# MATH 129, HW 4

Bryden Cais

March 4, 2002

## 1 Units, roots of unity, and the unit circle

1. Suppose that a monic polynomial $P(X) = c_0 + c_1 X + \cdots + X^N \in \mathbf{Z}[X]$ has roots $\alpha_1, \ldots, \alpha_N$ with $|\alpha_j| < A$ for some $A > 0$ and all $j$. Since the coefficients of $P$ are given as the elementary symmetric functions in the roots of $P$, we may write

$$c_{N-k-1} = \sum_{j_0 < \cdots < j_k} \alpha_{j_0} \cdots \alpha_{j_k},$$

from which we obtain the inequality

$$|c_{N-k-1}| \leq \binom{N}{k+1} |A|^{k+1},$$

which shows that all the coefficients of $P$ are bounded. Since $P \in \mathbf{Z}[X]$, there can only be finitely many such $P$ of a given degree $N$.

2. Because of containment properties, if we show that $\mu(\mathbf{Z}^{\mathrm{ab}}) = \mu$, we have shown that $\mu(\bar{\mathbf{Z}}) = \mu(\mathbf{Q}^{\mathrm{ab}}) = \mu(\bar{\mathbf{Q}}) = \mu$. To see that $\mu(\mathbf{Z}^{\mathrm{ab}}) = \mu$, notice that $\mu(\mathbf{Z}^{\mathrm{ab}}) \subset \mu$ by definition, and that we have $\mu \subset \mu(\mathbf{Z}^{\mathrm{ab}})$ because any root of unity $\alpha$ has irreducible polynomial $\Phi_d$ (where $\Phi_d$ is the d th cyclotomic polynomial) for some $d$ and the galois group of $\Phi_d$ is $(\mathbf{Z}/d\mathbf{Z})^*$, and is hence abelian. That is, any root of unity is in $\mathbf{Z}^{\mathrm{ab}}$.

We next show that $V(\bar{\mathbf{Z}}) = \mu$, and therefore also that $V(\mathbf{Z}^{\mathrm{ab}}) = \mu$, since obviously $V(\bar{\mathbf{Z}}) \supset V(\mathbf{Z}^{\mathrm{ab}})$ and $\mu \subset V(\mathbf{Z}^{\mathrm{ab}})$ since every conjugate of a root of unity as a root of some cyclotomic polynomial and is thus a root of unity itself. Let $x \in V(\bar{\mathbf{Z}})$ have monic irreducible polynomial

$P$ of degree $N$. Consider $x, x^2, x^3, \ldots$. For each $j$, we have that the minimal polynomial of $x^j$ has degree $N$ or less since $x^j \in \mathbf{Q}(x)$ and $[\mathbf{Q}(x) : \mathbf{Q}] = N$. Moreover, since all the conjugates of $x$ have absolute value 1, so do all the conjugates of $x^j$. Finally, the minimal polynomial of $x^j$ is in $\mathbf{Z}[X]$ since $x$ is integral, and thus so is any symmetric function in any of the conjugates of $x^j$. We can reinterpret the result of item 1 in the following useful way: there are at most a finite number of distinct algebraic integers of absolute value less than $A > 0$ and degree less than or equal to $N > 0$. Clearly, an infinite number of such algebraic integers would imply an infinite number of monic polynomials of degree at most $N$ with roots bounded in absolute value by $A$, and this contradicts item 1. Therefore, there are only a finite number of distinct $x^j$, so that we have $x^i = x^j$ for some $i \neq j$ and therefore that $x$ is a root of unity.

Now we show that $V(\mathbf{Q}^{\mathrm{ab}}) = U(\mathbf{Q}^{\mathrm{ab}})$ and therefore also that $U(\mathbf{Z}^{\mathrm{ab}}) = \mu$ since, again, $\mathbf{Z}^{\mathrm{ab}} \subset \mathbf{Q}^{\mathrm{ab}}$. Observe that complex conjugation $x \longrightarrow \bar{x}$ is always an automorphism of the galois group of $\mathbf{Q}(\alpha)$ for any $\alpha \in \mathbf{Q}^{\mathrm{ab}}$. Since this galois group is assumed to be abelian, any $\sigma \in G_{\mathbf{Q}}$ commutes with complex conjugation. Therefore, if $x\bar{x} = 1$, $1 = \sigma(x\bar{x}) = \sigma(x)\sigma(\bar{x}) = \sigma(x)\bar{\sigma(x)} = |\sigma x|$ so that $x \in V(\mathbf{Q}^{\mathrm{ab}})$. Since obviously $V(\mathbf{Q}^{\mathrm{ab}}) \subset U(\mathbf{Q}^{\mathrm{ab}})$, we have $V(\mathbf{Q}^{\mathrm{ab}}) = U(\mathbf{Q}^{\mathrm{ab}})$.

