Math 306, Spring 2012
Homework 1 Solutions

(1) (3 pts/part) Each of the following statements is false. Disprove each one by providing a counterexample or by appealing to the definition.
   (a) If R is a ring, then for every nonzero $f, g \in R[t]$, we have $\deg(f+g) = \deg(f) + \deg(g)$.
   (b) Every ring R has a field of fractions.
   (c) Every integral domain is a field.
   (d) If K is a field, then $K[t]$ is a field.

   Solution:
   (a) Let $R = \mathbb{Z}$. Also let $f = t$ and $g = -t + 1$. Then $\deg(f) + \deg(g) = 2$ but $\deg(f+g) = 0$.
   (b) The field of fractions is defined only for integral domains R.
   (c) Let $R = \mathbb{Z}$. Then R is not a field.
   (d) Let $K = \mathbb{Q}$. Then $K[t]$ is not a field since the element t has no multiplicative inverse.

(2) (5 pts) Let R be a commutative unital ring. We say that an element $u \in R$ is a *unit* if u has a multiplicative inverse. Prove that the set $U(R) = \{u \in R \colon u \text{ is a unit}\}$ is an abelian group under multiplication.

   Solution: Certainly 1 is a unit in R, so $U(R)$ contains an identity element. Associativity and commutativity of multiplication is inherited from R. Let $u \in U(R)$. Then there is $u' \in R$ such that $uu' = 1$. Hence u' is a unit, so $u' \in U(R)$ and $U(R)$ is closed under inverses. Now let $u, v \in U(R)$. Therefore there are $u', v' \in R$ such that $uu' = 1$ and $vv' = 1$. Since $uvu'v' = 1$, it follows that uv is a unit in R, so $U(R)$ is closed under multiplication. Hence $U(R)$ is an abelian group.

(3) (a) (3 pts) Using the notation from the previous problem, find the elements of $U(\mathbb{Z}_5)$, $U(\mathbb{Z}_6)$, $U(\mathbb{Z}_{12})$ and $U(\mathbb{Z}_{24})$.
   (b) (5 pts) Use the Fundamental Theorem of Abelian Groups to express each of these groups as a product of cyclic groups of prime power order. No proof required.

   Solution:
   (a) We have the abelian groups $U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$, $U(\mathbb{Z}_6) = \{1, 5\}$, $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$, and $U(\mathbb{Z}_{24}) = \{1, 5, 7, 11, 13, 17, 19, 23\}$.
   (b) The fundamental theorem gives $U(\mathbb{Z}_5) \cong \mathbb{Z}_4$, $U(\mathbb{Z}_6) \cong \mathbb{Z}_2$, $U(\mathbb{Z}_{12}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and $U(\mathbb{Z}_{24}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) (5 pts/part) Suppose that S is a set and that R is a ring. Let R^S denote the set of all functions $f \colon S \to R$.
   (a) Prove that R^S is a ring, under the operations defined by the following: for all $f, g \in R^S$ and all $s \in S$, let $(f+g)(s) = f(s) + g(s)$ and $(fg)(s) = f(s)g(s)$. You may assume closure and associativity of both operations.
   (b) Prove that, if S has more than one element, then R^S is not an integral domain.

   Solution:
   (a) Consider the zero function $0 \colon S \to R$ defined to be $0(s) = 0$ for all $s \in S$. Then for all $s \in S$ and $f \in R^S$ we have $(0+f)(s) = 0(s) + f(s) = 0 + f(s) = f(s)$. Hence $0 + f = f$. Similarly $f + 0 = f$, so R^S has an identity element. Define the one function $1 \colon S \to R$ given by $1(s) = 1$ for all $s \in S$. Then for all $s \in S$ and $f \in R^S$ we have $(1f)(s) = 1(s)f(s) = 1 \cdot f(s) = f(s)$, so $1f = f$. Similarly $f1 = f$. Therefore R^S has a multiplicative identity. For each $f \in R^S$, define $g \colon S \to R$ by setting $g(s) = -f(s)$ for all $s \in S$. Then clearly $f + g = 0$ and $g + f = 0$, so f has an inverse in R^S. Therefore R^S is a group. For all $f, g \in R^S$, we have $(f+g)(s) = f(s) + g(s) = g(s) + f(s) = (g+f)(s)$ for all $s \in S$, so $f + g = g + f$. Therefore R^S is abelian. Lastly, let $f, g, h \in R^S$ and $s \in S$. Then $[f(g+h)](s) = f(s)(g+h)(s) = f(s)(g(s)+h(s)) = f(s)g(s) + h(s)g(s) = (fg + fh)(s)$, so $f(g+h) = fg + fh$, so multiplication distributes over addition. Hence R^S is a ring.

(b) Suppose S contains the distinct elements a and b. Define $f, g\colon S \to R$ by setting

$$f(s) = \begin{cases} 1 & \text{if } s = a, \\ 0 & \text{otherwise} \end{cases} \quad \text{and } g(s) = \begin{cases} 1 & \text{if } s = b, \\ 0 & \text{otherwise.} \end{cases}$$

Then f and g are nonzero in R^S but $fg = 0$, so R^S is not an integral domain.

