Factoring Polynomials

Sue Geller*

June 19, 2006

Factoring polynomials over the rational numbers, real numbers, and complex numbers has long been a standard topic of high school algebra. With the advent of computers and the resultant development of error-correcting codes, factoring over finite fields (e.g., $\mathbf{Z}_p$, for p a prime number) has become important as well. To understand this discussion, you need to know what polynomials are, and how to add, subtract, multiply and divide them. Many of the theorems below will be familiar, but you may not have seen the proofs. Some may be new. All of them have been useful to various mathematicians. This is not an exhaustive list, but hopefully enough to give you an idea of the variety of information that can be gleaned and used.

A field is a set F with two operations, usually denoted $+$ and $\cdot$, such that F is an abelian group under the operation $+$ with identity 0, $F \setminus \{0\}$ is an abelian group under the operation $\cdot$ with identity 1, and the distributive law, $a(b+c) = ab+ac$ for all $a, b, c \in F$, holds. For example, the rational numbers, the real numbers, the complex numbers, and $\mathbf{Z}_p$, for p a prime number, are all fields. (For $\mathbf{Z}_p$, recall that $x \in \mathbf{Z}_p$ has a multiplicative inverse (or generates the units) if and only if $x \neq 0$. So $\mathbf{Z}_p \setminus \{0\}$ is an abelian group, whence $\mathbf{Z}_p$ is a field.) So for this dicussion F will always denote a field, and $F[x]$ the ring of polynomials with coefficients in the field F. Similarly, $\mathbf{Z}[x]$ is the ring of polynomials with integer coefficients. We call F or $\mathbf{Z}$ the ground ring. You need not know what a ring is to understand what follows, but for completeness, a commutative (which all of ours are) ring is a set R with two operations, usually denoted $+$ and $\cdot$, such that F is an abelian group

under the operation + with identity 0, $\cdot$ is a commutative, associative binary operation, and the distributive law holds. From high school algebra we know that the set of polynomials is a commutative ring which has a multiplicative identity 1.

Recall that, for integers a, b with $b \neq 0$, there exist unique integers q, r so that $a = qb + r$ where $0 \leq r < |b|$, i.e., the division algorithm. Also recall that a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_n \neq 0$ is said to have degree n. Note that the zero polynomial does not have a degree, so degree 0 polynomials are non-zero "constants", i.e., are non-zero elements of the ground ring. So we can use the idea of the division algorithm on the degree of the polynomials to get a similar theorem for polynomials.

Theorem 1 ***Division Algorithm:*** *Let f, g be polynomials with rational (or real or complex or any other field) coefficients where $g \neq 0$. Then there exist unique polynomials q, r with coefficients in the same field as f and g so that $f = qg + r$ where $r = 0$ or $deg(r) < deg(g)$.*

Proof: We start with existence. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be polynomials where $a_n \neq 0$ and $b_m \neq 0$. (Note: If $f = 0$, $0 = 0g + 0$, so the assumption that $a_n \neq 0$ is okay.) We proceed by induction on the degree of f. If $n = 0$, then either $f = c = (cd^{-1})g$, where $g = d$ has degree 0 or $f = 0g + f$ where degree$(g) > 0$ satisfies the conditions. Assume that, if $n < k$, then there exist polynomials q, r with coefficients in the same field as f so that $f = qg + r$ where $r = 0$ or $\deg(r) < \deg(g)$. Now assume that the degree of f is k. If $k < m$, then $f = 0g + f$ satisfies the conditions. If $m \leq n$, then $f(x) - a_k(b_m^{-1})x^{n-m}g(x)$ has degree at most $k - 1 < k$. So there exist q_1, r so that $f(x) - a_k(b_m^{-1})x^{n-m}g(x) = q_1(x)g(x) + r(x)$ where $r = 0$ or $\deg(r) < \deg(g)$. Thus $f(x) = (a_k b_m^{-1}x^{n-m} + q_1(x))g(x) + r(x)$. Letting $q(x) = a_k b_m^{-1}x^{n-m} + q_1(x)$, we see that $f = qg + r$ with the coeffiecients of q, r in the same field as f, as required.

