Math 204A (Number Theory), UCSD, fall 2020
Problem Set 1 – due Thursday, October 15, 2020

In general, solutions should be submitted via CoCalc. To do this, place your solutions in the folder `assignments/2020-10-15/` in your course project. (This folder acts like a homework dropbox.) You may submit handwritten text (scanned from paper or written on a tablet) or a typed PDF (e.g., created using LaTeX on CoCalc).

For this set *only*, if you are unable to use CoCalc, you may also submit solutions through Zulip, by sending me a private message with an attachment.

Collaboration and research is fine, as long as you do the following.

- Try the problems yourself first!
- Write the solutions in your own words.
- Acknowledge all sources and collaborators.

1. Compute the minimal polynomials of the following algebraic numbers:
   (a) $\sqrt{2}+\sqrt{3}$;
   (b) $\sqrt{2+\sqrt{3}}$.

   In each case, be sure to include a proof that your answer is minimal.

2. Take a diagram of the primes in the Eisenstein integers (this could be the photo of my shower, another diagram from the Internet, or one you make yourself in Sage) and locate one prime with each of the square norms $13, 19, 31, 37, 43$. Also indicate how to write each of these primes in the form $a + b\zeta_3$ with $a, b \in \mathbb{Z}$.

3. For each of the following fields K, show that the ring of integers of K is Euclidean, and determine which rational primes factor nontrivially.
   (a) $\mathbb{Q}(\sqrt{-2})$, using the complex absolute value.
   (b) $\mathbb{Q}(\sqrt{-7})$, using the complex absolute value.
   (c) $\mathbb{Q}(\sqrt{2})$, using the function $a + b\sqrt{2} \mapsto |a^2 - 2b^2|$.

4. Let $D \neq 1$ be a squarefree integer. Compute the ring of integers of $\mathbb{Q}(\sqrt{D})$ (the answer was stated in lecture).

5. Let I be the ideal $(2, 1+\sqrt{-3})$ in the ring $\mathbb{Z}[\sqrt{-3}]$. Show that:
   (a) $I \neq (2)$ but $I^2 = 2I$;
   (b) I is the unique prime ideal containing (2);
   (c) (2) is not a product of prime ideals.

Then explain why this does *not* contradict anything from the lecture.

6. Compute the rings of integers of the following number fields.

   (a) $\mathbb{Q}(2^{1/3})$.

   (b) $\mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha - 4 = 0$.

   (c) $\mathbb{Q}(\zeta_5)$.

7. Let $P(x) \in \mathbb{Z}[x]$ be a polynomial such that, if we factor $P(x)$ over $\mathbb{C}$ as $(x-\alpha_1)\cdots(x-\alpha_n)$, then $|\alpha_j| \leq 1$ for $j = 1, \dots, n$.

   (a) For m a positive integer, define the polynomial $P_m(x) = (x - \alpha_1^m)\cdots(x - \alpha_n^m)$. Prove that $P_m(x) \in \mathbb{Z}[x]$. (Hint: show that the coefficients are in $\mathbb{Q} \cap \overline{\mathbb{Z}}$.)

   (b) Prove that the coefficients of $P_m(x)$ can be bounded independently of m.

   (c) What does this imply about $\alpha_1, \dots, \alpha_n$?