ROOTS ON A CIRCLE

KEITH CONRAD

1. Introduction

The nth roots of unity obviously all lie on the unit circle (see Figure 1 with $n = 7$). Algebraic integers which are not roots of unity can also appear there. The quartic polynomial $z^4 - 2z^3 - 2z + 1$ has two roots on the unit circle (see Figure 2). To explain this, we use the symmetry in the coefficients of $z^4 - 2z^3 - 2z + 1$, which tells us that if α is a root then so is $1/\alpha$. Write the two real roots as α_1 and $1/\alpha_1$. If α_2 is a non-real root then so are $1/\alpha_2$ and $\overline{\alpha}_2$, neither of which is real or equal to α_2, so they must be equal. The condition $1/\alpha_2 = \overline{\alpha}_2$ is the same as $|\alpha_2| = 1$.

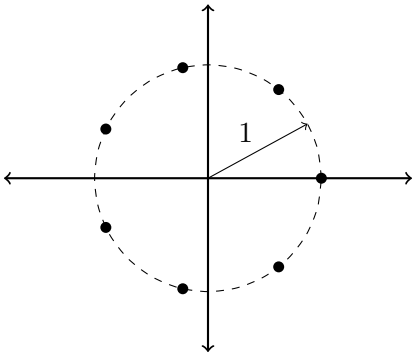

Figure 1. The 7th roots of unity.

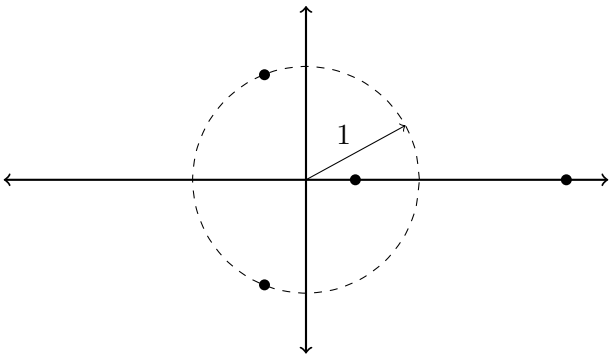

Figure 2. The roots of $z^4 - 2z^3 - 2z + 1$.

A famous polynomial with many, but not all, roots on the unit circle is Lehmer's polynomial [1, p. 477]

$$z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1,$$

whose roots are plotted in Figure 3. There are 2 real roots (approximately .850 and 1.176) and 8 roots on the unit circle. How do you prove those non-real roots are really on the unit circle? From the symmetry in the coefficients, the roots come in reciprocal pairs, and since the coefficients are real the non-real roots come in complex conjugate pairs. If α is one of the non-real roots, then $1/\alpha$ and $\overline{\alpha}$ are also roots, but it is not immediately clear how to show $1/\alpha = \overline{\alpha}$, so $|\alpha| = 1$. The argument we gave for the quartic does not apply in this case since there are too many non-real roots.

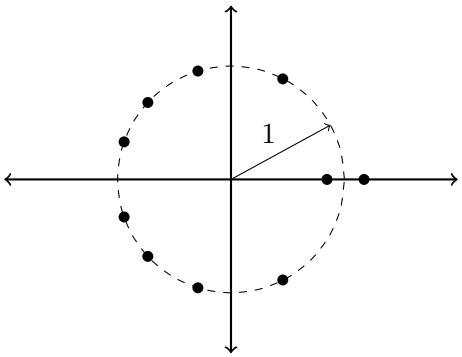

FIGURE 3. The roots of $z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$.

Generally, we want to explain how to count the number of roots of a polynomial that lie on the unit circle. For an irreducible polynomial in $\mathbf{Q}[z]$, having a root on the unit circle imposes a symmetry property on the polynomial and a constraint on its degree, as follows.

Theorem 1.1. *Let $f(z) \in \mathbf{Q}[z]$ be irreducible with degree $n > 1$. If $f(z)$ has a root on the unit circle then n is even and $z^n f(1/z) = f(z)$.*

Proof. Let α be a root of $f(z)$ with $|\alpha| = 1$. Since f has real coefficients, $\overline{\alpha} = 1/\alpha$ is also a root of $f(z)$. The product $z^n f(1/z)$ is a polynomial in $\mathbf{Q}[z]$ of degree n (its leading coefficient is $f(0)$) with root α, so by irreducibility of $f(z)$, $z^n f(1/z) = cf(z)$ for some nonzero rational number c. Setting $z = 1$, $f(1) = cf(1)$. Since $f(1) \neq 0$ by our hypotheses, $c = 1$, so $f(z) = z^n f(1/z)$. Setting $z = -1$, we get $f(-1) = (-1)^n f(-1)$. Since $f(-1) \neq 0$, $(-1)^n = 1$, so n is even. □

In Section 2 we will describe a method of root counting that applies to any polynomial satisfying the conclusion of Theorem 1.1, whether or not it is irreducible in $\mathbf{Q}[z]$. In Section 3 we will describe a different method that applies with no special hypotheses.

2. The Palindromic Case

It turns out that the conclusions in Theorem 1.1 essentially say $f(z)$ can be expressed in terms of $z + 1/z$.

Theorem 2.1. *For a polynomial $f(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_1 z + c_0$ with even degree $n = 2m$, the following conditions are equivalent:*

(1) *the polynomial has palindromic coefficients:* $c_k = c_{n-k}$ *for all* k,
(2) $z^n f(1/z) = f(z)$,
(3) $f(z) = z^m g(z + 1/z)$ *for a polynomial* g *of degree* m.

