Math 539
Stuff I Learned

Prompted by my confusion near the end of class on Wednesday, November 30, I went ahead and looked things up about algebraic numbers on the unit circle. Writing up these comments might be randomly helpful to you, but really I'm doing it to cement my own newfound understanding.

DEFINITIONS AND BACKGROUND. A complex number is *algebraic* if it is the root of some polynomial with integer coefficients (not identically zero). Every algebraic number has a *minimal polynomial* of smallest degree (unique up to scaling by integers); this minimal polynomial is irreducible over $\mathbb{Q}$, and its degree is called the *degree* of the algebraic number.

If α is an algebraic number of degree d, then the field $\mathbb{Q}(\alpha)$ is a d-dimensional vector space over $\mathbb{Q}$; in particular, any $d+1$ distinct powers of α are linearly dependent over $\mathbb{Q}$. Applying this fact to $1, \alpha^k, \alpha^{2k}, \dots, \alpha^{dk}$, this implies that for every integer k, the power α^k is an algebraic number of degree at most d.

The *conjugates* of an algebraic number are the roots of its minimal polynomial (including the number itself).

The set of all algebraic numbers is a subfield of $\mathbb{C}$, in fact the smallest algebraically closed subfield; it is called the *algebraic closure of the rational numbers*. It is a countable set, since the set of all polynomials with integer coefficients is countable.

A number is an *algebraic integer* if it is the root of some monic polynomial with integer coefficients, or equivalently if its minimal polynomial can be chosen to be monic. The set of all algebraic integers forms a subring of $\mathbb{C}$; it is a dense subset of $\mathbb{C}$.

Let $s_{n,m}$ denote the mth *symmetric polynomial* in n variables: if A is a set of n complex numbers (not necessarily distinct), then

$$s_{n,m}(A) = \sum_{\substack{B\subset A \\ |B|=m}} \prod_{b\in B} b.$$

So for example, $s_{5,3}(\{t_i\}) = t_1t_2t_3 + t_1t_2t_4 + t_1t_2t_5 + \cdots + t_3t_4t_5$, and $s_{n,1}$ is just the sum of its n arguments and $s_{n,n}$ is the product of its n arguments.

Let $D = \{z \in \mathbb{C}\colon |z| \le 1\}$ denote the unit disk and $S = \{z \in \mathbb{C}\colon |z| = 1\}$ the unit circle.

KRONECKER'S THEOREM. *Suppose that α is an algebraic integer such that all of the conjugates of α lie within D. Then α is a root of unity.*

Note that the primitive mth roots of unity, $e^{2\pi i\ell/m}$ where $(\ell, m) = 1$, are all the conjugates of one another, and hence roots of unity do satisfy the hypothesis of the theorem. Note also that the theorem fails for algebraic numbers, since we can just take any algebraic number and divide it by a huge integer to force all of its conjugates to lie in D.

PROOF (courtesy of Vishaal). Let $p(t)$ be the minimal polynomial of α, and let d be the degree of $p(t)$. If $\alpha = \alpha_1, \dots, \alpha_d$ are the roots of $p(t)$, then

$$p(t) = x^d - s_{d,1}(\{\alpha_i\})x^{d-1} + s_{d,2}(\{\alpha_i\})x^{d-1} - \cdots + (-1)^d s_{d,d}(\{\alpha_i\}).$$

Now each $|\alpha_i| \le 1$, and so $s_{d,j}(\{\alpha_i\})$ is the sum of $\binom{d}{j} \le 2^d$ terms each bounded in modulus by 1. Therefore $p(t)$ belongs to the finite set F of monic polynomials of degree d each of whose coefficients is an integer bounded in absolute value by 2^d.

Now the conjugates of α^k are just α_i^k $(1 \le i \le d)$. Therefore the same argument applies, showing that the minimal polynomial of each α^k is in F as well. Since F is a finite set, we can find a polynomial $f(t) \in F$ that is the minimal polynomial of at least $d+1$ powers of α. But $f(t)$ has degree d, and so two of these powers of α coincide, which means that α is a root of unity.

(We've glossed over the fact that α^k might in fact be an algebraic integer of degree lower than d, in which case its conjugates are still α_i^k but now these kth powers of conjugates are not distinct. The details can be worked out.) □

However, it is false that an algebraic integer on S must be a root of unity. One important class of counterexamples is related to *Salem numbers*: An algebraic integer, not in D, is a Salem number if all of its other conjugates are in D. It can be shown that a Salem number must have even degree $d \ge 4$ and that one of its conjugates lies in $D \setminus S$ but the rest of its conjugates lie on S. Therefore these remaining $d-2$ conjugates are algebraic integers on S that are not roots of unity. An example of two such algebraic integers is

$$\frac{1}{4}\left(1 - \sqrt{13} \pm i\sqrt{2(\sqrt{13}+1)}\right).$$

One can verify that these are on S. These are two of the roots of the irreducible polynomial

$$t^4 - t^3 - t^2 - t + 1 = \left(t^2 - \frac{1+\sqrt{13}}{2}t + 1\right)\left(t^2 - \frac{1-\sqrt{13}}{2}t + 1\right),$$

the other two roots being

$$\frac{1}{4}\left(1 + \sqrt{13} \pm \sqrt{2(\sqrt{13}-1)}\right).$$

In any case, the factor $i^a q^{1/2}/\tau(\chi)$ in the functional equation for Dirichlet L-functions is manifestly an algebraic number, but it does not in fact have to be an algebraic integer. The simplest example uses the character χ (mod 5) for which $\chi(2) = i$ (and so $\chi(4) = -1$ and $\chi(3) = -i$). This character is odd, so $a = 1$; and the quantity

$$\frac{i^a q^{1/2}}{\tau(\chi)} = \frac{i\sqrt{5}}{e^{2\pi i/5} + ie^{4\pi i/5} - ie^{6\pi i/5} - e^{8\pi i/5}}$$

turns out to equal $\sqrt[4]{-(3+4i)/5}$, more precisely the fourth root of $-(3+4i)/5$ that lies in the first quadrant. This number is a root of the irreducible polynomial $5t^8 + 6t^4 + 5$, hence is not an algebraic integer.