# Homework 8, Math 401

due on April 3, 2020

Before you start, please read the syllabus carefully.

1. Let $F$ be an arbitrary field with $\mathrm{char}(F) = p$. Prove that $\mathbb{F}_p \subset F$, i.e., $\mathbb{F}_p$ is a subfield of $F$. (This is a quick proof of $\mathbb{F}_p \subset S$ of Claim 2 in class. )

2. Prove that for an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$, the field extension $\mathbb{F}_p[x]/\langle f(x)\rangle$ is also the splitting field of $f(x)$. (Hint: prove that $f(x)|x^q - x$ for $q = p^{\deg(f)}$.)

3. Prove that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $d|n$.

4. For an arbitrary field $F$, we define a formal operation on $f(x) \in F[x]$ called *derivative* as following
$$f'(x) := \sum_n a_n \cdot n \cdot x^{n-1},$$
if $f(x) = \sum_n a_n \cdot x^n$.

   (a) Prove that
   $$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x),$$
   for $F[x]$ for arbitrary field $F$.

   (b) Prove that if $f(x)$ has a multiple root $\alpha$, equivalently $(x-\alpha)^2|f(x))$, then $\alpha$ is also a root of $f'(x)$.

   (c) Does the converse from above holds? i.e., if $f'(\alpha) = 0$, does it imply that $\alpha$ is a multiple root $f(x)$? If yes, give a proof, if no, give a counter example or give a correct statement.

   (d) Prove that $f(\alpha) = f'(\alpha) = \cdots = f^{(k)}(\alpha) = 0$ if and only if $(x-\alpha)^{k+1}|f(x)$ for $f(x)$ in polynomial ring $F[x]$ where $F$ is an arbitrary field. (Does this remind you of Taylor expansion in calculus?)

5. Let $f(x) = x^2 + x + 1 \in \mathbb{F}_p[x]$ where $p > 3$ is a prime number.

   (a) Determine if $f(x)$ is irreducible in $\mathbb{F}_p[x]$. (Give a criteria on when $f(x)$ is irreducible.)

   (b) For $p = 5$, using your criteria to determine whether $f(x)$ is irreducible. If yes, denote $K = \mathbb{F}_5[x]/\langle f(x)\rangle$. Show that $K$ contains all 24-th roots of unity $\zeta_{24}$ (i.e. elements $\alpha$ such that $\alpha^{24} = 1$).

   (c) For $p = 7$, using your criteria to determine whether $f(x)$ is irreducible. If no, determine the factorization of $f(x)$.

   (d) The largest prime number ever found up to now is $p = 2^{82589933} - 1$. Use your criteria to determine whether $f(x)$ is irreducible. You are not allowed to use computer.

6. Let $f_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 \in \mathbb{F}_3[x]$ where $p > 3$ is a prime number. Denote $K_p$ to be the splitting field of $f_p(x)$ over $\mathbb{F}_3$.

   (a) Prove that $x^r - 1 | x^s - 1$ in $\mathbb{F}_3[x]$ if and only if $r|s$.

   (b) Prove that $f_p(x)|x^q - x$ for $q = 3^n$ if and only if $p|3^n - 1$.

   (c) Determine $[K_p : \mathbb{F}_p]$.

   (d) **Bonus** Determine when $f_p(x)$ is irreducible in $\mathbb{F}_3[x]$. For $p = 7, 11, 13$, use your criteria to determine yes/no.

   **Answer**: a) it is clear that if $s = rd$, then we can write $x^s - 1 = (x^r - 1)((x^r)^{d-1} + \cdots + 1)$. On the other hand, if $s = rq + r'$ with $0 < r' < r$, then we have $x^s - 1 = (x^{rq} - 1)x^{r'} + (x^{r'} - 1)$. We know that $x^r - 1 | (x^{rq} - 1)x^{r'}$ and $x^r - 1 \nmid x^{r'} - 1$, so $x^r - 1 \nmid x^s - 1$.

   b) Denote $f_p(x)(x - 1) = g(x) = x^p - 1$. Notice that $g'(x) = px^{p-1}$ which has no common roots with $g(x)$, so $g(x)$ has distinct roots. Therefore $x - 1$ and $f_p(x)$ are relatively prime to each other. It is clear that $x - 1|x^{q-1} - 1$. By the unique factorization of polynomials over fields, $f_p(x)|x^{q-1} - 1$ and $x - 1|x^{q-1} - 1$ if and only if $g(x)|x^{q-1} - 1$ (since $f_p$ and $x - 1$ are relatively prime). Again by the unique factorization of polynomials in $\mathbb{F}_p[x]$, $f_p(x)|x^q - x$ if and only if $f_p(x)|x^{q-1} - x$ since the irreducible factor $x \nmid f_p(x)$. Therefore $f_p(x)|x^q - x$ if and only if $g(x)|x^{q-1} - 1$. Finally $g(x) = x^p - 1|x^{q-1} - 1$ if and only if $p|3^n - 1$ by a).

   c) Since $g(x)$ has distinct roots, we know that $f_p(x)$ splits in $K$ if and only if $f_p(x)|x^q - x = \prod_{\beta \in \mathbb{F}_q}(x - \beta)$ if and only if $p|q - 1$. Therefore denote $[K_p : \mathbb{F}_3] = n$, then $3^n$ is the smallest integer $n$ such that $p|3^n - 1$. Equivalently, this is the order of 3 in $\mathbb{F}_p^*$.

   d) $f_p(x)$ is irreducible if and only if $[K_p : \mathbb{F}_3] = p - 1$. So we compute the order of 3 in $\mathbb{F}_p^*$, we get yes, no, no.

7. Given $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ such that $\sigma(x) = x^p$. Prove that $\sigma$ is a ring isomorphism.