392 Homework 3 solutions

- Suppose that $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$. Let $\alpha \in \mathbb{Q}$ be a root of $f(x)$. Show that $\alpha \in \mathbb{Z}$. (*Hint.* Let $\alpha = \frac{a}{b}$ with $GCD(a,b) = 1$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Now substitute α in for x and multiply through by b^{n-1}.)

  Solution. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with each $a_i \in \mathbb{Z}$. Let $\alpha = a/b$ be a rational root written in lowest terms. Then,
$$\frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + a_1\frac{a}{b} + a_0 = 0.$$
  Multiply through by b^{n-1} to get
$$\frac{a^n}{b} + a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1} = 0.$$
  All terms after the first one are integers, so $\frac{a^n}{b} \in \mathbb{Z}$. But a and b had no common divisors, so this implies that $b = 1$. Hence $\alpha = a/b$ was already an integer.
- Exercises 4.1 1,2,3,4(b)(c),5,7.
  1 Let $\phi : R \to S$ be a ring homomorphism. Prove that $\phi(-a) = -\phi(a)$. Is the zero function $a \mapsto 0$ a ring homomorphism?
  Solution. $\phi(-a) + \phi(a) = \phi(-a + a) = \phi(0) = 0$. *Hence,* $\phi(-a) = -\phi(a)$. *The zero function is NOT a ring homomorphism because 1 maps to 0 and $1 \neq 0$ (by the axioms of 'ring' that we are using that is a requirement). So $\phi(1_R) \neq \phi(1_S)$.*
  2 Consider $\phi : \mathbb{Z}_2 \to \mathbb{Z}_6$ mapping $\bar{0}$ to $\bar{0}$ and $\bar{1}$ to $\bar{3}$. Show this is additive and multiplicative but does not map 1 to 1.
  Solution. Obviously it doesn't map 1 to 1. For additive, we need to check just 4 things:
$$\phi(\bar{0} + \bar{0}) = \phi(\bar{0}) = \bar{0} = \bar{0} + \bar{0} = \phi(\bar{0}) + \phi(\bar{0}),$$
$$\phi(\bar{0} + \bar{1}) = \phi(\bar{1}) = \bar{3} = \bar{0} + \bar{3} = \phi(\bar{0}) + \phi(\bar{1}),$$
$$\phi(\bar{1} + \bar{0}) = \phi(\bar{1}) = \bar{3} = \bar{3} + \bar{0} = \phi(\bar{1}) + \phi(\bar{0}),$$
$$\phi(\bar{1} + \bar{1}) = \phi(\bar{0}) = \bar{0} = \bar{3} + \bar{3} = \phi(\bar{1}) + \phi(\bar{1}).$$
  Similarly for multiplicative we check
$$\phi(\bar{0}.\bar{0}) = \phi(\bar{0}) = \bar{0} = \bar{0}.\bar{0} = \phi(\bar{0}).\phi(\bar{0}),$$
$$\phi(\bar{0}.\bar{1}) = \phi(\bar{0}) = \bar{0} = \bar{0}.\bar{3} = \phi(\bar{0}).\phi(\bar{1}),$$
$$\phi(\bar{1}.\bar{0}) = \phi(\bar{0}) = \bar{0} = \bar{3}.\bar{0} = \phi(\bar{1}).\phi(\bar{0}),$$
$$\phi(\bar{1}.\bar{1}) = \phi(\bar{1}) = \bar{3} = \bar{3}.\bar{3} = \phi(\bar{1}).\phi(\bar{1}).$$

  3 (a) Prove that if $I \subseteq R$ is an ideal and $1 \in I$ then $I = R$. (b) Prove that $a \in R$ is a unit if and only if $(a) = R$. (c) Prove that the only ideals in a ring R are (0) and R if and only if R is a field.

Solution. (a) If $1 \in I$ then for any $a \in R$, we have that $a = a.1 \in I$ since I is extra closed under multiply. Hence, $R \subseteq I$. Since $I \subseteq R$ already, this means that $I = R$.
(b) Suppose $a \in R$ is a unit. Then, $1 = aa^{-1} \in (a)$. So by the first part, $(a) = R$.
Conversely, suppose that $(a) = R$. Then, $1 \in (a)$, i.e. 1 is a multiple of a. Hence there is some $b \in R$ such that $1 = ab$ and a is a unit.
(c) Suppose R is a field and $I \subseteq R$ is a non-zero ideal. Then take any $0 \neq a \in I$. It is a unit. So $1 = aa^{-1}$ also belongs to I. So $I = R$ by the first part. Thus in a field, the only ideals are (0) and the whole thing.
Conversely suppose that R is a ring such that the only ideals are (0) and the whole thing. Take any $0 \neq a \in R$. Then (a) is a non-zero ideal, so it must be all of R. So by the second part, a is a unit. Hence R is a field.

4(b) Find all ideals in $\mathbb{Z}_7$.
Solution. It is a field so by question 3, the only ideals are (0) and the whole thing.

4(c) Find all ideals in $\mathbb{Z}_6$.
Solution. The non-units in $\mathbb{Z}_6$ are $\bar{0}, \bar{2}, \bar{3}, \bar{4}$. If an ideal contains anything else, it is the whole thing. So the ideals are $(0), \mathbb{Z}_6$, $(\bar{2})$ and $(\bar{3})$.

5 Let $I = (f(x))$ and $J = (g(x))$ be ideals in $F[x]$. Prove that $I \subseteq J$ if and only if $g(x)|f(x)$. Then list all the ideals of $\mathbb{Q}[x]$ containing $(x^2 + x - 1)^3(x - 3)^2$.
Solution. Suppose $(f(x)) \subseteq (g(x))$. Then $f(x) \in (g(x))$. So $f(x)$ is a multiple of $g(x)$, i.e. $g(x)|f(x)$.
Conversely suppose $g(x)|f(x)$. Then $f(x)$ is a multiple of $g(x)$, hence any multiple of $f(x)$ is also a multiple of $g(x)$. This shows that $(f(x)) \subseteq (g(x))$.
Finally suppose that I is an ideal of $\mathbb{Q}[x]$ containing $(x^2 + x - 1)^3(x - 3)^2$. By Proposition 1.2, $I = (g(x))$ for some monic $g(x) \in \mathbb{Q}[x]$. By the first part, $g(x)|(x^2+x-1)^3(x-3)^2$. Hence $g(x) = (x^2 + x - 1)^a(x - 3)^b$ for $0 \leq a \leq 3$ and $0 \leq b \leq 2$, and $I = (g(x))$. These are the only 12 possibilities for the ideal I.

7 Find all ring homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$.
Solution. Suppose $\phi : \mathbb{Z} \to \mathbb{Z}$ is a ring homomorphism. Then $\phi(1) = 1$. Hence, $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2$. Similarly, $\phi(3) = \phi(2+1) = \phi(2)+\phi(1) = 2+1 = 3$. Continuing in this way you see that $\phi(n) = n$ for all $n > 0$. Also $\phi(0) = 0$ and $\phi(-n) = -\phi(n)$. Hence, $\phi(n) = n$ for all $n \in \mathbb{Z}$. Therefore: the only homomorphism $\mathbb{Z} \to \mathbb{Z}$ is the identity map.