Math 103B, Winter 2018

Modern Algebra II, HW 7

Due Friday March 2nd by 5PM in your TA's box

From Lauritzen's book:

- Exercises 4.10 (starting page 179): *1, 3, 5, 6, 7*

Problem A. Let $\mathbb{Z}[\omega]$ be the ring of Eisenstein integers. Here $\omega = \frac{1}{2}(-1+i\sqrt{3})$.

(a) Verify that every prime number $p \equiv 2 \pmod 3$ remains prime in $\mathbb{Z}[\omega]$. (`Hint`: If not, taking norms yields $p = a^2 - ab + b^2 \equiv (a+b)^2 \pmod 3$.)

(b) Check that $p = 3$ and $(1-\omega)^2$ are associated elements of $\mathbb{Z}[\omega]$. (cf. 3.5.1.)

(c) In this question let $p \equiv 1 \pmod 3$ be a prime number. If you are familiar with the quadratic reciprocity law (p. 170), show that the congruence

$$x^2 \equiv -3 \pmod p$$

has a solution $x \in \mathbb{Z}$. If not, accept this as a fact. Use this fact to show that p does *not* remain prime in $\mathbb{Z}[\omega]$.

Problem B. Let R be a commutative ring and consider the ring $R[\![X]\!]$ of formal power series $f = \sum_{i=0}^{\infty} a_i X^i$ with coefficients $a_i \in R$. (Here "formal" means you ignore questions about convergence[1] and identify f with the sequence of coefficients $(a_0, a_1, \ldots)$. These are added componentwise, and multiplied by the rule

$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, \ldots) \qquad c_n := \sum_{i+j=n} a_i b_j$$

which reflects how convergent power series over $\mathbb{C}$ multiply.)

(a) Show that $R[\![X]\!]$ is a ring containing $R[X]$ as a subring.

(b) Prove that $f = \sum_{i=0}^{\infty} a_i X^i$ is a unit of $R[\![X]\!]$ if and only if $a_0 \in R^{\times}$.

[1] Convergence does not even make sense for an arbitrary ring R.

(c) If R is a field, deduce from (b) that $R[\![X]\!]$ is a local ring and (X) is its unique maximal ideal. (`Hint`: You may use the result in Problem B part (b) on HW4.)

(d) Let S be another commutative ring, and $\varphi : R \to S$ a homomorphism. Suppose $\alpha \in S$ is a **nilpotent** element (meaning $\alpha^i = 0$ for some $i \geq 1$). Verify that there exists a unique homomorphism $\tilde{\varphi} : R[\![X]\!] \to S$ with the following two properties:

(i) $\tilde{\varphi}(a) = \varphi(a)$ for all $a \in R$;

(ii) $\tilde{\varphi}(X) = \alpha$.

Problem C. Consider the polynomial ring $\mathbb{Z}[X]$ in one variable over the integers. Fix a prime number p, and let (p, X) be the ideal of $\mathbb{Z}[X]$ generated by the two elements p and X.

(a) Check that (p, X) is a proper ideal, meaning $(p, X) \neq \mathbb{Z}[X]$. (`Hint`: Otherwise write $1 = pf(X) + Xg(X)$ and substitute $X = 0$.)

(b) Give an isomorphism of rings

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[X]/(p, X)$$

and conclude that (p, X) is a maximal ideal of $\mathbb{Z}[X]$.

(c) Prove that (p, X) is <u>not</u> a principal ideal. (`Hint`: Say h generates the ideal. Writing p as a polynomial multiple of h shows h must be an integer by comparing degrees. Factoring $X = (aX^m + \cdots)h$ proves $h = \pm 1$ which violates (a).) Conclude $\mathbb{Z}[X]$ is not a PID.

(d) In this part consider the two principal ideals (X) and (p). Show that there are isomorphisms

$$\mathbb{Z}[X]/(X) \simeq \mathbb{Z} \qquad \mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$$

and infer that both p and X are prime elements of $\mathbb{Z}[X]$.