Math 103B, Winter 2018

Modern Algebra II, HW 9

Due Friday March 16th by 5PM in your TA's box

From Lauritzen's book:

- Exercises 4.10 (starting page 179): *26, 28*[1]*, 29(iii+iv), 30, 38*[2]*, 44*

Problem A. Let $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ as usual.

(a) Check that the polynomial $X^3 - X^2 + 1$ in $\mathbb{F}_3[X]$ is irreducible (by verifying it has no roots in $\mathbb{F}_3$). Conclude that

$$\mathbb{F}_3[X]/(X^3 - X^2 + 1)$$

is a finite field with exactly 27 elements.

(b) Factor $X^3 + X^2 + 1$ into irreducible polynomials of $\mathbb{F}_3[X]$ (note the sign change of the X^2-coefficient) and produce an isomorphism

$$\mathbb{F}_3[X]/(X^3 + X^2 + 1) \xrightarrow{\sim} \mathbb{F}_3 \times \mathbb{F}_9$$

for some finite field $\mathbb{F}_9$ with exactly 9 elements. (`Hint`: Chinese.)

Problem B. Let F be a finite field of characteristic p (a prime number).

(a) Suppose $f \in F[X]$ has derivative $f' = 0$. Show that f is a polynomial in X^p. (`Hint`: If $f = a_0 + a_1 X + \cdots + a_n X^n$ show that $a_i = 0$ unless $p|i$.)

(b) Let E be a field containing F as a subfield, and assume f is **irreducible** in $F[X]$. Prove that f has no repeated roots in E. (`Hint`: Suppose $\alpha \in E$ is a root of f with multiplicity > 1. Then $f'(\alpha) = 0$ shows f and f' are not coprime in $F[X]$, and therefore $f|f'$ since f is assumed to be irreducible. Comparing degrees shows $f' = 0$. Invoke part (a) and write

$$f = b_0^p + b_1^p X^p + \cdots + b_r^p X^{pr} = (b_0 + b_1 X + \cdots + b_r X^r)^p$$

[1]`Hint`: In part (iv) explain why it suffices to check $\alpha^3 \neq 1$ and $\alpha^5 \neq 1$ – and check this.
[2]`Hint`: In part (ii) first observe that $p^r - 1$ divides $p^s - 1$ when $r|s$. Then cancel an X.

using that the Frobenius map $\varphi : F \longrightarrow F$ taking $b \mapsto b^p$ is surjective since $|F| < \infty$. The last equation above gives a contradiction. Why?)

Problem C. Please submit your teaching evaluations, thank you!