We will call a polynomial "palindromic" when its coefficients satisfy (1), and hence also (2) or (3).

Proof. It is simple to check that (1) and (2) are equivalent and that (3) $\Rightarrow$ (2).

To prove (2) $\Rightarrow$ (3), rewrite the equation $z^n f(1/z) = f(z)$ as $z^m f(1/z) = (1/z)^m f(z)$. Since $f(z)$ has degree $2m$,

$$\left(\frac{1}{z}\right)^m f(z) = c_{2m}z^m + c_{2m-1}z^{m-1} + \cdots + c_m + \cdots + \frac{c_1}{z^{m-1}} + \frac{c_0}{z^m}, \tag{2.1}$$

which is a polynomial in z and $1/z$ of degree m. The symmetry condition (1) tells us that z^i and z^{m-i} on the right side of (2.1) have equal coefficients. The power $c_{2m}(z + 1/z)^m$ has initial and final terms that match those in (2.1), so $(1/z)^m f(z) - c_{2m}(z + 1/z)^m$ is a polynomial in z and $1/z$ of degree less than m. It is palindromic since the difference of palindromic polynomials in z and $1/z$ is still palindromic. Therefore by induction on the degree, we can write $(1/z)^m f(z) - c_{2m}(z + 1/z)^m = h(z + 1/z)$ where $h(z) \in \mathbf{C}[z]$ and it has degree less than m. Now add $c_{2m}(z + 1/z)^m$ to both sides. □

Example 2.2. The polynomial $z^8 - z^5 - z^4 - z^3 + 1$ is palindromic. Divide by z^4 to get $z^4 - z - 1 - 1/z + 1/z^4$. Now subtract $(z + 1/z)^4$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 = -4z^2 - z - 7 - \frac{1}{z} - \frac{4}{z^2}.$$

Next add $4(z + 1/z)^2$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 + 4\left(z + \frac{1}{z}\right)^2 = -z + 1 - \frac{1}{z}.$$

Add $z + 1/z$:

$$\left(z^4 - z - 1 - \frac{1}{z} + \frac{1}{z^4}\right) - \left(z + \frac{1}{z}\right)^4 + 4\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) = 1.$$

Bringing all the powers of $z + 1/z$ to the right side and multiplying through by z^4, we have

$$z^8 - z^5 - z^4 - z^3 + 1 = z^4\left(\left(z + \frac{1}{z}\right)^4 - 4\left(z + \frac{1}{z}\right)^2 - \left(z + \frac{1}{z}\right) + 1\right).$$

In Theorem 2.1, we made no assumptions about irreducibility or that the coefficients are rational. (The theorem was, however, inspired by the situation of Theorem 1.1 where $f(z)$ was irreducible.) Theorem 2.1 provides a bijection between all polynomials $g(z)$ of degree m and all palindromic polynomials $f(z)$ of degree $2m$ (with coefficients in any ring). Obviously f is monic if and only if g is monic, and the nature of the recursive process to obtain g from f, as shown in Example 2.2, shows f has integral coefficients if and only if g has integral coefficients. If $f(z)$ is irreducible in $\mathbf{Q}[z]$ then $g(z)$ is also irreducible in $\mathbf{Q}[z]$ because the equation $f(z) = z^m g(z+1/z)$ forces f to factor nontrivially if g does. However, if $g(z)$ is irreducible in $\mathbf{Q}[z]$ then it does not follow that $f(z)$ is irreducible. For example, if $g(z) = z^2 - 5$ then $z^2 g(z + 1/z) = (z^2 - z - 1)(z^2 + z - 1)$.

Here is a link between roots on the unit circle and real roots.

Theorem 2.3. *For a polynomial $f(z) = c_n z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ of even degree satisfying $c_k = c_{n-k}$ for all k, write $f(z) = z^m g(z + 1/z)$. The roots of f on the unit circle, considered as pairs of reciprocals, correspond to the roots of g in the interval $[-2, 2]$ by $\{\alpha, 1/\alpha\} \leftrightarrow \alpha + 1/\alpha$.*

Proof. We have $f(z) = 0$ if and only if $g(z + 1/z) = 0$. (Note $f(0) = c_0 = c_n \neq 0$.)

If $|z| = 1$, so $z = \cos\theta + i\sin\theta$, then $z + 1/z = 2\cos\theta$ lies in the interval $[-2, 2]$. Conversely, if $-2 \leq t \leq 2$, so $t = 2\cos\theta$ for some angle θ, then $t = z + 1/z$ for the two numbers $z = \cos\theta \pm i\sin\theta$ (which are really one number when $t = \pm 2$, namely $z = 1$ for $t = 2$ and $z = -1$ for $t = -2$). □

Setting $z = \pm 1$ in the equation $f(z) = z^m g(z + 1/z)$, we get $f(\pm 1) = \pm g(\pm 2)$. Since we are usually interested in polynomials $f(z)$ that are irreducible over $\mathbf{Q}$ with degree greater than 1, $f(\pm 1)$ will not be 0, so $g(z)$ will not vanish at ± 2. Therefore the endpoints of $[-2, 2]$ will not really matter when we talk about roots, although we should specify that a root of $g(z)$ is in $(-2, 2)$ not just $[-2, 2]$ to be sure it has the form $z + 1/z$ for *two* values of z.

