1. Give precise and complete mathematical definitions of the following:

   (a) (5 points) A unit in a ring $R$ is . . .

   **Solution:** an element with a multiplicative inverse. (Equivalently, an element that divides 1.)

   (b) (5 points) An element in a ring $R$ is irreducible if . . .

   **Solution:** the element is nonzero, not a unit, and in any factorization of that element as $ab$, either $a$ or $b$ is a unit (i.e., every factorization of the element is trivial).

2. (15 points) Suppose $R$ is a commutative ring and $u$ and $v$ are units in $R$. Show that $uv$ is also a unit. Is this always true if $R$ is not commutative?

   **Solution:** Suppose $u$ and $v$ are units in $R$ with multiplicative inverses $u^{-1}$ and $v^{-1}$, respectively. Then
   
   $$(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = uu^{-1} = uv^{-1} = 1.$$
   
   So the element $v^{-1}u^{-1}$ is a multiplicative inverse for $uv$, showing that $uv$ is a unit.

   This holds even if $R$ is noncommutative; we used the associative property of the multiplication in $R$, but not commutativity. (In a commutative ring, we can write the inverse of $uv$ as $u^{-1}v^{-1}$, of course, but in a commutative ring that’s the same as $v^{-1}u^{-1}$.)

3. (20 points) Suppose that $K$ is an infinite field and $f(x), g(x) \in K[x]$ are such that $f(a) = g(a)$ for all $a \in K$. Prove that $f(x) = g(x)$ in $K[x]$. (Hint: Think about the roots of $f(x) - g(x)$.)

   **Solution:** Consider the polynomial $f(x) - g(x)$. This is a polynomial in $K[x]$ of some degree, say $n$. (In fact $f(x) - g(x)$ has degree at most $\max(\deg f, \deg g)$. The degree could be strictly lower than the maximum of the degrees of $f$ and $g$ if they have the same degree and the same leading coefficient, so the leading term disappears when we subtract.)

   We proved that a polynomial of degree $n \geq 0$ in $K[x]$ can have at most $n$ distinct roots in $K$. But $f(a) = g(a)$ for all $a \in K$ and $K$ is infinite, so $f(x) - g(x)$ has infinitely many roots in $K$. That implies that $f(x) - g(x)$ can’t have nonnegative degree and therefore must be the 0 polynomial in $K[x]$. So $f(x) = g(x)$.

   [Note that this doesn’t hold if $K$ if finite. For example, all the elements $a$ of $\mathbb{Z}_5$ satisfy $a^5 - a = 0$ (check this) and so are roots of the polynomial $f(x) = x^5 - x$. If we take $g(x)$ to be the constant polynomial 0, then $f(x)$ and $g(x)$ have the same roots. But $f(x) \neq g(x)$. In fact, $f(x)p(x)$, for any nonzero $p(x) \in \mathbb{Z}_5[x]$ will obviously have all five elements of $\mathbb{Z}_5$ as roots, so there are infinitely many different polynomials in $\mathbb{Z}_5[x]$ with the same roots.

   More generally, any finite field has $p^n$ elements, for some prime $p$ and some positive integer $n$, and in such a field, every element will satisfy $a^{p^n} - a = 0$ (though we’re not in position to prove this right now). So this same kind of construction will work for any finite field—there’s a nonzero polynomial $f(x)$ for which every element of the field is a root.]
4. (20 points) Let $a$ and $b$ be integers. Show that a nonnegative common divisor $d$ of $a$ and $b$ is the gcd of $a$ and $b$ if and only if $c \mid d$ for every common divisor $c$ of $a$ and $b$.

**Solution:** First suppose that $d = (a, b)$ and $c$ is a common divisor of $a$ and $b$. We know that there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. Since $c$ divides both $a$ and $b$, it divides $ax + by$, so $c$ divides $d$.

Conversely, suppose that $d$ is a nonnegative common divisor of $a$ and $b$ with the property that, for any common divisor $c$ of $a$ and $b$, $c$ divides $d$. To show that $d$ is the greatest common divisor of $a$ and $b$, we must show that $d$ is greater than any other common divisor $c$. If $c$ is negative, we know that $d > c$ since $d$ is nonnegative. If $c$ is positive, the fact that $c \mid d$ says that $qc = d$ for some positive integer $q$. But $q \geq 1$ implies $qc \geq c$, so $d = qc$ is greater than or equal to $c$.

5. Let $R$ be a ring. Recall that a zero-divisor in $R$ is a nonzero element $r \in R$ such that there is a nonzero element $s \in R$ with $rs = 0$.

(a) (6 points) Give an example of zero divisors in a ring.


(b) (7 points) Suppose $R$ has no zero divisors (such an $R$ is called an integral domain, or just a domain). Show that the cancellation property holds in $R$: For all $a, b, c \in R$, if $a \neq 0$ and $ab = ac$, then $b = c$.