Next, we show that $V(\bar{\mathbf{Z}}) \neq U(\bar{\mathbf{Z}})$ and therefore that $V(\bar{\mathbf{Q}}) \neq U(\bar{\mathbf{Q}})$ because of containment. To do this, we must produce some element of $\bar{\mathbf{Z}}$ of norm 1 that has a conjugate not of norm 1. We claim that

$$\gamma = (2 - \sqrt{3})(\sqrt{7} + 2i\sqrt[4]{3})$$

is such an algebraic integer. To see this, first observe that $\gamma \in \bar{\mathbf{Z}}$, clearly, and that the square of the absolute value of $\gamma$ is $(2-\sqrt{3})^2(7 + 4\sqrt{3}) = (2-\sqrt{3})^2(2+\sqrt{3})^2 = 1$. Moreover, the automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ which sends $i\sqrt[4]{3}$ to $\sqrt[4]{3}$ sends $\gamma$ to $(2+\sqrt{3})(\sqrt{7} + 2\sqrt[4]{3})$, which evidently does not have norm 1.

It is not difficult to show that $U$ and $U(\bar{\mathbf{Q}})$ are distinct. For example, the algebraic numbers are countable (by a standard argument of Cantor), but the set of points on the unit circle is not countable, so that there exist uncountably many complex numbers of absolute value 1 that are not algebraic.

Now we show that $U(\bar{\mathbf{Z}})$ is distinct from $U(\bar{\mathbf{Q}})$, $V(\mathbf{Q}^{\mathrm{ab}})$, and that $\mu$ is distinct from $V(\mathbf{Q}^{\rm ab})$. To do this, we consider

$$\beta = \frac{3+i\sqrt{7}}{4}.$$

Notice that $|\beta| = 1$ and that $\beta \in \bar{\mathbf{Q}} \setminus \bar{\mathbf{Z}}$ since its minimal polynomial is $X^2 - (3/2)X + 1$. Moreover, we in fact have $\beta \in \mathbf{Q}^{\rm ab}$ since $\beta$ lies in a degree two extension of $\mathbf{Q}$. For this same reason, all of the conjugates of $\beta$ have norm 1, so that $\beta \in V(\mathbf{Q}^{\rm ab}) \setminus \bar{\mathbf{Z}}$. Finally, $\beta$ is not a root of unity since it is not in $\bar{\mathbf{Z}}$.

It remains to show that $V(\bar{\mathbf{Q}}) \neq V(\mathbf{Q}^{\rm ab})$.

3. First, every $\alpha \in K$ satisfies a minimial polynomial of degree less than or equal to $N = [K : \mathbf{Q}]$. Thus, $K \cap \mu$ is finite by item 1, since every root of unity has minimal polynomial of degree less than or equal to $N$ with all roots of absolute value 1. Second, $K \cap \mu$ is a subgroup of $\mathcal{O}_K^*$ since every root of unity is invertable and the product of two roots of unity is again a root of unity. Finally, this is in fact a cyclic subgroup since if $K \cap \mu$ contains roots of unity of order $a$, $b$, then it contains a root of unity of order $\mathrm{lcm}(a, b)$. (This is a standard fact from elementary number theory). Thus, there is some root of unity $\rho \in K \cap \mu$ with order a multiple of the order of any other root of unity, so that $K \cap \mu =< \rho >$ is cyclic.

4. Let $\alpha \in \bar{\mathbf{Z}}$ and suppose that all of the conjugates of $\alpha$ are in a disc centered at $\alpha$ of radius 1/4. Then we have $|\alpha - \sigma(\alpha)| < 1/4$ for any $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Now let $\sigma_1, \ldots, \sigma_n$ denote the distinct conjugates of $\alpha$. Then for any $i$, $j$, we have $|\sigma_i(\alpha) - \sigma_j(\alpha)| < 1/2$, and therefore, by our formula for $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$, we have

$$|\,\mathrm{disc}(\alpha)| = \left| \prod_{i \neq j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \right| < 1.$$

Since $\alpha \in \bar{\mathbf{Z}}$, we have $\mathrm{disc}(\alpha) \in \mathbf{Z}$, and therefore $\mathrm{disc}(\alpha) = 0$. This implies that $1, \alpha, \ldots, \alpha^{n-1}$ are not linearly independent over $\mathbf{Q}$, and therefore that $n = 1$, that is, $\alpha \in \mathbf{Q}$. Since $\alpha$ is rational algebraic integer, it is in $\mathbf{Z}$.