Example 2.4. To prove Lehmer's polynomial has 8 roots on the unit circle, we express Lehmer's polynomial in terms of $z+1/z$. Carrying out the method of Example 2.2, Lehmer's polynomial is equal to

$$z^5\left(\left(z+\frac{1}{z}\right)^5 + \left(z+\frac{1}{z}\right)^4 - 5\left(z+\frac{1}{z}\right)^3 - 5\left(z+\frac{1}{z}\right)^2 + 4\left(z+\frac{1}{z}\right) + 3\right).$$

The polynomial $w^5 + w^4 - 5w^3 - 5w^2 + 4w + 3$ has all real roots, which are approximately -1.886, -1.468, $-.584$, $.913$, 2.026. Since 4 of the roots are in $(-2, 2)$, there are 8 roots of Lehmer's polynomial on the unit circle.

Example 2.5. The polynomial $z^4 - 2z^3 - 2z + 1$ from Figure 2 is palindromic. We can write

$$z^4 - 2z^3 - 2z + 1 = z^2\left(\left(z+\frac{1}{z}\right)^2 - 2\left(z+\frac{1}{z}\right) - 2\right),$$

so the roots of $z^4 - 2z^3 - 2z + 1$ on the unit circle are related to the real roots of $w^2 - 2w - 2$ in $[-2, 2]$. This quadratic has roots $\approx -.732$ and 2.732. One of them is in $(-2, 2)$, so we get two roots to the quartic on the unit circle.

Example 2.6. The palindromic polynomial $z^6 - z^4 - 2z^3 - z^2 + 1$ from Figure 4 can be written as

$$z^6 - z^4 - 2z^3 - z^2 + 1 = z^3\left(\left(z+\frac{1}{z}\right)^3 - 4\left(z+\frac{1}{z}\right) + 2\right),$$

so the roots of $z^6 - z^4 - 2z^3 - z^2 + 1$ on the unit circle are related to the roots of $w^3 - 4w + 2$ in $[-2, 2]$. This cubic has roots ≈ -2.214, $.539$, and 1.675. Two of the roots of $w^3 - 4w + 2$ are in $(-2, 2)$ so $z^6 - z^4 - 2z^3 - z^2 + 1$ has four roots on the unit circle.

So far our examples have had all but two roots on the unit circle and the remaining two roots are real. Is there an example where f is irreducible in $\mathbf{Q}[z]$ and all but two of its roots are on the unit circle and the other two roots are not real? No. Such a situation requires $g(z)$ to have all but one root in $[-2, 2]$ and therefore its remaining root must be real since $g(z)$ has real coefficients. When t is real and outside $[-2, 2]$, the solutions to $z + 1/z = t$ are both real (and reciprocals).

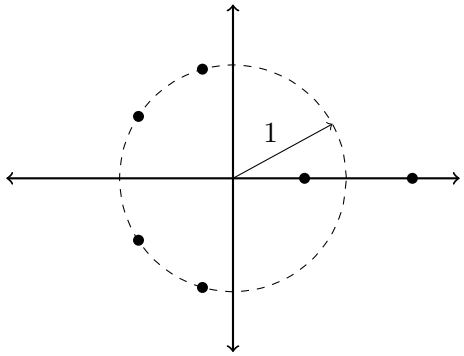

FIGURE 4. The roots of $z^6 - z^4 - 2z^3 - z^2 + 1$.

What about an example where all but four roots are on the unit circle? Let's try for at least four roots on the unit circle and four roots off. The minimal choice here would be $\deg g = 4$ with g having two roots in $[-2, 2]$ and its other two roots not being real.

Example 2.7. The polynomial $g(z) = z^4 - z - 1$ has two real roots, which are approximately $-.724$ and 1.22. Both are in $(-2, 2)$. Define

$$f(z) = z^4 g\left(z + \frac{1}{z}\right) = z^8 + 4z^6 - z^5 + 5z^4 - z^3 + 4z^2 + 1.$$

Since g has 2 roots in $(-2, 2)$ and two non-real roots, f has 4 roots that are on the unit circle and 4 roots that are off the unit circle and are not real. See Figure 5.

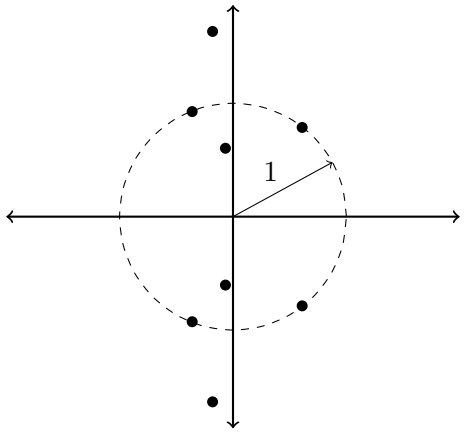

FIGURE 5. The roots of $z^8 + 4z^6 - z^5 + 5z^4 - z^3 + 4z^2 + 1$.

3. The General Case

Since Theorem 2.3 only works on palindromic polynomials, it can't be applied to non-palindromic polynomials with roots on the unit circle.

Example 3.1. The polynomial $z^{10} + 5z^8 + z^7 + 12z^6 + 2z^5 + 13z^4 + z^3 + 8z^2 - z + 2$, which is not palindromic, appears to have 4 roots on the unit circle in Figure 6.