**Solution:** Suppose $R$ is an integral domain and $a, b, c \in R$ with $a \neq 0$ and $ab = ac$. Then $ab - ac = 0$ and the distributive property tells us that $a(b - c) = 0$. Since $a$ is not a zero divisor (because $R$ has no zero divisors), we must have $b - c = 0$. Hence $b = c$.

(c) (7 points) Suppose $f(x), g(x) \in \mathbb{Q}[x]$ and let $p(x) = f(x)g(x)$. Suppose that $a \in \mathbb{Q}$ is a root of $p(x)$. Show that $a$ is a root of $f(x)$ or $g(x)$.

**Solution:** Observe that $\mathbb{Q}$ is an integral domain: if $a \neq 0$ and $ab = 0$, then $0 = a^{-1}0 = a^{-1}ab = b$. (No unit can be a zero divisor, and all the nonzero elements of a field are units. You actually showed that any field is an integral domain in an exercise.)

So if $p(a) = 0$, we have $f(a)g(a) = 0$. Since $f(a)$ and $g(a)$ are elements of $\mathbb{Q}$ with $f(a)g(a) = 0$, it must be the case that one of $f(a)$ and $g(a)$ is 0. So $a$ is a root of $f(x)$ or $g(x)$.

6. (a) (5 points) Give an example of a polynomial $f(x) \in \mathbb{Q}[x]$ that is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$. Justify your answer.

**Solution:** Take $f(x) = x^2 - 2$. If this has a nontrivial factorization, that must be the product of two degree-1 polynomials in $\mathbb{Q}[x]$. But then $f(x)$ would have roots in $\mathbb{Q}$, and we know the roots of $f(x)$ are $\pm \sqrt{2} \notin \mathbb{Q}$. In $\mathbb{R}[x]$, of course, $x^2 - 2$ factors as $(x - \sqrt{2})(x + \sqrt{2})$, so $f(x)$ is reducible in $\mathbb{R}[x]$.

(b) (5 points) Give an example of a polynomial $g(x) \in \mathbb{R}[x]$ that is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$. Justify your answer.
Solution: Take $g(x) = x^2 + 1$. This is irreducible in $\mathbb{R}[x]$, again since any nontrivial factorization would have two degree-1 factors which would mean $g(x)$ had a root in $\mathbb{R}$. Since the square of any real number is nonnegative, that’s impossible. But $g(x) = (x - i)(x + i)$ in $\mathbb{C}[x]$, so $g(x)$ is reducible in $\mathbb{C}[x]$.

(c) (5 points) Give an example of a polynomial $h(x) \in \mathbb{C}[x]$ that is irreducible in $\mathbb{C}[x]$. Justify your answer

Solution: The Fundamental Theorem of Algebra says that every polynomial in $\mathbb{C}[x]$ can be factored as a product of degree-1 polynomials in $\mathbb{C}[x]$. So any irreducible polynomials have degree 1. On the other hand, any degree-1 polynomial is irreducible, since it can’t have a factorization in which both factors have degree strictly less than 1. So we can take $g(x) = x$, for example.

The next two questions are for extra credit. Don’t attempt them until you’ve done everything you can on the other problems, since I will give very little partial credit on them.

7. (10 points Extra Credit) Suppose that $R$ is an integral domain ($R$ has no zero divisors). Show that if $a, b \in R$ are two elements that divide each other, then $b = ua$ for some unit $u$.

Solution: Suppose that $a$ and $b$ are elements of the integral domain $R$ such that $a$ divides $b$ and $b$ divides $a$. So there exist elements $u, v \in R$ with $ua = b$ and $vb = a$. Then $vua = vb = a$.

If $a = 0$, then, since $b = ua$, we must have $b = 0$. So $a = (1)b$. If $a \neq 0$, the cancellation property for an integral domain (see problem 5(c) on this exam) applied to $vua = 1a$ says that $vu = 1$. So $u$ and $v$ are units. Then $b = ua$ with $u$ a unit.

8. (10 points Extra Credit) We define an element $r$ of a ring $R$ to be prime if, whenever $r$ divides a product $ab$ of two elements of $R$, it divides at least one of $a$ and $b$. Suppose that $R$ is an integral domain ($R$ has no zero divisors). Prove that every prime element in $R$ is irreducible.

Solution: Suppose that $p \in R$ is prime and that $p$ has a factorization $ab$ in $R$. We must show that one of $a, b$ is a unit.

Suppose $p = ab$. Then we certainly have $p \mid ab$. Since $p$ is prime, this means that $p$ divides (at least) one of $a$ and $b$. Suppose $p$ divides $a$. But $p = ab$ also means that $a$ divides $p$. By the result of the previous problem, $p = ua$ for some unit $a$. We can then write $ua = ab$ and, commuting and then using the cancellation property since we’re in an integral domain, conclude that $b = u$. So $b$ is a unit and our factorization is trivial. Since this argument applies to any factorization of $p$, we have shown that $p$ is irreducible in $R$. 

- 3-