MATH 3032: Abstract Algebra

Assignment 3

due 4 March 2025, end of day

Homework should be submitted as a single PDF attachment to `denisalja@dal.ca`. Please title the file in a useful way, for example `Math3032_HW#_Name.pdf`.

You are encouraged to work with your classmates, but your writing should be your own. If you do work with other people, please acknowledge (by name) whom you worked with. You are expected to think about every problem on every assignment, but you are not expected to solve every problem on every assignment. The purpose of homework assignments is to learn.

1. Use Euclid's algorithm to find the greatest common divisor of the the following pairs of integers:

   (a) 11391 and 5673

   (b) 507885 and 60808

   (c) 91442056588823 and 779086434385541.

   Don't be afraid of the size: even for the last one, Euclid's algorithm only requires 7 steps.

2. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a ring R are called *comaximal* if neither is all of R, but there is no ideal other than R that contains their union. Explain that in a PID, (a) and (b) are comaximal if and only if the gcd of a and b is 1.

3. Let R an integral domain and $a, b \in R$. Show that the following conditions on $d \in R$ are equivalent:

   - (d) is the largest principal ideal contained in $(a) \cap (b)$.
   - d a *least common multiple* of a and b in the sense that d is a multiple of both a and of b, and that any element of r which is a multiple of both a and b is also a multiple of d.

   Conclude that in a PID, every pair of elements has an lcm, unique up to multiplication by an invertible.

   Indeed, show that $\frac{ab}{(a,b)}$ is an lcm of a, b.

4. Suppose that $n \geq 3$ is squarefree, and set $R = \mathbb{Z}[\sqrt{-n}]$.

   (a) Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducible in R.

   (b) Prove that 2 is not prime. Hint: what are $(\sqrt{-n})^2$ and $(1 + \sqrt{-n})^2$? Hint: n is either even or odd.

   Conclude that R is not a UFD.

   Why doesn't your argument work if $n = 1, 2$?

5. Suppose that R is a PID and that $D \subset R$ is a multiplicatively-closed subset. Show that $R[D^{-1}]$ is a PID.

6. Determine all ways to write $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.

7. * Use the Eisenstein integers $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ to classify which $n \in \mathbb{Z}$ can be written as a^2+ab+b^2 for some $a, b \in \mathbb{Z}$.

   Note: Feel free to completely skip this question. A complete solution would be a full problem set in and of itself. See for example `http://categorified.net/23Winter3032/HW6.pdf`.