Math 5320

Homework 7

From the book, do Ch. 12: 4.1, 4.3 as well as the problems given below. You will want to use what you prove in problem 1 to do Ch. 12: 4.1.

1. It is possible to extend the idea of taking a derivative to polynomials with coefficients in any field that acts just like how we might hope it should: the derivative of x^n is $n \cdot x^{n-1}$.

   More formally, given any field F, the ring of polynomials $F[x]$ can be thought of as an infinite-dimensional vector space over F. A possible choice of basis for $F[x]$ is $\{1, x, x^2, x^3, \ldots\}$. We can define a homomorphism of F-vector spaces
   $$\varphi : F[x] \to F[x]$$
   such that $\varphi(1) = 0$, $\varphi(x) = 1$, $\varphi(x^2) = 2x$ and more generally $\varphi(x^n) = nx^{n-1}$. We call $\varphi(p(x))$ the derivative of $p(x)$. Note that φ is not a ring homomorphism! But, φ does satisfy the product rule: Given $f(x), g(x) \in F[x]$, $\varphi(f(x)g(x)) = f(x)\varphi(g(x)) + \varphi(f(x))g(x)$ (I won't prove this here, but just assert that it's a fact, and it's a property that you will need to use to complete this problem). Also, to keep notation compact, we will just use the notation $'$ to denote the derivative, so take $p'(x) := \varphi(p(x))$ in the rest of the problem.

   (a) Let $p(x) \in F[x]$. We showed in class that if $a \in F$ is a root of F, then we can write $p(x) = (x - a)p_1(x)$ for some $p_1(x) \in F[x]$. Prove that if $p(a) = 0$ and $p'(a) = 0$, then $(x - a)^2$ is a factor of $p(x)$.

   (b) Furthermore, show that if $p(a) = 0, p'(a) = 0, \ldots,$ and $p^{(n)}(a) = 0$, then $(x - a)^{n+1}$ divides $p(x)$.

By completing the next few exercises, you will work through characterizing which prime integers are prime elements of $\mathbb{Z}[i]$, as well as proving a fun number theory fact about the prime integers that are not prime elements of $\mathbb{Z}[i]$. Notice that unlike in $\mathbb{Z}[x]$, prime integers are not necessarily irreducible in $\mathbb{Z}[i]$. For instance, $5 = (2 + i)(2 - i)$.

The book covers this topic in 12.5, so if you get stuck, it's there as a resource.

2. What are the units in $\mathbb{Z}[i]$? Hint: Recall that the norm of an element $a + bi \in \mathbb{Z}[i]$ is defined to be $N(a + ib) := (a + ib)(a - ib) = a^2 + b^2$ and that norms are multiplicative, that is, the norm of a product is the product of the norms. You will probably want to prove this by first showing that any unit in $\mathbb{Z}[i]$ has norm 1.

3. Let $\pi \in \mathbb{Z}[i]$ be a prime element of $\mathbb{Z}[i]$. Prove that its complex conjugate $\bar{\pi}$ is also a prime element of $\mathbb{Z}[i]$.

4. Show that if p is a prime integer that is not prime in $\mathbb{Z}[i]$, then p is the product of prime element π of $\mathbb{Z}[i]$ and its conjugate $\bar{\pi}$.

5. Use the previous problem to show that if a prime integer p is not prime in $\mathbb{Z}[i]$, then it can be written as a sum of squares $p = a^2 + b^2$ with $a, b \in \mathbb{N}$. Also, show the converse.

6. Is 2 a prime element in $\mathbb{Z}[i]$?

7. Show that if p is a prime integer, then p is a prime in $\mathbb{Z}[i]$ if and only if $x^2 + 1$ is irreducble in $\mathbb{F}_p[x]$, where $\mathbb{F}_p := \mathbb{Z}/(p)$. You will want to use the fact that $\mathbb{Z}[x]/(x^2 + 1, p) \cong \mathbb{Z}[i]/(p) \cong \mathbb{F}_p/(x^2 + 1)$. You don't have to prove this is an isomorphism, but if you don't remember how to prove it from earlier in the semester, I suggest reviewing (or asking me about it).

8. Show that $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$ if and only if there are no roots of $x^2 + 1$ in $\mathbb{F}_p[x]$.

   Finally, we will show that if p is an odd prime, then there exists some $a \in \mathbb{F}_p$ such that $a^2 = -1$ (that is, $x^2 + 1$ is not irreducible in $\mathbb{F}_p[x]$) if and only if $p \equiv 1 \mod 4$. Note that such an a exists if and only if the group homomorphism $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ that maps elements to their squares has -1 in its image. Furthermore, -1 is the only element of $\mathbb{F}_p^*$ with order 2, so it will suffice to analyze whether the image of φ contains an element of order 2 or not.

   The kernel of φ consists of elements of $\mathbb{F}_p^*$ that are roots of $x^2 - 1 = 0$. Since $p \geq 2$, we have two distinct roots: 1 and -1 (there can be only two because $x^2 - 1$ is a degree 2 polynomial). The group $\mathbb{F}_p^*$ has $p - 1$ elements, and so the image of φ has $\frac{p-1}{2}$ elements. It is a consequence of the first Sylow theorem that the image of φ will have an element of order 2 if (and only if) 2 divides $\frac{p-1}{2}$.

   In summary: We showed that any prime integer p is prime in $\mathbb{Z}[i]$ if and only if $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$ if and only if $p \equiv 1 \mod 4$. We also showed that any prime integer p is not prime in $\mathbb{Z}[i]$ if and only if it can be written as a sum of two squares if and only if $p = 2$ or $p \equiv 3 \mod 4$.