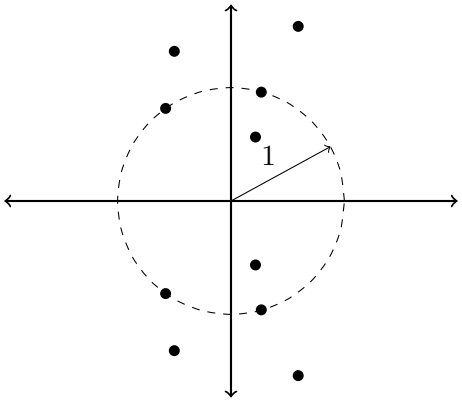

FIGURE 6. The roots of $z^{10} + 5x^8 + x^7 + 12x^6 + 2x^5 + 13x^4 + x^3 + 8x^2 - x + 2$.

How can we verify there are 4 roots on that circle? One method is to factor the polynomial. If it really has roots on the unit circle then it must be reducible in $\mathbf{Q}[z]$ since it is not palindromic. We can apply Theorem 2.3 to the irreducible factors; whichever factors have roots on the unit circle must be palindromic. However, it would be good if there were a method we could directly apply to polynomials without having to pass to their irreducible factors.

A solution suggested by F. Rodriguez Villegas is to apply a Möbius transformation to pass between the unit circle and the real line. The Möbius transformation

$$M(z) = \frac{z-i}{z+i},$$

which is illustrated in Figure 7, sends the upper half-plane onto the open unit disc and the real line onto the unit circle *without the point* 1 (although you could say ∞ is sent to 1). Its inverse is

$$M^{-1}(z) = \frac{i(1+z)}{1-z} = \frac{z+1}{i(z-1)},$$

which sends the unit circle without 1 onto the real line.

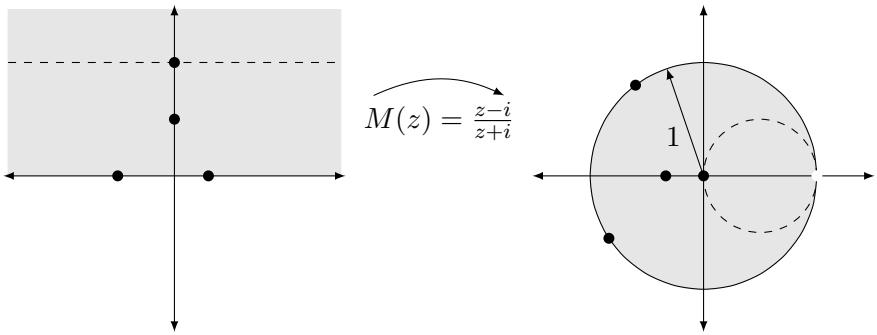

FIGURE 7. The Möbius transformation $M(z) = (z-i)/(z+i)$.

For any polynomial $f(z)$ of degree $n > 0$ (where $f(z)$ need not be palindromic and n need not be even), compose $f(z)$ with $M(z)$ and then multiply by $(z+i)^n$ to clear out the denominator: define

$$f^*(z) = (z+i)^n f(M(z)) = (z+i)^n f\left(\frac{z-i}{z+i}\right).$$

Any real root of $f^*(z)$ is transformed by $M(z)$ into a root of $f(z)$ on the unit circle. Conversely, every root of f on the unit circle other than 1 has the form $(z-i)/(z+i)$ for some real number z which is a root of f^*. Therefore counting roots of f on the unit circle is the same as counting real roots of f^* as long as we remember to check separately whether or not 1 is a root of f (which is easy). There is no special role for the interval $[-2,2]$, we don't have to double the count when passing from real roots of the auxiliary polynomial to roots of f on the unit circle, and it doesn't matter whether or not f itself has real coefficients (although we will stick to that case in examples).

Writing $f^*(z) = a(z)+ib(z)$ where $a(z)$ and $b(z)$ have real coefficients, a real root of $f^*(z)$ is the same thing as a common real root of $a(z)$ and $b(z)$, that is, a root of $\gcd(a(z), b(z))$. Thus counting roots of a $f(z)$ on the unit circle is the same as counting real roots of an auxiliary polynomial, which sounds like what we were doing before but the mechanics of it work a little differently.

Example 3.2. For Lehmer's polynomial $L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$,

$$L^*(z) = (z+i)^{10} f\left(\frac{z-i}{z+i}\right) = -z^{10} - 149z^8 + 518z^6 - 314z^4 + 43z^2 - 1.$$

Here $b(z) = 0$. There are 8 real roots of $a(z) = L^*(z)$, so $L(z)$ has 8 roots on the unit circle.

Example 3.3. Let $f(z) = z^4 - 2z^3 - 2z + 1$, from Figure 2. We have

$$f^*(z) = (z+i)^4 f\left(\frac{z-i}{z+i}\right) = -2z^4 - 12z^2 + 6 = -2(z^4 + 6z^2 - 3).$$

Again, $b(z) = 0$. There are two real roots of $a(z) = f^*(z)$ (approximately $\pm.6812$; this isn't related to the Golden ratio, which is $1.61803\ldots$), so $f(z)$ has two roots on the unit circle.

Example 3.4. Let $f(z) = z^6 - z^4 - 2z^3 - z^2 + 1$, from Figure 4. Since

$$f^*(z) = (z+i)^6 f\left(\frac{z-i}{z+i}\right) = -2z^6 - 38z^4 + 26z^2 - 2 = -2(z^6 + 19z^4 - 13z^2 - 1),$$

again $b(z) = 0$ and $a(z) = f^*(z)$. The polynomial $a(z)$ has four real roots, so $f(z)$ has four roots on the unit circle.

