Math 538: Problem Set 5 (optional)

Do a good amount of problems; choose problems based on what you already know and what you need to practice. Examples are important.

Problems

1. (Discriminants)
   (a) Let $f(x) = x^n + b$. Show that $D(f) = (-1)^{\frac{n(n=1)}{2}} n^n b^{n-1}$.
   (b) Let $f(x) = g(x) \cdot (x - \alpha)$ for some polynomial $g(x)$. Show that $D(f) = D(g)g(\alpha)^2 = D(g)\left(f'(\alpha)\right)^2$.
   (c) Let $f(x) = x^n + ax + b$. Show that $(-1)^{\frac{n(n=1)}{2}} D(f) = (-1)^{(n-1)}(n-1)^{(n-1)}a^n + n^n b^{n-1}$.
   (d) Let $f(x) = x^{2n} + ax^2 + b$. Find the discriminant of f.

2. (The discriminant of cyclotomic fields) For an integer n write $K_n = \mathbb{Q}(\zeta_n)$. p always denotes a prime number.
   (a) Show that the discriminant of K_p is $(-1)^{\phi(p)/2} p^{p-1}$.
   (b) Show that the discrimimant of K_{p^k} is $\pm p^{(kp-k-1)p^{k-1}}$.
   (c) Let $p^k \| n$. We have seen in class that the extension $K_n : K_{p^k}$ is unramified at p. Use this to calculate the p-part of the discriminant of K_n and conclude that this discriminant is
   $$\pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$
   (d) Show that $\mathbb{Q}(\zeta_n) \simeq \mathbb{Q}(\zeta_m)$ as fields iff $n = m$ or $n = 2m$ with m odd or $m = 2n$ with n odd.

3. (The unit Theorem) Call a triangle *almost equilateral* if is not equilateral, but its sides are integers and any two differ by at most 1. Show that there are infinitey many almost equilateral triangles with integral area.

The class number

4. (Another proof that the class group is finite) Let K be a number field, $[K : \mathbb{Q}] = n$, and fix an integral basis $\{\omega_i\}_{i=1}^n \subset \mathcal{O}_K$.
   (a) Let $\mathfrak{a} \lhd \mathcal{O}_K$ be non-zero, let $N = [\mathcal{O}_K : \mathfrak{a}] = N_{\mathbb{Q}}^K \mathfrak{a}$ and let $A = \left\{ \sum_{i=1}^n a_i \omega_i \mid a_i \in \mathbb{Z} \cap \left[0, N^{1/n} + 1\right] \right\}$. Show that there are distinct $\alpha, \beta \in A$ such that $\gamma = \alpha - \beta \in \mathfrak{a}$.
   (b) Show that that there is a constant C, depending only on the choice of the ω_i, such that $\left| N_{\mathbb{Q}}^K \gamma \right| \leq C \cdot N$.
   (c) Defining $\mathfrak{b}$ by $(\gamma) = \mathfrak{a}\mathfrak{b}$ show that $N_{\mathbb{Q}}^K \mathfrak{b} \leq C$.
   (d) Conclude that $\mathrm{Cl}(K)$ is finite.

5. Suppose that the class group is represented by ideals all of whom have norm at most C'. Show that the class group is generated by the prime ideals of norm at most C'. In particular, $h_K = 1$ iff the primes of norm at most C' are principal.

6. Find repesentatives for the ideal classes of (a) $\mathbb{Q}(\sqrt{-5})$, (b) $\mathbb{Q}(\sqrt{-11})$, (c) $\mathbb{Q}(\sqrt{23})$, (d) $\mathbb{Q}(\sqrt[3]{2})$. What is the class number?

