MAT 150C: MODERN ALGEBRA
Homework 4

Instructions. Please write the answer to each problem, including the computational ones, in connected sentences and explain your work. Just the answer (correct or not) is not enough. Write your name in every page and upload to Gradescope *with the correct orientation.* Make sure to indicate to Gradescope which pages correspond to each problem. **Finally, if you used another sources or discussed the problem with classmates, be sure to acknowledge it in your homework.**

1. (a) Show that if $\mathbb{F}$ is a field of positive characteristic $p > 0$, then $(a+b)^p = a^p + b^p$ for every $a, b \in \mathbb{F}$.

   (b) Let p be a prime number and $r > 0$ an integer. Let $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ be the cyclotomic polynomial. Show that the polynomial

   $$\Phi_{p^r}(x) := \Phi_p(x^{p^{r-1}}) = \frac{(x^{p^{r-1}})^p - 1}{x^{p^{r-1}} - 1}$$

   is irreducible in $\mathbb{Z}[x]$. (Hint: This is very similar to the proof that $\Phi_p(x)$ is irreducible)

2. At the end of class on Friday 04/17 I said a huge lie and this is your opportunity to correct me. Indeed, I mentioned that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because $5 \equiv 1 \mod 4$. But in fact, there is nothing special about 5. Here we will see that, for every integer $n > 2$, $\mathbb{Z}[\sqrt{-n}]$ is not a UFD. Note that $\mathbb{Z}[\sqrt{-n}] \subseteq \mathbb{C}$, so it is indeed a domain. Take $n > 2$.

   (a) Define a function $N : \mathbb{Z}[\sqrt{-n}] \to \mathbb{Z}$ by $N(\alpha + \beta\sqrt{-n}) = \alpha^2 + n\beta^2$. Show that $N(ab) = N(a)N(b)$ for $a, b \in \mathbb{Z}[\sqrt{-n}]$.

   (b) Show, using part (a), that $a \in \mathbb{Z}[\sqrt{-n}]$ is a unit if and only if $N(a) = 1$. Use this to find all the units in $\mathbb{Z}[\sqrt{-n}]$.

   (c) Use parts (a) and (b) to show that $2 \in \mathbb{Z}[\sqrt{-n}]$ is irreducible. (Hint: If $2 = ab$ is a decomposition, then $N(2) = N(a)N(b)$)

   (d) Assume n is odd. Show that $N(1 + \sqrt{-n})$ is divisible by 2, and use this to find $a, b \in \mathbb{Z}[\sqrt{-n}]$ such that 2 divides ab but 2 does not divide a nor b. This tells us that 2 is not a prime element in $\mathbb{Z}[\sqrt{-n}]$. Conclude that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD.

   (e) Now assume n is even. Use a similar procedure to part (d) to show that 2 is not a prime element in $\mathbb{Z}[\sqrt{-n}]$.

3. We have seen in class (04/20) that $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain, therefore a PID and therefore a UFD. Adapt the proof we saw in class to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain as well.