Assignment 8, March 30

Corrections: none yet.

1. Use quadratic reciprocity and the multiplicative property of the Legendre symbol to determine which rational primes p have $\left(\frac{3}{p}\right) = 1$ and which primes have $\left(\frac{-3}{p}\right) = 1$. (This completes the partial result that was in exercise 5 of assignment 7. This approach is less painful.)

2. Suppose $p \in \mathbb{Z}[i]$ is a Gaussian prime. For $x \in \mathbb{Z}[i]$ and $x \notin (p)$, define the Legendre symbol $\left(\frac{x}{p}\right)$ to be ± 1 depending on whether x is a square mod p in $\mathbb{Z}[i]/(p)$. Define $\left(\frac{x}{p}\right) = 0$ if $x \in (p)$.

   (a) Show that $\left(\frac{-1}{p}\right) = 1$ for all p.

   (b) Show that $\left(\frac{x}{p}\right)$ is multiplicative.

   (c) Find $x \in \mathbb{Z}[i]$ with $x^2 = i \bmod (3)$. Here, (3) is the principal ideal generated by 3. We seek $x \in \mathbb{Z}[i]$ so that $x^2 - i \in (3)$.

   (d) For an ideal I of a ring R, the norm is the number of elements in the quotient:
   $$N(I) = |R/I| \ .$$
   We talk about norms of mostly for prime ideals in rings of algebraic integers where the norm is finite and the quotient is a field. $N(I)$ is also called the *index* of I in R (terminology often used for subgroups of groups). Show that $N((p)) = |p|^2$. [This was on an old assignment, but please review the proof.]

   (e) Show that $\left(\frac{i}{p}\right) = 1$ if $N((p)) = 1 \bmod 8$. Explain how this is consistent with part (c). *Hint*: The multiplicative group of the quotient field has a generator.

   (f) Use part (a) to show that $N((p)) = 1 \bmod 4$ for every Gaussian prime ideal.

   (g) Let q be a rational prime. Explain how parts (d) and (f) imply that q is also prime in $\mathbb{Z}[i]$ if $q = 3 \bmod 4$.

3. Let $R = \mathbb{C}[x, y]$ and let $I \subset R$ be the set of polynomials $f(x, y)$ with $f(1, 0) = 0$ and $f(-1, 0) = 0$.

(a) Show that I is an ideal.

(b) Show that $I = (y, x^2 - 1)$. [The Hilbert basis theorem implies that I is finitely generated, but it is in general hard to find an explicit set of generators.]

4. Let $\mathcal{O}_{\overline{\mathbb{Q}}}$ be the ring of algebraic integers in the algebraic closure $\overline{\mathbb{Q}}/\mathbb{Q}$. Recall that $y \in \overline{\mathbb{Q}}$ is an algebraic integer if there is a (monic, integer) polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ($a_j \in \mathbb{Z}$) with $f(y) = 0$. Show that $\mathcal{O}_{\overline{\mathbb{Q}}}$ is not Noetherian. *Hint*: You can take the square root of anybody in $\mathcal{O}_{\overline{\mathbb{Q}}}$.

5. Let $\mathbb{Z}_p$ be the $p-$adic integers.

   (a) Show that for every $x \in \mathbb{Z}_p$ there is a unique sequence of "pidgits" (sounds like "digits"), $a_k \in \{0, \ldots, p-1\}$, so that the "pidgit sum" below converges and is equal to x:

   $$x = \sum_{k=0}^{\infty} a_k p^k$$

   Warning: Do not take uniqueness for granted. The digits d_k in the digit sum representation of a real number $x = \sum d_k 10^{-k}$ are not always unique.

   (b) Find the pidgit sum representation for $\frac{1}{6}$ in $\mathbb{Z}_7$. Said differently, find a pidgit sum x so that $6x = 1$ in $\mathbb{Z}_7$. You can start by assuming a pidgit sum exists and figuring out what the pidgits have to be, starting with a_0. Once you see the answer, you can verify that it is correct.

   (c) Which elements of $\mathbb{Z}_p$ are units?

   (d) What are the ideals of $\mathbb{Z}_p$?

   (e) Show that $\mathbb{Z}_p$ is a Noetherian ring.