Now suppose that $f = pg + s$ where $s = 0$ or $\deg(s) < \deg(g)$. Then $0 = (p - q)g + s - r$. So $(p - q)g = r - s$. If $r - s \neq 0$ (so $p \neq q$), then $\deg(r - s) < \deg g \leq \deg((p - q)g)$. Contradiction. Therefore, $r = s$, and $pg = qg$. Since g is not a zero-divisor, $p = q$.

NOTE: When we wrote b_m^{-1} we used the fact that the coefficients came from a field, i.e., that all non-zero coefficients had inverses. We could just have easily allowed any coefficient ring (such as $\mathbf{Z}$) and insisted that the leading coefficient, b_m, of g be invertible (or ± 1 in the case of $\mathbf{Z}$).

Example:

1. We can use long division to find that $x^4 + 3x^3 - 2x^2 + 7x - 16 = (x^2 + 6x + 12)(x^2 - 3x + 4) + (19x - 64)$.
2. If $f(x) = 8x^7 + 6x^5 - 3x + 2$ and $g(x) = 2x^3 - 3$, then $f(x) = (4x^4 + 3x^2 + 6x)g(x) + 9x^2 + 15x + 2$.

We now turn to a special case of the division algorithm, that of the divisor having degree one. This case helps us prove many of the theorems we used in high school algebra, especially the correspondence between roots of a polynomial and factors of that polynomial, and the fact that a polynomial of degree n has at most n roots in the ground field.

Corollary 1 ***Remainder Theorem:*** *Let f be a polynomial with coefficients in a field or in the integers or in any ring. Let a be a number in the ground ring. Then there exists a polynomial q with coefficients in the same field or ring as f such that $f = (x - a)q + f(a)$.*

Proof: Since the leading coefficient of $x - a$ is 1, we may apply the Division Algorithm to $f(x)$ and $(x - a)$ and get that $f = q(x - a) + r$ where the coefficients of q, r are in the same field or ring as those of f and either $r = 0$ or $\deg r < \deg(x - a) = 1$. So $r(x)$ is a constant. Evaluating at a, we get $f(a) = q(a)(a - a) + r = r$. By the uniqueness part of the Division Algorithm, $f(x) = (x - a)q(x) + f(a)$.

Corollary 2 ***Factor Theorem:*** *The number a is a root of f if and only if $x - a$ is a factor of $f(x)$.*

Proof: The number a is a root of f if and only if $f(a) = 0$ if and only if $f(x) = (x - a)q(x)$.

Theorem 2 *A polynomial of degree n with coefficients in a field or in* $\mathbf{Z}$ *has at most n roots in that field or in* $\mathbf{Z}$*..*

Proof: Let f be a polynomial of degree n. Let $a_1, \ldots$ be the roots of $f(x)$. By repeated applications of the factor theorem, after t roots we have $f(x) = (x-a_1)g_1(x) = (x-a_1)(x-a_2)g_2(x) = \cdots = (x-a_1)\ldots(x-a_t)g_t(x)$. Then $n = \deg f(x) = t + \deg g_t(x)$. So $t \leq n$. Thus the number of roots is finite and at most n.

We now turn our attention to theorems that help us factor polynomials over the rational numbers. If $f(x) = a_n x^n + \cdots + a_0$ is a polynomial with rational coefficients, let d be the least common multiple of the denominators of the a_i. Then $g = df$ is a polynomial with integer coefficients which has the same roots as f, since multiplying by a non-zero constant does not change the solutions to $f(x) = 0$. Thus we may assume that we start with a polynomial with integer coefficients, rather than rational coefficients, when we try to find ways to factor rational polynomials.

Theorem 3 *Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *where* $a_n \neq 0$ *and the* a_i *are integers. If* p *and* q *are relatively prime integers so that* $f(p/q) = 0$*, then* q *divides* a_n *and* p *divides* a_0*.*

Proof: By assumption, $0 = f(p/q) = a_n(p/q)^n + ... + a_1(p/q) + a_0$. Multiplying the equation by q^n we find that $0 = a_n p^n + a_{n-1}qp^{n-1} + \cdots + a_1 q^{n-1}p + a_0 q^n$. Since p divides $a_i q^{n-i}p^i$ for $i = 1, \ldots, n$, p divides $a_0 q^n$. But p and q are relatively prime, so p divides a_0. Similarly, q divides $a_i q^{n-i}p^i$ for $i = 0, \ldots, n-1$, whence q divides $a_n p^n$. But p and q are relatively prime, so q divides a_n.

