Advanced Algebra H.W(I)

1. Let Q denote the ring of real quarternions. For $x = a+bi+cj+dk \in Q$ the *conjugate* of x is $x^* := a - bi - cj - dk$.
   (a) Show $(a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2$ for $a, b, c, d \in \mathbb{R}$.
   (b) Suppose $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2 \in \mathbb{Z}$. Show that there exist $a, b, c, d \in \mathbb{Z}$ such that
   $$(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) = a^2+b^2+c^2+d^2.$$
   (c) Suppose $u \in \mathbb{Z}$ and $2u = a^2+b^2+c^2+d^2$ for some $a, b, c, d \in \mathbb{Z}$. Then $u = e^2+f^2+g^2+h^2$ for some $e, f, g, h \in \mathbb{Z}$. (Hint. Try $e = (a+b)/2$ and $f = (a-b)/2$.)

   Solution:
   (a) Since $ij = -ji, jk = -kj, ki = -ik$ and $i^2 = j^2 = k^2 = -1$, $(a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2$.
   (b) $i^* = -i, j^* = -j, k^* = -k.x = a_1+b_1i+c_1j+d_1k$, then $x^* = a_1 - b_1i - c_1j - d_1k$.
   Let $x = a_1+b_1i+c_1j+d_1k$, $y = a_2+b_2i+c_2j+d_2k$,
   Then $(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) = xx^*(a_2^2+b_2^2+c_2^2+d_2^2) = x(a_2^2+b_2^2+c_2^2+d_2^2)x^* = x(yy^*)x^* = (xy)(y^*x^*) = (xy)(xy)^*$.
   $\exists a, b, c, d$ s.t $xy^* = a+bi+cj+dk$.
   Then $(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) = a^2+b^2+c^2+d^2$.
   (c) Let $e = \frac{a+b}{2}$, $f = \frac{aub}{2}$. Then $e^2+f^2 = \frac{1}{2}(a^2+b^2)$. Similarly to g,h.
   We want to show e, f, g, h are integers.
   We only claim that a, b, c, d have even odd numbers. It's easy to see.

2. Let R be a commutative ring of prime characteristic p.
   (a) Show that
   $$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$
   for all $a, b \in \mathbb{N}$.
   (b) Show that the map $f : R \to R$ given by $f(a) = a^p$ is a homomorphism of rings.

   Solution:
   (a) By induction on n.
   $n = 1$, $(a+b)^p = \sum_{i=0}^{i=p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$.
   $n = k$ is true. Consider $n = k+1$.
   $(a+b)^{p^{k+1}} = ((a+b)^{p^k})^p = ((a^{p^k} + b^{p^k}))^p = a^{p^{(k+1)}} + b^{p^{(k+1)}}$.
   (b) $f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$, and $f(ab) = (ab)^p = (a^p)(b^p) = f(a)f(b)$. Hence f is a homomorphism.

3. An element a of a ring is *nilpotent* if $a^n = 0$ for some n. Prove that in a commutative ring $a+b$ is nilpotent if a and b are. Show that this result may be false if R is not commutative.

Solution:

(a) Since a, b are nilpotent, $\exists s, t$: integers s.t $a^s = 0$ and $b^s = 0$.

$(a+b)^{s+t} = \sum_{i=0}^{s+t} \binom{s+t}{i} a^i b^{s+t-i} = 0$. $\because$ if $i \geq s$, then $a^i = 0$. if $i < s$, then $s + t - i > t$ this implies $b^{s+t-i} = 0$.

(b)

$$a = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$a^2 = b^2 = 0$, a, b are nilpotent.

$$a + b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$(a+b)^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : \text{not nilpotent.}$$

4. In a ring R show that the following conditions are equivalent.
   (a) R has no nonzero nilpotent elements.
   (b) If $a \in R$ and $a^2 = 0$, then $a = 0$.

Solution:
$(a) \Rightarrow (b)$ Trivial.
$(b) \Rightarrow (a)$ Suppose $\exists b \neq 0$ is nilpotent. Then $\exists k$: smallest positive integer s.t $b^k = 0$
Case 1: if k is even. Let $k = 2d, d \geq 1$. $b^k = b^{2d} = ((b^d))^2 = 0$. By (b), $b^d = 0$, a contradiction.
Case 2: if k is odd. Let $k = 2d+1, d \geq 1$. $b^k = 0$. $b^k \cdot b = b^{2d+2} = ((b^{d+1}))^2 = 0$. By (b), $b^{d+1} = 0$, a contradiction.

5. Give an example of a nonzero homomorphism $f : R \to R'$ of rings such that $f(1) \neq 1'$. Is it possible $1'$ in the image of f?

Solution:

(a) $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $f(n) = (n, 0)$. $\forall n \in \mathbb{Z}$
(b) N0. Suppose $\exists a \in R$ s.t $f(a) = 1'$. Then $1' = f(a) = f(1 \cdot a) = f(1) \cdot f(a) = f(1) \cdot 1' = f(1)$, a contradiction.

6. Find a nonidentity homorphism ϕ of $\mathbb{R}$ into $\mathbb{R}$.

Solution:
Define $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(a) = 0, \forall a \in \mathbb{R}$.

7. Show that the only ring homomorphism ϕ of $\mathbb{R}$ into $\mathbb{R}$ with $\phi(1) = 1$ is the identity.

Solution:
$\phi : \mathbb{R} \to \mathbb{R}$ s.t $\phi(1) = 1$.
$\forall k \in \mathbb{N}, \phi(k) = \phi(1+1+\cdots+1) = \phi(1)+\phi(1)+\cdots\phi(1) = 1+1+\cdots+1 = k$.
$0 = \phi(0) = \phi(k-k) = \phi(k) + \phi(-k) \Rightarrow \phi(-k) = -k$.
$\forall a \in \mathbb{Z}, 1 = \phi(a \cdot \frac{1}{a}) = \phi(a) \cdot \phi(\frac{1}{a}) = a \cdot \phi(\frac{1}{a}) \Rightarrow \phi(\frac{1}{a}) = \frac{1}{a}$.
$\forall a, b \in \mathbb{Z}, \phi(\frac{b}{a}) = \phi(b) \cdot \phi(\frac{1}{a}) = b \cdot \frac{1}{a} = \frac{b}{a}$.
$\forall x \in \mathbb{R}, \phi(x^2) = \phi(x) \cdot \phi(x) = (\phi(x))^2$.
$\forall x \in \mathbb{R}^+, \phi(x) = \phi(\sqrt{x})^2 > 0$.
$\forall a, b \in \mathbb{R} and a - b > 0, \phi(a-b) = \phi(a) - \phi(b) > 0$, This implies $\phi(a) > phi(b)$.
$\forall x \in \mathbb{R}$. Suppose $\phi(a) = c$, where $a \neq c$. W.L.O.G, suppose $a > c$. Then $\exists r \in \mathbb{Q}$ s.t $a > r > c$. $c = \phi(a) > \phi(r) = r > c$, a contradiction. Hence $\phi(a) = a, \forall a \in \mathbb{R}$.