## 2 A computation

We already know from class that the ring of integers of $K_1 = \mathbf{Q}[\zeta_5]$ is $\mathbf{Z}[\zeta_5]$, and that $\mathrm{disc}(K_1) = 125$. We now show that the ring of integers of $K_2 = \mathbf{Q}[\sqrt[5]{2}]$ is $\mathbf{Z}[\sqrt[5]{2}]$. We have the inclusions

$$\mathbf{Z}[\sqrt[5]{2}] \subset \mathcal{O}_{K_2} \subset \frac{1}{N(P'(\sqrt[5]{2}))}\mathbf{Z}[\sqrt[5]{2}],$$

where $P(x) = X^5 - 2$. Using the known imbeddings of $K_2$ in $\mathbf{C}$, we easily compute

$$N(P'(\sqrt[5]{2}) = N(10/\sqrt[5]{2}) = 5 \cdot 10^4 = \mathrm{disc}(K_2).$$

Now, it is obvious that $\mathbf{Z}[\sqrt[5]{2}] = \mathbf{Z}[\sqrt[5]{2} - 2]$. Moreover, since the minimal polynomial of $\sqrt[5]{2}$ is $P(X) = X^5 - 2$, the minimal polynomial of $\sqrt[5]{2} - 2$ is $P(X+2) = X^5 + 10X^4 + 40X^3 + 80X^2 + 80X + 30$. Thus, since $P(X)$ is 2-Eisenstein and $P(X+2)$ is 5-Eisenstein, we see that multiplication by the primes $2,\ 5$ is injective on $\mathcal{O}_{K_2}/\mathbf{Z}[\sqrt[5]{2}]$. But since the index of $\mathbf{Z}[\sqrt[5]{2}]$ in $K_2$ divided $\mathrm{disc}(K_2) = 5 \cdot 10^4$, we see that in fact $\mathcal{O}_{K_2}/\mathbf{Z}[\sqrt[5]{2}] = 0$, so that $\mathcal{O}_{K_2}$ is as claimed. Now, since $K_2$ is of degree 5 over $\mathbf{Q}$ and $K_1$ is of degree 4, we find that $K_1K_2 = \mathbf{Q}(\sqrt[5]{2}, \zeta_5)$ is of degree 20. Hence, we have the following inclusions (since $\gcd(\mathrm{disc}(K_1), \mathrm{disc}(K_2)) = 125$)

$$\mathbf{Z}[\sqrt[5]{2}, \zeta_5] = \mathbf{Z}[\sqrt[5]{2}][\zeta_5] \subset T \subset \frac{1}{125}\mathbf{Z}[\sqrt[5]{2}, \zeta_5],$$

where $T$ is the ring of integers of $K_1K_2$.

## 3 The sign of the discriminant

We know that

$$\mathrm{disc}(K) \ = \ |\sigma_i(\alpha_j)|^2,$$

where $\sigma_1, \dots, \sigma_n$ denote the $n$ distinct embeddings of $K$ in $\mathbf{C}$ and $\alpha_1, \dots, \alpha_n$ is an integral basis for $K$. Consider

$$x \ = \ |\sigma_i(\alpha_j)|.$$

We have

$$\bar{x} \ = \ |\bar{\sigma}_i(\alpha_j)|,$$

where $\bar{\sigma}$ denotes the automorphism $\tau\sigma$ where $\tau$ is complex conjugation. If $\sigma$ is a real embedding of $K$ then $\sigma = s\bar{i}gma$, otherwise $\bar{\sigma}$ and $\sigma$ are distinct. Since the sign of the determinant is changed when we swap columns or rows, it is not difficult to see that

$$\bar{x} \ = \ (-1)^k x,$$

where $k$ is the number of pairs of complex embeddings (since complex conjugation of the matrix $(\sigma_i(\alpha_j))$ swaps precisely $k$ rows). Therefore, since

$$[K : \mathbf{Q}] = 2k + r$$

where $r$ is the number of real embeddings, we see that $k = ([K : \mathbf{Q}] - r)/2$. Now if $k$ is even, then $\bar{x} = x$ so that the determinant $|\sigma_i(\alpha_j)|$ is real and hence its square is positive. On the other hand, if $k$ is odd, $\bar{x} = -x$ so that the determinant $|\sigma_i(\alpha_j)|$ is pure imaginary and its square is negative. Thus, we see that the sign of the discriminant is

$$(-1)^k \ = \ (-1)^{\frac{[K:\mathbf{Q}]-r}{2}}.$$