Example: Let $f(x) = 2x^4 + 3x^3 - 2x^2 + 7x - 6$. Since p divides 6 and q divides 2, the possible rational roots are $\pm 1, \pm 2, \pm 3, \pm 6, \pm 1/2, \pm 3/2$. Testing shows that none of these possibilities is in fact a root.

Theorem 4 *Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *where* $a_n \neq 0$*, and the* a_i *are integers. If* $a_0, a_n, f(1)$ *are all odd, then* f *has no rational roots.*

Proof: First we note that, if $n = 1$ and a_0, a_1 are odd, then $f(1) = a_1 + a_0$ is even. So we may assume that $n \geq 2$.

We will prove this one by contradiction, the most commonly used proof technique to show something doesn't happen. (Even in life it is hard to prove something isn't, but easier to prove something is.) So suppose that such an f has a rational root p/q where p and q are relatively prime. By the previous theorem, we know that p divides a_0 and q divides a_n. In particular we now know that p and q are odd because a_0, a_n are. Thus $p^i q^j$ is also odd for every pair of nonnegative integers i, j. Since $f(p/q) = 0$ we have as we did in the last proof that $0 = q^n f(p/q) = a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_1 q^{n-1} p + a_0 q^n$. Since $f(1) = \Sigma a_i$ is odd, an odd number of the a_i are odd. Therefore the expansion of $q^n f(p/q)$ has an odd number of odd terms, so cannot be zero. This is a contradiction. Therefore, f has no rational roots.

Example: Let $f(x) = 15x^{19} + 7x^{13} - 2x^8 + 13x^6 - 12x^4 - 3x^3 + 2x^2 + 28x + 343$. We easily observe that $a_n = 15,$ and $a_0 = 343$ are odd. Rather than compute $f(1)$, note that 5 of the coefficients are odd, so $f(1)$ is odd. Therefore f does not have any rational roots.

Theorem 5 *Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ where $a_n \neq 0$ and the a_i are integers. Suppose $f(a) \neq 0$, $a \in \mathbf{Z}$. If p and q are relatively prime integers so that $f(p/q) = 0$, then $(p - aq)$ divides $f(a)$.*

Proof: Let p/q be a rational root of f where p and q are relatively prime. Next note that $f - f(a)$ is a polynomial of positive degree n that has a as a root. Thus, by the Factor Theorem, $f - f(a) = (x - a)g$ where g is also a polynomial with integer coefficients. If we evaluate at p/q, we get $((p/q) - a)g(p/q) = f(p/q) - f(a) = -f(a) \neq 0$. Multiplying by q^n we see that $(p - aq)q^{n-1} g(p/q) = -q^n f(a)$. Since $\deg g = n - 1$, the number $q^{n-1} g(p/q)$ is an integer. Thus $p - aq$ divides $q^n f(a)$. But p and q are relatively prime, so q and $p - aq$ are also relatively prime. Thus $p - aq$ divides $f(a)$.

Example: Let $f(x) = 60x^6 - 212x^5 + 203x^4 + 48x^3 - 133x^2 + 10x + 24$. There are lots of factors of 60 and 24 and I don't want to check all of them (there are 72 combinations after deleting repeats). First I check $f(1) = 0$ and get a root. In fact it is a double root and $f(x) = (x-1)^2(60x^4 - 92x^3 - 41x^2 + 58x + 24)$. Note that removing factors of $x \pm 1$ does not change the leading coefficient nor the absolute value of the constant term. So we still have 72 possible rational roots. Let's see what we can eliminate. $f(-1) = 308$. So $p + q$ divides 308. Also $f(2) = 200$. So $p - 2q$ divides 200. This pair of constraints reduces

the list of possible roots to 16 possibilities. For example, $\pm 1/60$ are possible roots. But $1 + 60 = 61$ and $-1 + 60 = -59$ do not divide 308. So they are not roots. Can you eliminate the other 54 possible roots that I eliminated?