Example 3.5. For the polynomial $f(z) = z^8 + 4z^6 - z^5 + 5z^4 - z^3 + 4z^2 + 1$ from Example 2.7,

$$f^*(z) = 13z^8 - 72z^6 + 90z^4 - 64z^2 + 17.$$

Yet again $b(z) = 0$. The polynomial $a(z) = f^*(z)$ has 4 real roots, so $f(z)$ has 4 roots on the unit circle.

Example 3.6. We now turn to $f(z) = z^{10} + 5z^8 + z^7 + 12z^6 + 2z^5 + 13z^4 + z^3 + 8z^2 - z + 2$, from Figure 6, which seemed to have 4 roots on the unit circle but we could not directly check this with Theorem 2.3 since $f(z)$ is not palindromic. For this polynomial,

$$f^*(z) = (44z^{10} - 198z^8 + 448z^6 - 548z^4 + 260z^2 - 38) + i(22z^9 - 88z^7 + 180z^5 - 184z^3 + 38z)$$

where finally $b(z)$ is not 0. The greatest common divisor of $a(z)$ and $b(z)$ is $22z^8 - 88z^6 + 180z^4 - 184z^2 + 38 = b(z)/z$, which has 4 real roots, so $f(z)$ has 4 roots on the unit circle.

Example 3.7. Let $f(z) = z^n - 1$, so $f^*(z) = (z+i)^n - (z-i)^n$. Since the roots of $f(z)$ are all on the unit circle, $f^*(z)$ must have all real roots. Examples of the decomposition of $f^*(z)$ as $a(z) + ib(z)$ are given in Table 1. Unlike before, now it is $a(z)$ that is always 0. The roots of $b(z)$ are all real. In fact its roots are the numbers $\cot(\pi k/n)$ for $1 \leq k \leq n-1$.

n	$a(z)$	$b(z)$
1	0	-2
2	0	$-4z$
3	0	$-6z^2 + 2$
4	0	$-8z^3 + 8z$
5	0	$-10z^4 + 20z^2 - 2$
6	0	$-12z^5 + 40z^3 - 12z$

TABLE 1. Polynomials $a(z)$ and $b(z)$ for $z^n - 1$.

Example 3.8. Let $f(z) = z^6 + iz^5 + (3+i)z^4 + (1+i)z^3 + (1+3i)z^2 + z + i$. Here the coefficients are complex. The roots are plotted in Figure 2.4 and we will show there are two roots on the unit circle.

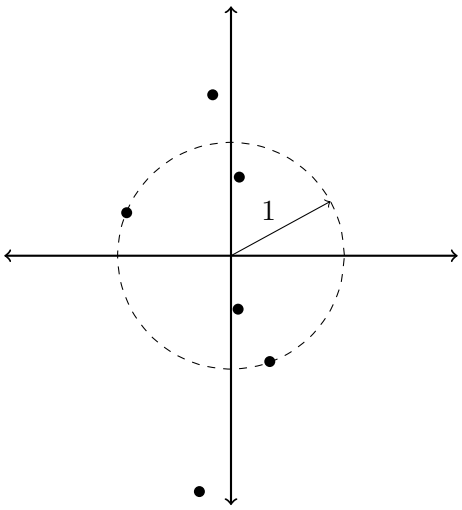

FIGURE 8. The roots of $z^6 + iz^5 + (3+i)z^4 + (1+i)z^3 + (1+3i)z^2 + z + i$.

Since

$$f^*(z) = (1+i)(7z^6 - 6z^5 - 13z^4 + 12z^3 + 9z^2 - 14z - 3),$$

both $a(z)$ and $b(z)$ equal $7z^6 - 6z^5 - 13z^4 + 12z^3 + 9z^2 - 14z - 3$, which has two real roots. Therefore $f(z)$ has two roots on the unit circle.

Since we often saw in the examples that $b(z) = 0$, it is natural to ask what makes that happen (or what makes $a(z) = 0$).

Theorem 3.9. *For $f(z) = \sum_{k=0}^{n} c_k z^k$ of degree n, write $f^*(z) = a(z) + ib(z)$, where $a(z)$ and $b(z)$ have real coefficients.*

(1) *$f(z)$ has real coefficients if and only if $f^*(-\overline{z}) = (-1)^n \overline{f^*(z)}$. Concretely: when n is even, $f(z)$ is real if and only if $a(z)$ is even and $b(z)$ is odd, and when n is odd, $f(z)$ is real if and only if $a(z)$ is odd and $b(z)$ is even.*
(2) *$a(z) = 0$ if and only if $f(z) = -z^n \overline{f(1/\overline{z})}$, while $b(z) = 0$ if and only if $f(z) = z^n \overline{f(1/\overline{z})}$. Concretely, $a(z) = 0$ if and only if $c_k = -\overline{c}_{n-k}$ for all k, while $b(z) = 0$ if and only if $c_k = \overline{c}_{n-k}$ for all k.*
(3) *If 1 is a root of f with multiplicity m then $\deg(f^*) = n - m$. In particular, f^* has degree n if and only if $f(1) \neq 0$.*
(4) *The leading coefficient of f is $f^*(-i)/(-2i)^n$.*
(5) *f has coefficients in $\mathbf{Q}(i)$ if and only if f^* has coefficients in $\mathbf{Q}(i)$.*
(6) *f has coefficients in $\mathbf{Z}[1/2, i]$ if and only if f^* has coefficients in $\mathbf{Z}[1/2, i]$.*

Part 3 explains why $b(z)$ for $z^n - 1$ in Table 1 has degree $n - 1$ rather than n.