Quintic examples

7. (Artin) Let $f(x) = x^5 - x + 1$ and let $K = \mathbb{Q}(\alpha)$ where α is a root of f.
   (a) Show that $D(f) = 19 \cdot 151$ and conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
   (b) Suppose that f was reducible. Show that f would have an irreducible quadratic factor, and hence a root α such that $\mathbb{Q}(\alpha)$ is a quadratic field $\mathbb{Q}(\sqrt{d})$.
   (c) By considering ramification show that in (c) we must have $d = -19$ or $d = -151$ or $d = 19 \cdot 151$.
   (d) Show that f has a unique real root and use this to rule out $d = 19 \cdot 151$.
   (e) Show that every root of f is a unit and use this to rule out $d = -19$ and $d = -151$.
   (f) (Alternative route) Show that the images of f are irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$ and $(\mathbb{Z}/3\mathbb{Z})[x]$.

8. Continuing with the field K from the previous problem.
   (a) Show that K has one real place and two complex places.
   (b) Show that every ideal class in $\mathcal{O}_K$ has a representative of norm at most $\frac{5!}{5^5}\left(\frac{4}{\pi}\right)^2\sqrt{2869} < 4$.
   (c) Suppose there was an ideal $\mathfrak{p} \lhd \mathcal{O}_K$ of norm p, where $p \in \{2,3\}$. Show that p is prime, and that f has a root in $\mathbb{Z}/p\mathbb{Z} \simeq \mathcal{O}_K/\mathfrak{p}$ (show the isomorphism!)
   (d) Conclude that every ideal of $\mathcal{O}_K$ is principal.

9. (A new variant) Let $f(x) = x^5 + ax - 1$ where $a \in \mathbb{R}_{\geq 1}$.
   (a) Show that f has a unique real root ε, satisfying $\frac{1}{a+1} < \varepsilon < \frac{1}{a}$.
   (*b) For each primitive 8th root of unity ζ, it seems that $\zeta a^{1/4}$ is not far from a root of f. Show that if a is large enough then f has a root within $\frac{1}{3a}$ of $\zeta a^{1/4} - \frac{1}{4a}$.
   (c) Suppose $a \in \mathbb{Z}$. Show that any root of f is a unit.

9. Let $f(x) = x^5 + 2x - 1$, and let α be a root of f , $K = \mathbb{Q}(\alpha)$.
   (a) Show that f is irreducible and that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
   (b) Show that there is unique prime above 11317 in $\mathcal{O}_K$. Show that it is principal and find a generator. Find the ramification index and residue degree.
   (c) Find the primes of K above 2 (Hint: $\mathfrak{q} = (2, \varepsilon - 1)$ is one of them).
   (d) Show that every prime of K above $3, 5$ has residue degree at least 2.
   (**e) Find the class number h_K.

10. (Toward the normal closure)
    DEF Let β be another root of f, let $g(x) = \frac{f(x)}{x-\alpha} \in K[x]$ and let $L = K(\beta)$.
    FACT Gauss's Lemma holds in number fields.
    (a) Show that the image of $g(x)$ is irreducible in $\mathcal{O}_K/frakq$ (the ideal from 9(c)). Show that $g(x)$ is irreducible in $K[x]$.
    (b) Find the primes of L above $\mathfrak{q}$.
    (c) Show that $D_{L/K} | (\pi)^3$ where $\pi = 5\varepsilon^4 + 2$.
    DEF Let γ be yet another root, $h(x) = \frac{g(x)}{x-\gamma} \in L[x]$, $M = L(\gamma)$.
    (d) Show that $h(x)$ is irreducible in $L[x]$.

11. Let N be the normal closure of K over $\mathbb{Q}$ (the splitting field of f). Show that $T = \mathbb{Q}(\sqrt{11317}) \subset N$. Which primes of T ramify in the extension N/T?

Hint for 2b: Show that if $|z| = \frac{1}{3a}$ then $\left|f\left(\zeta a^{1/4} - \frac{1}{4a} + z\right)\right| > 1$ to conclude that f, g have the same number of roots in $B\left(\zeta a^{1/4} - \frac{1}{4a}, \frac{1}{3a}\right)$ where $g = x^5 + ax$.

Hint for 3b: The discriminant is the norm of the different.