Theorem 6 ***Descartes' Rule of Signs:*** *If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with real coefficients, then the number of positive roots of the polynomial equation $f(x) = 0$ is either equal to the number of times the coefficients in f change sign or less than that by an even number. The number of negative roots of f is obtained by applying the above rule for the number of positive roots to $f(-x)$.*

In the above example, $f(x) = 60x^6 - 212x^5 + 203x^4 + 48x^3 - 133x^2 + 10x + 24$, there are are 4 changes in sign, so $f(x)$ has $0, 2$, or 4 positive roots. If $g(x) = x^8 + 3x^6 - x^2 + 7$, there are 2 changes of sign, so $g(x)$ has 0 or 2 positive roots.

Proof: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Since we are counting positive roots, we may assume that $a_0 \neq 0$, namely, if $f = x^i g$ where $g(0) \neq 0$, we can work with g which has the same number of sign changes and positive roots as f. Recall that the derivative of $f(x)$ is $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$. Let $C(f)$ (resp., $C(f')$) be the number of sign changes of f (resp., f'). Similarly, let $Z_+(f)$ (resp., $Z_+(f')$) be the number of positive roots of f (resp., f') counting multiplicities – e.g., $f(x) = (x+1)^3(x-4)^7(x-5)$ has $Z_+(f) = 8$ since the roots are $-1, -1, -1, 4, 4, 4, 4, 4, 4, 4, 5$. We are first going to find relationships between $Z_+(f)$ and $Z_+(f')$ and between $C(f)$ and $C(f')$. Note that we assumed that $a_0 \neq 0$, but it is possible that $a_1 = 0$. If $a_1 \neq 0$, let $\ell = 1$, and if $a_1 = 0$, let ℓ be the first index so that $a_\ell \neq 0$ (and $a_{\ell-1} = \cdots = a_1 = 0$). We now need a theorem from calculus.

Rolle's Theorem Suppose $f(a) = f(b)$ for a function that is differentiable on $[a, b]$. Then there is a number $c \in (a, b)$ so that $f'(c) = 0$.

Proof continued: Since polynomials are differentiable everywhere, by Rolle's Theorem, between every two distinct roots of our polynomial f there is at least one root of f'. If a is a multiple root of f of order q, then a is root of f' of order $q - 1$. Thus if f has n positive roots, f' has at least $n - 1$ positive roots, or in symbols

$$Z_+(f) \leq Z_+(f') + 1. \tag{1}$$

Also, by considering the graph of $f(x)$ as x gets very large, we see that if a_n and a_0 (resp., a_ℓ) have the same sign, f (resp., f') has an even number of positive zeroes, and if differing signs, an odd number of positive zeroes. So if a_0 and a_ℓ have the same sign, then

$$Z_+(f) \equiv Z_+(f') \pmod 2 \text{ and } Z_+(f) \leq Z_+(f'). \tag{2}$$

If a_0 and a_ℓ have opposite signs, then

$$Z_+(f) \equiv Z_+(f') + 1 \pmod 2. \tag{3}$$

Lastly, a straightforward counting argument shows that

$$C(f) = \begin{cases} C(f') & \text{if } a_0 \text{ and } a_\ell \text{ have the same sign,} \\ C(f') + 1 & \text{if } a_0 \text{ and } a_\ell \text{ have opposite signs.} \end{cases} \tag{4}$$

We now proceed by induction on the degree of f. When $\deg f = 1$, $f(x) = a_1 x + a_0$ which has one positive root and $C(f) = 1$ if the signs of a_0 and a_1 are different, but no positive roots and $C(f) = 0$ if the signs of a_0 and a_1 are the same. Assume that Descartes' rule of signs is true if $\deg f = k-1$. Let f be a polynomial of degree k. Then $\deg f' = k - 1$. By the induction assumption, $Z_+(f') \equiv C(f') \pmod 2$ and $Z_+(f') \leq C(f')$. We now consider two cases depending on the signs of a_0 and a_ℓ.