Proof. This will involve a bit of careful computations with complex conjugation.

(1): To say $f(z)$ has real coefficients is equivalent to $f(z) = \overline{f(\overline{z})}$. This is equivalent to $f(M(z)) = \overline{f(\overline{M(z)})}$. Since $\overline{M(z)} = M(-\overline{z})$ by a direct calculation,

$$\overline{f(\overline{M(z)})} = \overline{f(M(-\overline{z}))} = \overline{\left(\frac{f^*(-\overline{z})}{(-\overline{z}+i)^n}\right)} = \frac{\overline{f^*(-\overline{z})}}{(-z-i)^n} = \frac{(-1)^n \overline{f^*(-\overline{z})}}{(z+i)^n},$$

so $f(z)$ has real coefficients if and only if $\overline{f^*(-\overline{z})} = (-1)^n (z+i)^n f(M(z)) = (-1)^n f^*(z)$. In terms of $a(z)$ and $b(z)$, $\overline{f^*(-\overline{z})} = a(-z) - ib(-z)$, so $f(z)$ has real coefficients if and only if $a(-z) = (-1)^n a(z)$ and $b(-z) = (-1)^{n-1} b(z)$.

(2): The equations $f^*(z) = a(z) + ib(z)$ and $\overline{f^*(\overline{z})} = a(z) - ib(z)$ let us solve for $a(z)$ and $b(z)$:

$$a(z) = \frac{f^*(z) + \overline{f^*(\overline{z})}}{2} \quad \text{and} \quad b(z) = \frac{f^*(z) - \overline{f^*(\overline{z})}}{2i}.$$

Therefore $a(z) = 0$ if and only if $\overline{f^*(\overline{z})} = -f^*(z)$ and $b(z) = 0$ if and only if $\overline{f^*(\overline{z})} = f^*(z)$.

For $\varepsilon = \pm 1$, the equation $\overline{f^*(\overline{z})} = \varepsilon f^*(z)$ is equivalent to

$$\overline{(\overline{z}+i)^n f(M(\overline{z}))} = \varepsilon (z+i)^n f(M(z)). \tag{3.1}$$

Since $M(\overline{z}) = \overline{M(-z)} = 1/\overline{M(z)}$, (3.1) is the same as

$$\overline{f(1/\overline{M(z)})} = \varepsilon \frac{(z+i)^n}{(z-i)^n} f(M(z)). \tag{3.2}$$

Replacing z with $M^{-1}(z) = (z+1)/(i(z-1))$ in (**??**), it becomes

$$z^n \overline{f(1/\overline{z})} = \varepsilon f(z).$$

For $\varepsilon = 1$ we get the condition for when $b(z) = 0$ and for $\varepsilon = -1$ we get the condition for when $a(z) = 0$.

(3): Write $f(z) = (z-1)^m q(z)$, where $q(1) \neq 0$. The operation $f \rightsquigarrow f^*$ is multiplicative, so $f^*(z) = ((z-1)^*)^m q^*(z) = (-2i)^m q^*(z)$. By an explicit calculation with polynomials, if $q(z)$ has degree d then the coefficient of z^d in $q^*(z)$ is $q(1) \neq 0$, so $q^*(z)$ has the same degree as q.

(4), (5), (6): These are explained by the formulas connecting $f(z)$ and $f^*(z)$:

$$f^*(z) = (z+i)^n f\left(\frac{z-i}{z+i}\right) \quad \text{and } f(z) = \left(\frac{i(z-1)}{2}\right)^n f^*\left(\frac{z+1}{i(z-1)}\right). \tag{3.3}$$

The second formula is derived by replacing z with $M^{-1}(z) = (z+i)/(i(z-1))$ in the definition $f^*(z) = (z+i)^n f(M(z))$. □

Is every polynomial $F(z)$ of the form $f^*(z)$ for some f? There is one constraint F has to satisfy, by the leading coefficient formula in the previous theorem: $F(-i) \neq 0$. This is the only obstruction.

Corollary 3.10. *For any polynomial $F(z)$ with degree N that satisfies $F(-i) \neq 0$, the polynomials $f(z)$ which satisfy $f^*(z) = F(z)$ are*

$$\left(\frac{i(z-1)}{2}\right)^{N+m} F\left(\frac{z+1}{i(z-1)}\right)$$

for $m \geq 0$. In particular, there is a unique $f(z)$ of the same degree as $F(z)$ such that $f^*(z) = F(z)$.

Proof. Since $\deg(f^*) \leq \deg f$, f needs to have degree at least N. If $f_1^*(z) = f_2^*(z)$ and $f_1(z)$ and $f_2(z)$ have the same degree then $f_1(z) = f_2(z)$. Since $(i(z-1)/2)^* = 1$, it suffices to show the polynomial

$$\left(\frac{i(z-1)}{2}\right)^{N} F\left(\frac{z+1}{i(z-1)}\right)$$

has degree N and satisfies $f^* = F$. Its degree is certainly at most N and the coefficient of z^N is $(i/2)^N F(-i) \neq 0$, so the degree is N. The reader can check this polynomial satisfies $f^*(z) = F(z)$.

