
620-321 Algebra, Semester 1, 2009
Answers to Problem Sheet 3

1. By definition, $\Phi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \varphi(a_i) x^i$. Let $f, g \in R[x]$ be given by $f = \sum_{i=0}^n a_i x^i$ and $g = \sum_{j=0}^n b_j x^j$. To check that Φ is a homomorphism:

$$\begin{aligned} \Phi(f + g) &= \Phi\left(\sum_{i=0}^n a_i x^i + \sum_{j=0}^n b_j x^j\right) = \Phi\left(\sum_{i=0}^n (a_i + b_i) x^i\right) = \sum_{i=0}^n \varphi(a_i + b_i) x^i \\ &= \sum_{i=0}^n (\varphi(a_i) + \varphi(b_i)) x^i = \sum_{i=0}^n \varphi(a_i) x^i + \sum_{i=0}^n \varphi(b_i) x^i = \Phi(f) + \Phi(g) \end{aligned}$$

$$\begin{aligned} \Phi(fg) &= \Phi\left(\sum_{i=0}^n a_i x^i \sum_{j=0}^n b_j x^j\right) = \Phi\left(\sum_{k=0}^{2n} \left(\sum_{i=0}^n a_i b_{k-i}\right) x^k\right) = \sum_{k=0}^{2n} \varphi\left(\sum_{i=0}^n a_i b_{k-i}\right) x^k = \sum_{k=0}^{2n} \left(\sum_{i=0}^n \varphi(a_i b_{k-i})\right) x^k \\ &= \sum_{k=0}^{2n} \left(\sum_{i=0}^n \varphi(a_i) \varphi(b_{k-i})\right) x^k = \sum_{i=0}^n \varphi(a_i) x^i \sum_{j=0}^n \varphi(b_j) x^j = \Phi(f) \Phi(g) \end{aligned}$$

3. (b) $1(18x^2 - 12x + 48)$ (c) $2(x^2 - 5x + 3)$
 4. (a) $2.2.(x^2 - x + 2)$ (b) $4x^2 - 4x + 8$ (c) $(4x + 2)(x + 4)$
 5. (a) Since p is a unit, there exists $v \in D$ such that $vp = 1$.

$$\begin{aligned} q|p &\implies p = aq \quad \text{for some } a \in D \\ &\implies 1 = vaq \\ &\implies q \text{ is a unit (with inverse } va) \end{aligned}$$

- (b) We know that $p = aq$ for some $a \in D$. Since p is irreducible, one of q or a is a unit. Suppose that q is not a unit. Then a is a unit, and $q = a^{-1}p$. So $q|p$ and therefore p and q are associates.
 (c) It is sufficient to show that p irreducible implies q irreducible. So suppose that p is irreducible. Clearly, q is not a unit, since p , being irreducible, is not a unit. Also, p non-zero implies that q is non-zero. We have that $p = aq$ for some $a \in D$ since $q|p$. Then

$$\begin{aligned} q = xy &\implies p = (ax)y \\ &\implies \text{one of } ax \text{ or } y \text{ is a unit, since } p \text{ irreducible} \\ &\implies \text{one of } a \text{ or } y \text{ is a unit (using (a))} \end{aligned}$$

So q is irreducible.

7. The (evaluation) map $\varphi : R[x] \rightarrow R$ defined by $f \mapsto f(a)$ is a ring homomorphism whose kernel is $\ker(\varphi) = \{f \in R[x] \mid f(a) = 0\}$. This kernel contains the principal ideal $(x - a)$. Modulo this ideal every polynomial f is congruent to an element of R , namely $f(a)$. So $(x - a)$ generates the kernel. The result then follows from the first isomorphism theorem.
 8. Consider the map $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Q}$ which sends x to $\frac{1}{2}$ and is the identity on \mathbb{Z} . The kernel consists of those polynomials f such that $f(\frac{1}{2}) = 0$. It suffices to show that any such polynomial satisfies $(2x - 1)|f(x)$. In $\mathbb{Q}[x]$ we know that if $f(\frac{1}{2}) = 0$ then $(x - \frac{1}{2})|f(x)$ or equivalently $(2x - 1)|f(x)$ in $\mathbb{Q}[x]$. But both lie in $\mathbb{Z}[x]$, so by results from lectures, this is also true in $\mathbb{Z}[x]$ which is the desired result.

10. Note that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ and is contained in the kernel of φ . Since $\mathbb{R}[x]$ is a PID and $x^2 + 1$ is irreducible, it follows that $x^2 + 1$ must generate the kernel.
11. First observe that $1 + \sqrt{2}$ satisfies $x^2 - 2x - 1 = 0$ and thus $x^2 - 2x - 1$ is in the kernel I of φ . If $f \in I$, then we can write $f = (x^2 - 2x - 1)q + r$ where $r = 0$ or the degree of r is ≤ 1 . Substituting $1 + \sqrt{2}$ we have $r(1 + \sqrt{2}) = 0$. Since r has coefficients in \mathbb{Q} , this is impossible unless $r = 0$. Thus $(x^2 - 2x - 1) \mid f$ in $\mathbb{Q}[x]$ and hence in $\mathbb{Z}[x]$.
12. The ideal $aR + bR$ is equal to (d) for some d , since R is a PID. Note that $d = ar + bs$ for some $r, s \in R$, and that therefore any common divisor of a and b divides d . Also, d itself is a common divisor since $(a) \subseteq (d)$ and $(b) \subseteq (d)$.
13. Since R is a PID, we know $(d) = aR + bR$ so $d = as + bt$ for some $s, t \in R$. Now this equation also holds in S and the element d still divides both a and b . If $e \in S$ also divides both a and b , say $a = ea_1$ and $b = eb_1$ then we have $d = as + bt = ea_1s + eb_1t = e(a_1s + b_1t)$ and thus $e \mid d$. Hence d is also the gcd of a and b in S .