Case I: Suppose the signs of a_0 and a_ℓ are the same. Then

$$Z_+(f) \overset{2}{\leq} Z_+(f') \overset{ind}{\leq} C(f') \overset{4}{=} C(f), \text{ and}$$

$$Z_+(f) \overset{2}{\equiv} Z_+(f') \overset{ind}{\equiv} C(f') \overset{4}{\equiv} C(f) \pmod 2.$$

Case II: Suppose that the signs of a_0 and a_ℓ are different. Then

$$Z_+(f) \overset{1}{\leq} Z_+(f') + 1 \overset{ind}{\leq} C(f') + 1 \overset{4}{=} C(f), \text{ and}$$

$$Z_+(f) \overset{3}{\equiv} Z_+(f') + 1 \overset{ind}{\equiv} C(f') + 1 \overset{4}{\equiv} C(f) \pmod 2.$$

We now go to the other extreme. Instead of looking for roots, we will develop some criteria to tell us that not only are there no roots in the ground field, but the polynomial doesn't even factor over that field.

Definition: A polynomial of positive degree — i.e., not a constant — over a field is *reducible* over that field if it is the product of two polynomials both of lower degree (equivalently, both of degree at least one). A polynomial is *irreducible* over a field if it is not reducible over that field. Over $\mathbf{Z}$, a non-constant polynomial is reducible if its coefficients have a common prime factor or if it is the product of two polynomials both of lower degree.

Example: $2x^2 + 4 = 2(x^2 + 2)$ is reducible over $\mathbf{Z}$, but is irreducible over the rationals.

Our first simplification is similar to what we did for roots of polynomials with rational coefficients, namely, we reduce our problem to one over the integers.

Theorem 7 *Let f be a polynomial with rational coefficients in lowest terms so that the numerators of the coefficients are relatively prime (i.e., have no common prime factor). Let d be the least common multiple (lcm) of the denominators of the coefficients of f. Let $g = df$. Then g has integer coefficients. Furthermore, f is irreducible over the rationals if and only if g is irreducible over the integers.*

Proof: First note that by starting with rational coefficients in lowest terms and then multiplying by the lcm of the denominators, the integer coefficients of g have no common prime factor (or their gcd is 1). Thus g has no factors of degree 0 other than ± 1. Also note that the degree of f equals the degree of g.

We will now prove the theorem by contrapositive, namely, f is reducible over the rationals if and only if g is reducible over the integers. So f is reducible over the rationals if and only if there exist polynomials $p, q \in \mathbf{Q}[x]$, both of degree less than the degree of f, so that $f = pq$. Since $df \in \mathbf{Z}[x]$, $dpq \in \mathbf{Z}[x]$. Thus $dpq = rs$ where $r, s \in \mathbf{Z}[x]$ and the degrees of r, s are less than the degree of g. Similarly, g is reducible over the integers if and only if there exist polynomials $p, q \in \mathbf{Z}[x]$, both of degree less than the degree of g, so that $g = pq = df$. Thus $f = (d^{-1}p)q$ where $d^{-1}p, q \in \mathbf{Q}[x]$ and the degrees of $d^{-1}p, q$ are both less than the degree of f.

The following is a famous theorem about irreducible polynomials.

Theorem 8 ***Eisenstein's Irreducibility Criterion:*** *Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *be a polynomial with integer coefficients and of positive degree. Suppose there is a prime* p *so that* p *does not divide* a_n*,* p *divides* $a_i,\ i = 0, ..., n-1$*, and* p^2 *does not divide* a_0*. Then* f *is irreducible over the rational numbers.*