□

On polynomials of a fixed degree, $f(z) \rightsquigarrow f^*(z)$ is a bijection. While it's true that if $f(z)$ has coefficients in $\mathbf{Z}[i]$ then $f^*(z)$ has coefficients in $\mathbf{Z}[i]$, the converse is false in general.

Example 3.11. When $F(z) = z^4 - 4z^2 + 2$, the solution to $f^*(z) = F(z)$ with degree 4 is

$$\left(\frac{i(z-1)}{2}\right)^{4} F\left(\frac{z+1}{i(z-1)}\right) = \frac{7}{16}z^4 - \frac{1}{4}z^3 + \frac{5}{8}z^2 - \frac{1}{4}z + \frac{7}{16}$$

In general, if $F(z) = \sum_{k=0}^N a_k z^k$ then

$$\left(\frac{i(z-1)}{2}\right)^{N} F\left(\frac{z+1}{i(z-1)}\right) = \frac{i^N}{2^N}\sum_{k=0}^{N} a_k(-i)^k(z+1)^k(z-1)^{N-k},$$

and asking for this to have z-coefficients in $\mathbf{Z}[i]$ amounts to some 2-power congruence conditions on linear combinations of the a_k's. (It's best to expand this polynomial in powers of $z-1$ rather than z, which doesn't affect whether or not coefficients are in $\mathbf{Z}[i]$.) To make sure the coefficients are in $\mathbf{Z}$ and not just $\mathbf{Z}[i]$, make sure the real and imaginary parts of $F(z)$ satisfy the even/odd conditions from Theorem 3.9, depending on the parity of N.

We can invert the process $f(z) \rightsquigarrow f^*(z)$ to generate examples of polynomials $f(z)$ in $\mathbf{Q}[z]$ with a specified number of roots on the unit circle starting with a polynomial in $\mathbf{Q}[z]$ having a specified number of real roots, but there is a lot more we have to keep track of compare to directly computing $z^m g(z+1/z)$ when $g(z)$ has enough roots in $(-2, 2)$, especially if you want $f(z)$ to be monic with integral coefficients.

4. Beyond the Unit Circle

The polynomial $z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$ has all of its roots on the circle $|z| = \sqrt{2}$ (see Figure 8). To verify this, we want to generalize the earlier theorems.

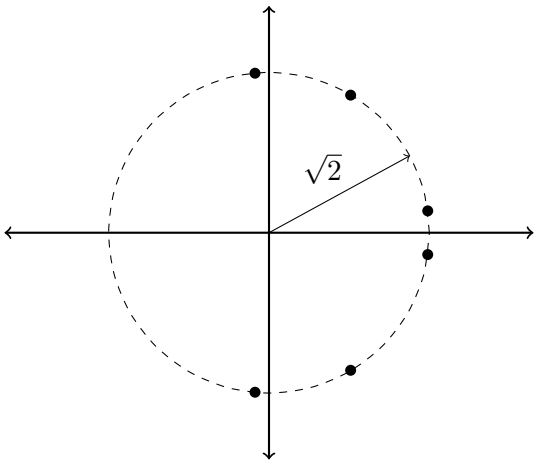

FIGURE 9. The roots of $z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$.

Theorem 4.1. *Let $f(z) \in \mathbf{Q}[z]$ be irreducible with degree $n > 1$. If $f(z)$ has a root with absolute value r, where $r^2 \in \mathbf{Q}$, then n is even and $(z/r)^n f(r^2/z) = f(z)$.*

Proof. Let α be a root of $f(z)$ with absolute value r, so $\overline{\alpha}$ is also a root and $\overline{\alpha} = r^2/\alpha$. The product $z^n f(r^2/z)$ is in $\mathbf{Q}[z]$ with degree n (the coefficient of z^n is $f(0)/r^n \neq 0$) and α is a root, so $z^n f(r^2/z) = cf(z)$ for some nonzero rational number c. Evaluating this equation at $z = r$ and then at $z = -r$, we see that $c = r^n$ and then that n is even. □

Theorem 4.2. *For a polynomial $f(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_1 z + c_0$ with even degree $n = 2m$, the following conditions are equivalent:*

1. *$c_k = r^{n-2k} c_{n-k}$ for all k,*
2. *$(z/r)^n f(r^2/z) = f(z)$,*
3. *$f(z) = (z/r)^m g(z/r + r/z)$ for a polynomial g of degree m.*

Proof. Apply Theorem 2.1 to $f(rz)$. □

Theorem 4.3. *For a polynomial $f(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_1 z + c_0$ of even degree satisfying $c_k = r^{n-2k} c_{n-k}$ for all k, write $f(z) = (z/r)^m g(z/r + r/z)$. The roots of f on the circle of radius r, considered as pairs $\{\alpha, r/\alpha\}$, correspond to the roots of g in the interval $[-2, 2]$ by $\{\alpha, 1/\alpha\} \leftrightarrow \alpha/r + r/\alpha$.*

Proof. Apply Theorem 2.3 to $f(rz)$. □

Example 4.4. To show $f(z) = z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$ from Figure 8 has its roots on the circle of radius $\sqrt{2}$, first check it satisfies either of the first two conditions of Theorem 4.2 when $r = \sqrt{2}$. Then it satisfies the third condition, and explicitly

$$f(z) = \left(\frac{z}{\sqrt{2}}\right)^3 \left(8\left(\frac{z}{\sqrt{2}} + \frac{\sqrt{2}}{z}\right)^3 - 16\sqrt{2}\left(\frac{z}{\sqrt{2}} + \frac{\sqrt{2}}{z}\right)^2 + 12\left(\frac{z}{\sqrt{2}} + \frac{\sqrt{2}}{z}\right) + 2\sqrt{2}\right).$$

The polynomial $8w^3 - 16\sqrt{2}w^2 + 12w + 2\sqrt{2}$ has all real roots (approximately $-.174, 1.021$, and 1.981) which are all in the interval $(-2, 2)$. Therefore $f(z)$ has all of its roots on the circle of radius $\sqrt{2}$ around the origin.

