

1. As we've discussed in class, the cyclotomic extension $\mathbb{Q}(\zeta_n)$ has Galois group $\Gamma(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where the element $a + n\mathbb{Z}$ corresponds to the automorphism characterized by $\zeta_n \mapsto \zeta_n^a$. Call this automorphism ϕ_a (note that $\phi_a = \phi_{a'}$ if $a \equiv a' \pmod{n}$). Consider the order-two subgroup $H = \{\phi_1, \phi_{-1}\}$. Prove that for p prime, $H^\dagger = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and that $[\mathbb{Q}(\zeta_p) : H^\dagger] = 2$. (This should also be true for nonprime n , and you may find that your proof works just as well in that case.)
2. This problem is meant to add some specificity to a vague step in our characterization of constructible points in the plane. Let $a, b \in \mathbb{C}$ be two distinct points. Prove that the line connecting a and b consists of all complex numbers z such that $z - a = \lambda(b - a)$ for some *real* number λ , and this in turn is equivalent to the equation

$$(\bar{a} - \bar{b})z - (a - b)\bar{z} = \bar{a}b - a\bar{b}.$$

Conclude that the line is characterized by an equation $\bar{z} = uz + v$, where $u, v \in \mathbb{Q}(a, b, \bar{a}, \bar{b})$.

3. Prove, as asserted in class, that if $\gcd(m, n) = 1$, then there exists integers u, v such that $\zeta_{mn} = \zeta_m^u \zeta_n^v$. Deduce that $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$.
4. Textbook exercise 7.8 (p. 96)
5. Textbook exercise 8.3 (p. 120; see p. 111 for a definition of elementary symmetric polynomials)
6. Textbook exercise 8.7
7. Textbook exercise 8.8