The base case $m = 0$ is clear. Suppose $\sqrt{-D}^m \in S$ for some $m \geq 0$. Thus there are integers a, b such that $\sqrt{-D}^m = a + b\sqrt{-D}$. Then

$$\sqrt{-D}^{m+1} = \sqrt{-D}\sqrt{-D}^m = \sqrt{-D}(a + b\sqrt{-D}) = -Db + a\sqrt{-D} \in S.$$

(b) Define the function $N : \mathbb{Z}[\sqrt{-D}] \to \mathbb{Z}$ (called the norm function) by

$$N(a + b\sqrt{-D}) = a^2 + Db^2 \qquad (a, b \in \mathbb{Z}).$$

Note that here we are using the fact that any element of $\mathbb{Z}[\sqrt{-D}]$ can be *uniquely* expressed in the form $a + b\sqrt{-D}$ with $a, b \in \mathbb{Z}$. Indeed, 1 and $\sqrt{-D}$ are linearly independent over $\mathbb{Q}$ (i.e. $a + b\sqrt{-D} = 0$ for $a, b \in \mathbb{Q}$ implies $a, b = 0$), for $\sqrt{-D}$ is not rational. We leave it to the reader to check that $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[\sqrt{-D}]$ (just write $\alpha = a + b\sqrt{-D}$ and $\beta = c + d\sqrt{-D}$ and compute both sides). Also it is clear that $N(\alpha) \geq 0$ for every $\alpha \in \mathbb{Z}[\sqrt{-D}]$, and $N(\alpha) = 0$ if and only if $\alpha = 0$.

Now suppose $\alpha \in \mathbb{Z}[\sqrt{-D}]^\times$. Then $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Since N takes values in the non-negative integers, it follows that $N(\alpha) = 1$. Conversely, if $\alpha = a + b\sqrt{-D} \in \mathbb{Z}[\sqrt{-D}]$ has norm 1, then

$$1 = N(\alpha) = a^2 + Db^2 = (a + b\sqrt{-D})(a - b\sqrt{-D}),$$

so that $\alpha \in \mathbb{Z}[\sqrt{-D}]^\times$. Thus the units of $\mathbb{Z}[\sqrt{-D}]$ are exactly the elements of norm 1.

Since $D > 0$, the only solutions $(a, b) \in \mathbb{Z}^2$ to $a^2 + Db^2 = 1$ are $(a, b) = (\pm 1, 0)$ if $D > 1$ and $(a, b) = (\pm 1, 0), (0, \pm 1)$ if $D = 1$. Thus the only elements of norm 1 (= units) in $\mathbb{Z}[\sqrt{-D}]$ are ± 1 if $D > 1$ and $\pm 1, \pm i$ if $D = 1$.

Remark: Let $D < 0$ with $-D$ a non-square (note: if $-D$ is a square then $\mathbb{Z}[\sqrt{-D}] = \mathbb{Z}$). One defines the norm function similarly. This time $N(a + b\sqrt{-D}) = a^2 + Db^2$ can be negative. The units of $\mathbb{Z}[\sqrt{-D}]$ are exactly the elements of norm ± 1. One can show that the group of units of $\mathbb{Z}[\sqrt{-D}]$ contains an infinite cyclic group in this case. (The equation $a^2 + Db^2 = 1$ with $D < 0$ has infinitely many solutions. Read about Pell's equation on Wikipedia.)

(c) Firstly, 2 is not a unit by (b). Now suppose $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}$. Taking norms we see that

$$(a^2 + 5b^2)(c^2 + 5d^2) = 4.$$

Since $2 \neq k^2 + 5\ell^2$ for any $k, \ell \in \mathbb{Z}$ (only need to look at $\ell = 0$, $k = \pm 1$, as otherwise $k^2 + 5\ell^2 > 2$), either we must have $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$. This implies that either $a + b\sqrt{-5}$ or $c + d\sqrt{-5}$ is a unit.

(d) For the first assertion note that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. For the second assertion, note that if $2 \mid a + b\sqrt{-5}$ then both a and b must be even (why?).

(e) No. In a PID, the ideal generated by an irreducible element is prime. We saw above that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but that the ideal (2) is not prime (as it contains $(1 + \sqrt{-5})(1 - \sqrt{-5})$, but it neither contains $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$).