Assignment 3

1. Show that the set $S \subseteq \mathbb{R}^n$ defined in the lectures is convex:

$$S = \left\{ (a_1, \dots, a_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2}) \colon |a_1| + \cdots + |a_{r_1}| + 2\left(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2} \right) \leq n \right\}.$$

For the purposes of this exercise, it is useful to work in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$, with $z_j = x_j + iy_j$. Then $\sqrt{x_j^2 + y_j^2} = |z_j|$, which has the advantage that it satisfies the triangle inequality, just like the absolute value of a real number. Now given $s = (a_1, \dots, a_{r_1}, z_1, \dots, z_{r_2}) \in S$ and $t = (b_1, \dots, b_{r_1}, w_1, \dots, w_{r_2}) \in S$, as well as $\lambda \in [0, 1]$, we put these triangle inequalities to work:

$$\begin{aligned} &\sum_{j=1}^{r_1} |\lambda a_j + (1-\lambda) b_j| + \sum_{j=1}^{r_2} |\lambda z_j + (1-\lambda) w_j| \\ &\leq \lambda \sum_{j=1}^{r_1} |a_j| + (1-\lambda) \sum_{j=1}^{r_1} |b_j| + \lambda \sum_{j=1}^{r_2} |z_j| + (1-\lambda) \sum_{j=1}^{r_2} |w_j| \\ &\leq \lambda n + (1-\lambda) n = n. \end{aligned}$$

2. Prove that as the degree n of a number field K goes to infinity, so does $|\Delta_K|$, the absolute value of its discriminant.

By Minkowski and using $n = r_1 + 2r_2$, we have

$$|\Delta_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2}$$

Therefore

$$\log |\Delta_K| \geq n \log(\pi/4) + 2n \log(n) - 2 \log(n!)$$

Stirling's approximation tells us that

$$\log(n!) \sim \frac{1}{2} \log(2\pi n) + n\big(\log(n) - 1\big),$$

so that $\log |\Delta_K|$ is bounded below by a function of n asymptotic to

$$n\big(2 + \log(\pi/4)\big) - \log(2\pi n),$$

which in turn diverges to ∞ as $n \to \infty$. (Crucial point is $2 + \log(\pi/4) > 0$.)

3. For $m \geq 3$, set $\zeta = e^{2\pi i/m}$ and $\omega = e^{\pi i/m}$.

   (a) Show that for all $k \in \mathbb{Z}$:

$$1 - \zeta^k = -2i\omega^k \sin(k\pi/m).$$

   Conclude that

$$\frac{1 - \zeta^k}{1 - \zeta} = \omega^{k-1} \frac{\sin(k\pi/m)}{\sin(\pi/m)}.$$

   Use the venerable $e^{i\theta} = \cos(\theta) + i \sin(\theta)$ to get

$$\omega^{-k} - \omega^k = -2i \sin(k\pi/m)$$

   then multiply by ω^k. The second identity follows immediately.

(b) Show that if k and m are not both even, then $\omega^{k-1} = \pm\zeta^h$ for some $h \in \mathbb{Z}$.

If k is odd we have $\omega^{k-1} = \zeta^{(k-1)/2}$ with $(k-1)/2 \in \mathbb{Z}$.
If k is even then m is odd.
Note that $\omega^m = e^{i\pi} = -1$, so that $\omega^{k-1} = -\omega^{m+k-1} = -\zeta^{(m+k-1)/2}$ with $(m+k-1)/2 \in \mathbb{Z}$ since k is even and m is odd.

(c) Show that if $\gcd(k, m) = 1$ then

$$u_k = \frac{\sin(k\pi/m)}{\sin(\pi/m)}$$

is a unit in $\mathbb{Z}[\zeta]$.

Since $\gcd(k, m) = 1$ we can use part (b):

$$u_k = \omega^{1-k}\frac{1-\zeta^k}{1-\zeta} = \pm\zeta^{-h}\frac{1-\zeta^k}{1-\zeta}.$$

The other consequence of $\gcd(k, m) = 1$ is that ζ and ζ^k are Galois-conjugate, so $N(1-\zeta^k) = N(1-\zeta)$ so that

$$N(u_k) = N(\pm\zeta^{-h})\frac{N(1-\zeta^k)}{N(1-\zeta)} = 1,$$

hence u_k is a unit.

4. Let $p > 2$ be a prime number. Let $x = p^n u \in \mathbb{Q}_p^\times$ with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Show that x is a square if and only if n is even and the reduction of u modulo p is a nonzero square.

First, suppose $x = y^2$ with $y \in \mathbb{Q}_p$. Since $x \neq 0$, we have $y \neq 0$. Write $y = p^m v$ where $m = v_p(y) \in \mathbb{Z}$ so that $v \in \mathbb{Z}_p^\times$. Letting $n = 2m$ and $u = v^2$, we have $x = p^{2m}v^2 = p^n u$, and since $v \in \mathbb{Z}_p^\times$ we know that the reduction $\bar{v}$ of v modulo p is nonzero. Hence the reduction $\bar{u} = \bar{v}^2$ of u modulo p is a nonzero square.
In the other direction, suppose $x = p^n u$ as stated. Since n is even, it suffices to show that u has a square root in $\mathbb{Z}_p^\times$. We want to prove that $y^2 - u = 0$ is solvable in $\mathbb{Z}_p$. Over $\mathbb{F}_p$ we have $y^2 - \bar{u} = 0$, which we are told has a nonzero root in $\mathbb{F}_p$; this is not a root of the derivative $2y$, so by Hensel's Lemma it can be lifted to a root in $\mathbb{Z}_p^\times$.