(5) (5 pts) Prove that an integral domain R with a finite number of elements is a field. (Hint: For each nonzero $a \in R$, consider the map $\lambda_a\colon R \to R$ given by $\lambda_a(r) = ar$ for all $r \in R$. Prove that λ_a is injective and use the fact that any injective function on a finite set is surjective.)

Solution: Let $a \in R$ be nonzero and consider the map $\lambda_a\colon R \to R$ given by $\lambda_a(r) = ar$ for all $r \in R$. Suppose that there are $r, s \in R$ such that $\lambda_a(r) = \lambda_a(s)$. Then $ar = as$, or $a(r - s) = 0$. Since R is an integral domain and $a \neq 0$, we must have $r - s = 0$, or $r = s$. Hence λ_a is injective. Since R is finite, the map λ_a must be surjective as well, so there is $b \in R$ such that $\lambda_a(b) = 1$, or $ab = 1$. Hence a has a multiplicative inverse, so R is a field.

(6) Suppose that K is a field. Let $f \in K[x]$, where $f = \sum_{i=0}^{n} a_i x^i$ with $a_i \in K$ for all i. Let $k \in K$. Define $\phi\colon K[x] \to K^K$ by $(\phi(f))(k) = \sum_{i=0}^{n} a_i k^i$.

(a) (5 pts) Prove that ϕ is a ring homomorphism. (Hint: for multiplicativity, it is best to use summation notation to write $fg = \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} = \sum_{j=0}^{m+n} c_j x^j$ where $c_j = \sum_{i=0}^{j} a_i b_{j-i}$. If this set of equations does not make sense to you, try to verify it by multiplying out some expression like $(a_0 + a_1 x)(b_0 + b_1 x + b_2 x^2)$. To prove additivity, assume without loss of generality that $n \leq m$.)

(b) (7 pts) Prove that, if K is finite, then ϕ is surjective but not injective.

Solution:

(a) Let $f, g \in K[x]$ be given by $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{j=0}^{m} b_j x^j$. Without loss of generality, assume that $n \leq m$. Let $k \in K$. Then $(\phi(f + g))(k) = \sum_{i=0}^{m} (a_i + b_i) k^i = \sum_{i=0}^{m} a_i k^i + \sum_{i=0}^{n} b_i k^i = \sum_{i=0}^{n} a_i k^i + \sum_{i=0}^{n} b_i k^i = (\phi(f))(k) + (\phi(g))(k) = (\phi(f) + \phi(g))(k)$. Hence $\phi(f + g) = \phi(f) + \phi(g)$. In addition, we have $(\phi(fg))(k) = \sum_{j=0}^{m+n} c_j k^j = \sum_{i=0}^{n} a_i k^i \sum_{j=0}^{m} b_j k^j = (\phi(f))(k)(\phi(g))(k)$, where $c_j = \sum_{i=0}^{j} a_i b_{j-i}$. Hence $\phi(fg) = \phi(f)\phi(g)$. Thus ϕ is a ring homomorphism.

(b) Suppose that $K = (k_1, \ldots, k_n)$ is finite and let $r \in K^K$. Consider the Lagrange polynomial $f \in K[x]$ for which $f(k_i) = r(k_i)$ for each i. Then $(\phi(f))(k) = r(k)$ for all $k \in K$. Therefore $\phi(f) = r$, so ϕ is surjective. To prove that ϕ is not injective, consider $f = (x - k_1)(x - k_2) \cdots (x - k_n)$ and $g = (x - k_1)^2 (x - k_2) \cdots (x - k_n)$. Then $f(k) = 0$ and $g(k) = 0$ for all $k \in K$ so $\phi(f) = \phi(g)$ but $f \neq g$ in $K[x]$.

(7) (5 pts) Recall that an ideal I in a commutative unital ring R is *prime* iff $a \in I$ or $b \in I$ whenever $ab \in I$. We say that an element $c \in R$ is *prime* if $c|a$ or $c|b$ whenever $c|ab$. Prove that the following are equivalent for an element $c \in R$:

(a) the element c is prime in R;
(b) the ideal (c) is prime in R;
(c) the quotient $R/(c)$ is an integral domain.

Solution: Suppose that c is prime in R. Now suppose that $ab \in (c)$. Then $c|ab$, so $c|a$ or $c|b$ since c is prime. So $a \in (c)$ or $b \in (c)$. Hence (c) is a prime ideal. Now suppose that $I = (c)$ is a prime ideal. Now let suppose that $(a + I)(b + I) = I$ in R/I. Then $ab + I = I$, so $ab \in I = (c)$. Then $a \in (c)$ or $b \in (c)$ since (c) is a prime ideal. Suppose that $R/(c)$ is an integral domain, and suppose that $c|ab$ in R. Then $ab \in (c)$, so $ab + (c) = (c)$, i.e. $(a + (c))(b + (c)) = (c)$, so $a + (c) = (c)$ or $b + (c) = (c)$ since $R/(c)$ is an integral domain. Therefore $a \in (c)$ or $b \in (c)$, i.e. $c|a$ or $c|b$. So c is prime.