Math 418: HW 1 due Wednesday, January 26, 2022.

Webpage: http://dunfield.info/418
Office hours: Monday and Tuesday from 1:30–2:30pm; other times possible by appointment.
Textbook: Dummit and Foote, *Abstract Algebra*, 3rd edition.

1. The background on rings I will be assuming is the contents of Chapter 7 of our text. Look through that chapter and find one thing you don't understand and work a problem from the text about it. (If everything in the chapter is clear, just pick some problem that's amusing and do that. If no problem looks amusing, you may be in the wrong class.)

2. Repeat Problem 1. That is, pick another problem from Chapter 7 and work it as well.

3. Consider $R = \mathbb{Z}[\sqrt{-5}]$ with the norm $N\colon R \to \mathbb{Z}_{\geq 0}$ given by $N(a) = |a|^2$. (This isn't a norm in the sense of Euclidean domains, but rather another sense we'll learn about later.) In the below problems, a key is that $N(a \cdot b) = N(a)N(b)$.

   (a) Prove that $a \in R$ is a unit if and only if $N(a) = 1$. Find all the units in R.

   (b) Recall that $r \in R$ is irreducible if whenever $r = ab$ then one of a or b is a unit. Use the norm to show that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible elements of R.

   (c) Show that $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are not unit multiples of one another. Thus R lacks unique factorization since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Weird, huh?

4. Let R be an integral domain. Recall that g is a greatest common divisor of two elements a, b if g divides a and b, and if d is any other common divisor then d divides g.

   (a) If g and g' are two gcds of elements (a, b) show that $g' = ug$ for some unit u.

   (b) Again consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. Prove that 6 and $2 + 2\sqrt{-5}$ have no gcd. Hint: Use that 2 and $1 + \sqrt{-5}$ are both common divisors of these elements.

5. Let R be a Principal Ideal Domain, and I an ideal of R. Prove that every ideal of $S = R/I$ is principal. (S may fail to be an integral domain, and hence is not always a P.I.D itself; for example, $R = \mathbb{Z}$ and $I = 4\mathbb{Z}$.)