1. Prove proposition 6.6 from the Module 6 notes.

   Proposition 6.6 (Properties of Multiplication in Rings). Let a, b, c belong to a ring R. Then

   (a) $a0 = 0a = 0$ To prove $a0 = 0$ Since $a0 = (0+0)a \implies a0 = a0+a0$ by the left distributive law. Implies $0 + a0 = a0 + a0$ since 0 is the additive identity so $0 + a0 = a0$ hence $a0 = 0$. Now for $0a = 0$. $0a = (0+0)a \implies 0+0a = 0a+0a$ by the right distributive law. Hence $0 = 0a$ by cancellation.

   (b) $a(-b) = (-a)(b) = -(ab)$ Since a0=0, a(b+(-b))=0 since -b is the additive inverse of b. ab+a(-b)=0 by the left distributive law. a(-b) is then the additive inverse of ab therefore a(-b)=-ab. b(-a)=-ab follows from without loss of generality of a and b.

   (c) $(-a)(-b) = (ab)$ Since a0=0 if R is a ring then $-a \in R$ so we have (-a)0=0. Then we have -a(b+(-b))=0 because b is the additive inverse of -b. Implies -ab+(-a)(-b)=0 by the left distributive law. (-a)(-b) is the additive inverse of -(ab) then. As (ab) is the additive inverse of -(ab) we havve that additive inverses are unique so we can say (-a)(-b) = ab.

   (d) $a(b-c) = ab-ac$ and $(b-c)a = ba-ca$ a(b-c)=a(b+(-c))=ab+a(-c) by the left distributive law. Implies this is equal to ab+-(ac) using part b). So ab-ac is equivelence. Similarly (b-c)a=(b+(-c))a=ba+(-c)a right distributive law. =ba-ca using part b) so ba+(-c)a=ba-ca.

   If R has a unity element 1, then

   (e) $(-1)a = -a$ Consider (-1)a+a=-1a+1a as 1a =a. Then byu the right distributive law -1a+a=(-1+1)a=-1a+a=0a then as a0=0 we have (-1+1)a=0 so as -a is the additive inverse of a -a=(-1)a.

   (f) $(-1)(-1) = 1$ From part c) we have (-a)(-b)=(ab) therefore (-1)(-1)=1*1=1

2. Suppose that a and b belong to a commutative ring R with unity. If a is a unit and $b^2 = 0$, show that $a + b$ is a unit. Consider $(a - b)(a + b) = a^2 - b^2$ as R is a commutative ring. Since $b^2 = 0$ we have $(a + b)(a - b) = a^2 + 0$ SDince a is a unit we can write $(a + b)(a^{-1} - ba^{-2}) = 1$ so $a + b$ is an invertible element. Hence a+b is a unit.

3. The set $\mathbb{R}[x]$ of all polynomials in the variable x with real coefficients under ordinary addition and multiplication is a commutative ring.

   (a) What is unity in $\mathbb{R}[x]$? What are the units of $\mathbb{R}[x]$? Explain. f(x)=1 and f(x)=-1. Unity in $\mathbb{R}[x]$ means $I \in R$ such that $Ir = r = rI \forall r \in R$.

   (b) Show that $\mathbb{Z}[x]$ forms a subring of R, where $\mathbb{Z}[x]$ is the subset of $\mathbb{R}[x]$ with integer coefficients. Let $a \in \mathbb{Z}[x]$ and $b \in \mathbb{Z}[x]$ then $a - b \in \mathbb{Z}[x]$ because the integers are closed under subtraction. Now consider ab. The product of integers is always an integer so $ab \in \mathbb{Z}[x]$. So it is closed under multiplication. Thus $\mathbb{Z}[x]$ forms a subring.

4. An element a in a ring R with unity is called *nilpotent* if there exists a positive integer n such that $a^n = 0$.

   (a) Give an example of a nontrivial ring R and a nonzero nilpotent element a. $R = \mathbb{Z}_4$ where $a = 2$.

   (b) Show that for an arbitrary ring R with unity, if a is a nilpotent element of R, then $1 - a$ is a unit. (Hint: Consider $(1 - a)(1 + a + a^2 + \cdots + a^{n-1})$.) Let a be a nilpoint element in an arbitrary ring R with unity. If the index of a is n then $a^n = 0$ but $a^r \neq 0$ for

$r < n$ Now $(1 + a + a^2 + \cdots + a^{n-1}) = frac1 - a^n 1 - a$. As $1 \in R$ and $a \in R$ then $(1 + a + a^2 + \cdots + a^{n-1}) \in R$ so $(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1 - a^n$ so $(1 - a)$ is a unit. Here $(1 + a + a^2 + \cdots + a^{n-1})$ is the inverse of $(1 - a)$.

(c) Show that for a *commutative* ring R with unity, the set of nilpotent elements forms a subring. Let S be the set of all nilpotent elements of a commutative ring R with unity. Let $a, b \in S$ So $a^m = b^n = 0$ for some $m, n \in \mathbb{Z}$. Then $a + b \in S$ since $(a + b)^{m+n} = 0$. And $ab \in S$ since $(ab)^{min(m,n)} = 0$. Therefore S is a subring of R.

5. Let R and S be commutative rings. Prove that (a, b) is a zero-divisor in $R \oplus S$ if and only if a or b is a zero-divisor or exactly one of a or b is 0. Let (a, b) be a zero divisor of $R \oplus S$. Then there exists a nonzero element $(c, d), c \in R, d \in S$ such that $(ac, bd) = (0, 0)$. Case 1: $c \neq 0 d \neq 0.$. If $a = 0, b \neq 0 \implies bd = 0$ so b is a zero divisor. If $a \neq 0, b = 0 \implies ac = 0$ so a is a zero divisor. If $a \neq 0, b \neq 0 \implies ac = 0, bd = 0$ hence a and b are zero divisors. Case 2: WLOG $c \neq 0, d = 0$. First if $a = 0, b \neq 0 \implies bd = 0$ so b is a zero divisor. If $a \neq 0, b = 0 \implies (ac, bd) = (0, 0)$. If $a \neq 0, b \neq 0 \implies bd = 0$ hence b is a zero divisor. Case 3 is case 2 wlog $c = 0, d \neq 0$. Now for the converse. Let a be a zero divisor. Then $\exists c \neq 0$ such that ac=0. Now (a,b)(c,d)=(0,0) so (a,b) is a zero divisor. Then wlog consider b as a zero divisor. then $\exists d \neq 0$ such that (a,b)(0,d)=(0,0) so (a,b) is a zero divisor. Now for the third case let exactly one of a and b be zero. Then (a,b)(c,0)=(0,0) when a=0. Now wlog consider when b=0. Then (a,b)(0,d)=(0,0). In all cases it follows that (a,b) is a zero divisor.