Math 146: Homework 3

Due: Friday, February 23, by 11:59pm

Please submit your solutions as a single PDF on Canvas

Reminders:

- You are encouraged to work together on homework. If you work with other students, please indicate who you worked with on this assignment.
- The usual extension policy applies to this assignment: if you would like an extension on this homework over the weekend, simply email the professor to ask for it. No justification is required.

1. Let F be a field and let $f \in F[x]$ have degree 1. Prove that the principal ideal generated by f is maximal.

2. Let R be a commutative ring. Prove that every maximal ideal is a prime ideal. (*Hint:* This is possible to do by working with the definitions directly, but it is much easier to do by working with statements we proved are equivalent to being maximal or prime.)

3. Let $R = \mathbb{Z}[i]$. For a prime number p, let (p) be the principal ideal generated by p in R.

a) Prove that the ideal (5) is not a prime ideal.

b) By Problem 2) and part a), evidently (5) is not a maximal ideal. Find an ideal I other than R and (5) such that $(5) \subseteq I$.

c) More generally, suppose p is such that there is a solution to the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$. Prove that the principal ideal (p) is not prime.

d) On the other hand, prove that (3) *is* maximal.

e) In fact, suppose that p is any prime such that there is no solution to the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$. Prove that the ideal (p) is maximal. (*Hint:* Suppose I is an ideal in R properly containing (p), so there is some $a + bi \in I$ with at least one of a and b not divisible by p. Can you find something "nicer" that must be in I and use it to show that I must be equal to R?)

(It is a fact from elementary number theory that there is a solution to the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$ if and only if $p \equiv 1, 2 \pmod 4$, while there is no solution if and only if $p \equiv 3 \pmod 4$. Thus, your work above proves that the ideal (p) in R is maximal if and only if $p \equiv 3 \pmod 4$.)

4. This problem will have you study the field $\mathbb{Q}(\sqrt[3]{2})$ obtained by starting with the rational numbers $\mathbb{Q}$ and adding a cube root of 2. You may assume below that $\sqrt[3]{2}$ is irrational. (For example, the usual proof that $\sqrt{2}$ is irrational adapts to prove the same for $\sqrt[3]{2}$, but there is no need to reproduce this below.)

Throughout this problem, let $f \in \mathbb{Q}[x]$ be given by $f = x^3 - 2$.

a) Prove that f is irreducible, i.e. that there do not exist polynomials $f_1, f_2 \in \mathbb{Q}[x]$ with $\deg f_1 = 1$ and $\deg f_2 = 2$ such that $f = f_1 f_2$.

b) Conclude that $\mathbb{Q}[x]/(f)$ is a field.[1]

[1] This will follow immediately from part a) and a theorem we should prove in lecture this week. If we don't get to that theorem, skip this part, but continue with the rest of the problem.

c) Use the polynomial division algorithm to find polynomials $q, r \in \mathbb{Q}[x]$ such that $x^4 + x + 1 = qf + r$, where $\deg r < \deg f$. Observe that $r(\sqrt[3]{2}) = \sqrt[3]{2}^4 + \sqrt[3]{2} + 1$.
(*Hint, sort of:* The expression $\sqrt[3]{2}^4 + \sqrt[3]{2} + 1$ is not "optimal," in a certain sense, and can be rewritten pretty easily. This gives you a way to check your work with the division algorithm. The big-picture point of this part of the problem is just to demonstrate that the polynomial division algorithm gives a systematic way of doing this "rewriting" process, and could be used equally well for more complicated polynomials than $x^3 - 2$.)

d) Use the polynomial Euclidean algorithm to find explicit polynomials $A, B \in \mathbb{Q}[x]$ such that $A \cdot (3x + 1) + B \cdot f = 1$.

e) Express $\frac{1}{3\sqrt[3]{2}+1}$ in the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, for $a, b, c \in \mathbb{Q}$.