MATH 154. HOMEWORK 4

1. (*i*) Prove that if $n \geq 1$ is odd and ζ_n is a primitive nth root of unity then $-\zeta_n$ is a primitive $2n$th root of unity. In particular, $\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_{2n})$ when n is odd. The rest of this exercise shows via Galois theory that this is the *only* case when $\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{m'})$ for $m' \neq m$.

(*ii*) Prove that the natural isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \simeq (\mathbf{Z}/m\mathbf{Z})^\times$ respects multiplicative change in m in the sense that if $m|m'$ then the diagram of natural maps

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_{m'})/\mathbf{Q}) & \xrightarrow{\simeq} & (\mathbf{Z}/m'\mathbf{Z})^\times \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) & \xrightarrow[\simeq]{} & (\mathbf{Z}/m\mathbf{Z})^\times \end{array}$$

(restriction on left, reduction on right) commutes: going around both ways gives the same composite map.

(*iii*) Using (*ii*), prove that if $m_1, m_2|M$ then $\mathbf{Q}(\zeta_{m_1}) \cap \mathbf{Q}(\zeta_{m_2}) = \mathbf{Q}(\zeta_{\gcd(m_1,m_2)})$ inside of $\mathbf{Q}(\zeta_M)$.

(*iv*) Prove that if $\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_m)$ with $n \neq m$ then either $m = 2n$ with n odd or $n = 2m$ with m odd. (Hint: Using (*iii*), reduce to the case $m|n$. Then study the *commutative* diagram in (*ii*).) Deduce that the group of roots of unity in $\mathbf{Q}(\zeta_n)$ consists of *exactly* the nth roots of unity except when n is odd, in which case it consists of the $2n$th roots of unity.

2. Let K be a number field. This exercise explores some issues related to $\mathscr{O}_K^\times$.

(*i*) For $\alpha \in \mathscr{O}_K$ prove that $\alpha \in \mathscr{O}_K^\times$ if and only if $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \pm 1$. (Hint: First reduce to the case $K = \mathbf{Q}(\alpha)$ via norm-transitivity, then use the relationship of $\mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ with the minimal polynomial of α over $\mathbf{Q}$.)

(*ii*) Give an example of a quadratic field K and $\alpha \in K$ not in $\mathscr{O}_K$ such that $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \pm 1$.

(*iii*) Choose $\alpha \in \mathscr{O}_K$. If α is a root of unity prove that $|\sigma(\alpha)| = 1$ for all embeddings $\sigma : K \to \mathbf{C}$. Then prove the converse, due to Kronecker. (Hint for converse: show that the degree and the coefficients in $\mathbf{Z}$ (!) of the minimal polynomial f_α of such an α are *bounded in terms of* $[K : \mathbf{Q}]$. Deduce the same bounds for each f_{α^m} for $m \geq 1$, and then that there are only *finitely many* possibilities for the f_{α^m}'s as m varies.) Note that $(3/5) + (4/5)i$ is a counterexample if we do not require $\alpha \in \mathscr{O}_K$.

3. Let $\mathscr{O} \subseteq \mathscr{O}_K$ be a subring (so it is finite free as a $\mathbf{Z}$-module, with rank $\leq [K : \mathbf{Q}]$ and $1 \in \mathscr{O}$). We call $\mathscr{O}$ an *order* in K if it has $\mathbf{Z}$-rank $[K : \mathbf{Q}]$. For example, if $K = \mathbf{Q}(\alpha)$ with $\alpha \in \mathscr{O}_K$ then $\mathbf{Z}[\alpha]$ is an order in K.

(*i*) Show that $\mathscr{O}$ is an order in K if and only if $\mathscr{O}$ has finite index in $\mathscr{O}_K$ as an abelian group.

(*ii*) If a number field F is a compositum of subfields K and K', prove $\mathscr{O}_K\mathscr{O}_{K'}$ is an order in F. (Hint: show $\mathscr{O}_K\mathscr{O}_{K'}$ spans F over $\mathbf{Q}$ and deduce $[\mathscr{O}_F : \mathscr{O}_K\mathscr{O}_{K'}] < \infty$ via the structure of modules over a PID.)

(*iii*) Assume $[K : \mathbf{Q}] = 2$. Using that $\mathscr{O}_K = \mathbf{Z} \oplus \mathbf{Z}\alpha$ for some α, prove that $\mathbf{Z} + f\mathscr{O}_K$ is an order in K with index f in $\mathscr{O}_K$. Then prove that it is the *only* order in K with index f. (Hint: if $\mathscr{O} \subseteq \mathscr{O}_K$ is an order, use the structure of $\mathscr{O}_K$ to show the finite group $\mathscr{O}_K/\mathscr{O}$ is cyclic.)

4. Let $M = (a_{ij})$ be an $n \times n$ matrix with entries in a field L, and let $M' = (a'_{i'j'})$ be an $n' \times n'$ matrix with entries in L. For a fixed choice of enumeration of the set of nn' ordered pairs (k, k') with $1 \leq k \leq n$ and $1 \leq k' \leq n'$, the $nn' \times nn'$ matrix $T_{M,M'} = (a_{ij}a'_{i'j'})_{(i,i'),(j,j')}$ makes sense.

(*i*) Prove that $\det(T_{M,M'})$ is independent of the choice of enumeration of the set of such ordered pairs (k, k'), and that if $N = (b_{ij})$ and $N' = (b'_{i'j'})$ then $T_{MN,M'N'} = T_{M,M'}T_{N,N'}$.

(*ii*) If M and M' are upper triangular, show that T is upper triangular for a suitable ordering of the set of pairs (k, k'). Deduce that $\det(T_{M,M'}) = \det(M)^{n'} \det(M')^n$ when M and M' are upper triangular.

(*iii*) Use the multiplicativity in (*i*) to deduce that $\det(T_{M,M'})$ is invariant under replacing M or M' with conjugates AMA^{-1} or $A'M'A'^{-1}$ respectively.

(*iv*) Using (*ii*) and (*iii*), prove in general that $\det(T_{M,M'}) = \det(M)^{n'} \det(M')^n$ by first increasing the field to acquire enough eigenvalues so that M and M' become upper-triangularized after suitable conjugations.

Remark. If you are familiar with tensor products, this exercise can be deduced more conceptually by constructing a natural isomorphism $\wedge^n(V) \otimes \wedge^{n'}(V') \simeq \wedge^{nn'}(V \otimes V')$ for vector spaces V and V' with respective dimensions n and n'. The key point is the *naturality* of the isomorphism.