Proof: Since we are interested in irreducibility over the rational numbers, we may assume that the a_i have no prime factor in common – i.e., that the a_i are relatively prime. By the previous theorem we need only prove that f is irreducible over the integers. We will do so by contradiction. Suppose f is reducible over the integers. Then there exist polynomials $g(x) = b_r x^r + \cdots + b_0, h(x) = c_s x^s + \cdots + c_0 \in \mathbf{Z}[x]$ with $r, s \geq 1$ so that $f = gh$. Since p divides $a_0 = b_0 c_0$, and p^2 does not divide $a_0 = b_0 c_0$, either p divides b_0 or p divides c_0 but not both. Without loss of generality we may assume that p divides b_0. Since p does not divide $a_n = b_r c_s$, p does not divide b_r. Let k be the least integer so that p divides b_i for $i < k$ and p does not divide b_k. So $1 \leq k \leq r < n$. Then $a_k = b_0 c_k + \cdots + b_{k-1} c_1 + b_k c_0$. Since p divides a_k (since $k < n$) and p divides $b_i,\ i = 0, ..., k-1$ (by choice of k), p divides $b_k c_0$. But p does not divide c_0 nor b_k. Contradiction. Therefore f is irreducible over the rational numbers.

Example: $3x^{19} - 7x^{15} + 49x^{10} - 28x^6 - 35$ is irreducible over the rational numbers because 7 does not divide 3, 7 does divide $-7, 49, -28, -35$ and $7^2 = 49$ does not divide -35.

We can make Eisenstein's Irreducibility Criterion more widely applicable by changing variables.

Theorem 9 *Let* f *be a polynomial over a field (such as the rationals). Then* f *is irreducible if and only if* $g = f(ax + b),\ a \neq 0$*, is irreducible. If* f *is a polynomial over the integers, then* f *is irreducible if and only if* $g = f(x + b)$ *is irreducible.*

Proof: We shall prove the contrapositive, namely, f is reducible over a field (resp., the integers) if and only if $g = f(ax + b),\ a \neq 0$, (resp., $f(x + b)$) is reducible.

Suppose f is reducible. Then $f = pq$ for some polynomials p, q of positive degree. By substituting $ax + b$ for x, we get that $g(x) = f(ax + b) =$

$p(ax+b)q(ax+b)$, whence g is reducible. Note that there is no difference here between fields and integers.

Suppose $g = f(ax+b)$ is reducible. Then $g = g(x) = f(ax+b) = p(x)q(x)$ for some polynomials p, q of positive degree. By substiting $a^{-1}(x-b)$ for x, we get that $f(x) = p(a^{-1}(x-b))q(a^{-1}(x-b))$, whence f is reducible. Note that we used the fact that in a field, a non-zero element has an inverse. Over the integers, if $f(x+b)$ is reducible, we can duplicate the argument with $a = 1$.

Example: We know that $f(x) = x^2 + x + 1$ is irreducible over the rational numbers since, by the quadratic formula, the roots of $f(x)$ are $(-1 \pm i\sqrt{3})/2$. All the coefficients are 1, so Eisenstein's Irreducibility Criterion does not apply directly. But $f(x+1) = (x+1)^2 + (x+1) + 1 = x^2 + 3x + 3$ which is irreducible by Eisenstein's Irreducibility Criterion. Thus f is also irreducible over the rational numbers.

Problems

1. Use the above theorems to factor the following polynomials over the rationals. Then factor them over the complex numbers.

   (a) $x^5 - 9x^3 - 8x^2 + 72$

   (b) $x^5 + x^4 + x^3 + x^2 + x + 1$

   (c) $x^4 - x^3 - x^2 - 5x - 30$

   (d) $12x^5 + 80x^4 + 79x^3 - 135x^2 - 158x - 40$

   (e) $20x^6 + 28x^5 + 23x^4 - 35x^3 - 55x^2 + 7x + 12$

2. Use Eisenstein's Irreducibility Criterion to prove that $2x^{17} - 18x^{12} + 24x^9 + 243x^6 - 30x^3 - 6$ is irreducible.

3. Let $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

   (a) Show that f_p has no linear factors over the rationals when p is odd.

   (b) Use Eisenstein's Irreducibility Criterion and a change of variables (say $x \to y + 1$) to prove that f_5 is irreducible over the rational numbers.

   (c) Use Eisenstein's Irreducibility Criterion to prove that f_p is irreducible over the rational numbers for every prime number p.
   Hint: $x^p - 1 = (x - 1)f_p$.