We can also count roots on the circle of radius r using the Möbius transformation

$$M_r(z) = r\frac{z-i}{z+i},$$

which sends the real line onto the circle of radius r, excluding the number r.

Example 4.5. When $f(z) = z^6 - 4z^5 + 9z^4 - 15z^3 + 18z^2 - 16z + 8$,

$$(z+i)^6 f\left(\sqrt{2}\frac{z-i}{z+i}\right) = (88-62\sqrt{2})z^6 + (-168+70\sqrt{2})z^4 + (168+70\sqrt{2})z^2 + (-88-62\sqrt{2}).$$

This polynomial has 6 real roots, so all the roots of f have absolute value $\sqrt{2}$.

Of course it is a pain to juggle $\sqrt{2}$ in these computations. Instead we could show $|\alpha^2/2| = 1$ for any root α of $f(z)$. The numbers $\alpha^2/2$ are roots of $h(z) = 8z^6 + 8z^5 - 6z^4 - 13z^3 - 6z^2 + 8z + 8$ and

$$h^*(z) = 7z^6 - 371z^4 + 133z^2 - 1,$$

which has 6 real roots.

Appendix A. The Geometry of $z + 1/z$

The function $z + 1/z$, particularly how it relates the unit circle and $[-2, 2]$, was used in Section 2 to count roots of a polynomial on the unit circle. We take a closer look here at the geometric effect of this function on the complex plane.

On $\mathbf{C}$, inversion $z \mapsto 1/z$ exchanges the interior and exterior of the unit circle (ignoring the origin) and also the upper and lower half-planes. See Figure 9, where, for instance, the regions marked A and $1/A$ are exchanged. and try to get a feel for how the different parts of the plane get moved around (*e.g.*, regions A and B share a border and so do their inverse regions $1/A$ and $1/B$). This process is quite simple on the unit circle, where inversion is just reflection across the x-axis.

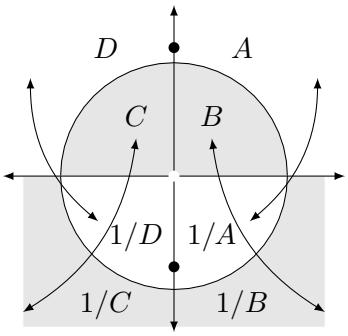

Figure 10. The function $1/z$.

If we look instead at the function $z \mapsto z + 1/z$ on the complex plane (ignoring the origin) then something quite different occurs. This function is 2-to-1 rather than 1-to-1: z and $1/z$

both go to the same place under $z + 1/z$, so the regions A and $1/A$ have the same values, and likewise for other pairs of inverse regions. What happens to the upper half-plane under $z \mapsto z + 1/z$ is illustrated in Figure 10: the regions B and C are spread out to the two quadrants in the lower half-plane and the regions A and D each fill up a whole quadrant in the upper half-plane. So $z + 1/z$ sends the upper half-plane onto the whole complex plane except for $(-\infty, -2]$ and $[2, \infty)$, which are doubly covered by the real line without 0. In the same way $z + 1/z$ on the lower half-plane fills up the complex plane.

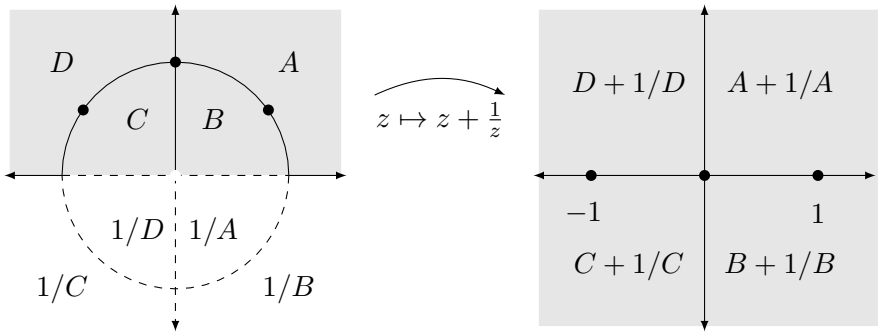

FIGURE 11. The function $z + 1/z$.

The circular arc from i to 1, which separates A and B, turns into the segment $[0, 2]$ on the real line. However, the boundary separating $A + 1/A$ and $B + 1/B$ is the whole positive x-axis, not just $[0, 2]$. Where did the part of the boundary $[2, \infty)$ between $A + 1/A$ and $B + 1/B$ come from? The explanation is that we should not forget the 2-to-1 nature of $z + 1/z$: we should look at where A has a common boundary with both B and $1/B$, not just $1/B$. That means not only the arc from i to 1 between A and B but also the interval $[1, \infty)$ between A and $1/B$. Under $z \mapsto z + 1/z$ the interval $[1, \infty)$ becomes $[2, \infty)$.

REFERENCES

[1] D. H. Lehmer, *Factorization of Certain Cyclotomic Functions*, Ann. of Math. **34** (1933), 461–479.