Math 1540: HW1

February 10, 2023

Book Problems:

55. If $(f, g) = h \neq 1$, then there must exist an extension field of F, E, which contains a root of h which is common between f and g since $(f, g) = h$

    Else, $(f, g) = 1$, then there exists no field E containing both F and a common root of $f(x)$ and $g(x)$ since $(\exists a, b \in F)(af + bg = 1)$ implies f and g share no roots $(a(x)f(x) + b(x)g(x) = 1 \neq 0$ for all $x)$.

56. (i) Let $f(x) = a_0 + a_1 x \ldots + a_n x^n$ then:

$$\begin{aligned}(f(x))^p &= (a_0 + a_1 x \ldots + a_n x^n)^p \\ &= a_0^p + a_1^p (x)^p \ldots + a_n^p (x^n)^p\end{aligned}$$

Because of Fermat's Little Theorem $a^p \equiv a \pmod{p}$:

$$\begin{aligned}&= a_0 + a_1 (x)^p \ldots + a_n (x^n)^p \\ &= a_0 + a_1 (x^p) \ldots + a_n (x^p)^n \\ &= f(x^p)\end{aligned}$$

(ii) If we replace $\mathbb{Z}_p$ with an infinite field, F, of characteristic p we can be no longer sure that Fermat's Little Theorem holds for all a_i in $f(x) = a_0 + a_1 x \ldots + a_n x^n$. $x^p - x$ only has p roots, and they are only the elements $\mathbb{Z}_p \subset F$. a_i could be in F and not $\mathbb{Z}_p$, so we are left will a less strong result: $(f(x))^p = a_0^p + a_1^p x^p \ldots + a_n^p (x^p)^n = g(x^p)$

61. Let's factor $x^8 - x$ in $\mathbb{Z}_2$

$$\begin{aligned}x^8 - x \\ x(x^7 - 1) \\ x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)\end{aligned}$$

Since we are in $\mathbb{Z}_2$, $3 = 1$ and we can factor it further:

$$\begin{aligned}x(x-1)(x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1) \\ x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)\end{aligned}$$

Now we can use either x^3+x+1 or x^3+x^2+1. I will use x^3+x+1. $\mathbb{Z}_2/(x^3+x+1) \cong \mathbb{F}_8$ so our elements will be $1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$

Therefore, our addition table will look like:

	0	1	x	x + 1	x^2	x^2 + 1	x^2 + x	x^2 + x + 1
0	0	1	x	x + 1	x^2	x^2 + 1	x^2 + x	x^2 + x + 1
1	1	0	x + 1	x	x^2 + 1	x^2	x^2 + x + 1	x^2 + x
x	x	x + 1	0	1	x^2 + x	x^2 + x + 1	x^2	x^2 + 1
x + 1	x + 1	x	1	0	x^2 + x + 1	x^2 + x	x^2 + 1	x^2
x^2	x^2	x^2 + 1	x^2 + x	x^2 + x + 1	0	1	x	x + 1
x^2 + 1	x^2 + 1	x^2	x^2 + x + 1	x^2 + x	1	0	x + 1	x
x^2 + x	x^2 + x	x^2 + x + 1	x^2	x^2 + 1	x	x + 1	0	1
x^2 + x + 1	x^2 + x + 1	x^2 + x	x^2 + 1	x^2	x + 1	x	1	0

And, our multiplication table will look like

	0	1	x	x + 1	x^2	x^2 + 1	x^2 + x	x^2 + x + 1
0	0	0	0	0	0	0	0	0
1	0	1	x	x + 1	x^2	x^2 + 1	x^2 + x	x^2 + x + 1
x	0	x	x^2	x^2 + x	x + 1	1	x^2 + x + 1	x^2 + 1
x + 1	0	x + 1	x^2 + 1	x^2 + 1	x^2 + x + 1	x^2	1	x
x^2	0	x^2	x + 1	x^2 + x + 1	x^2 + x	x	x^2 + 1	1
x^2 + 1	0	x^2 + 1	1	x^2	x	x^2 + x + 1	x + 1	x^2 + x
x^2 + x	0	x^2 + x	x^2 + x + 1	1	x^2 + 1	x + 1	x	x^2
x^2 + x + 1	0	x^2 + x + 1	x^2 + 1	x	1	x^2 + x	x^2	x+1

(Sorry for the non LaTeX, the tables were giving a lot of trouble)

62. If $\mathbb{F}_4$ was isomorphic to a subfield of $\mathbb{F}_8$, there would have to be a field extension of $\mathbb{F}_4$ to $\mathbb{F}_8$, a $\mathbb{F}_4$ vector space of dimension n; however this would imply $\exists n \in \mathbb{Z}, 4^n = 8$, which is not possible, so it is not possible that $\mathbb{F}_4$ is isomorphic to a subfield of $\mathbb{F}_8$.

Given Problems:

1. f has no repeated roots if and only if $(f, f') = 1$ is equivalent to f has repeated roots if and only if $(f, f') \neq 1$

   Assume $f(x)$ has repeated roots then $f(x) = (x - \alpha)^k g(x)$ where (α) is a repeated root. If $f(x) = (x - \alpha)^k g(x)$, then $f'(x) = k(x - \alpha)^{k-1} g(x) + (x - \alpha) g'(x) = (x - \alpha)(k(x - \alpha)^{k-2} g(x) + g'(x))$. Therefore, $(x - \alpha) | (f, f') \Rightarrow (f, f') \neq 1$

   Assume $(f, f') \neq 1$ then (f, f') is a non-constant polynomial, $h(x)$. Then $f = h(x) g_1(x)$ and $f' = h(x) g_2(x)$ Therefore, f and f' share roots of $h(x)$ and so f has repeated roots.

2. Let $f = hf'$ and $g = hg'$ where $h, f', g' \in F[x]$ and f' and g' are relatively prime.

   Then $\exists a, b \in F$ s.t:

$$af' + bg' = 1$$

   which is equivalent to

$$\begin{aligned} h(af' + bg') &= h(1) \\ haf' + hbg' &= h \\ af + bg &= h \end{aligned}$$

   Since $\exists a, b \in E$

$$af' + bg' = 1$$

   in E, this implies

$$af + bg = h$$

   Therefore, $(f, g)_F = (f, g)_E = h$

3. Eisenstein's Criterion says that if you have a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, and a prime p dividing each a_i for $0 \leq i < n$, but p doesn't divide a_n and p^2 doesn't divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. For $f(x) = x^n - m$, the conditions to meet the criterion are simplified to $p | m \wedge p \nmid 1 \wedge p^2 \nmid m$ since $a_0 = m$ and $a_n = 1$. Let m be expressed as a prime factorization $p_1 \ldots p_n$. By the definition of square free $(\forall p \in p_1 \ldots p_n)(p^2 \nmid m)$. Therefore, $(\forall p \in p_1 \ldots p_n)(p | m \wedge p \nmid 1 \wedge p^2 \nmid m)$.

4. Let $f(x) = x^4 + 6x^3 + 12x^2 + 6x + 1$ Let's apply a coordinate transformation to $f(x)$. Since a coordinate transformation does not change whether a polynomial is irreducible, we can pick a clever coordinate transformation to make the problem simpler. Since there are multiple terms with positive coefficients that are multiples of 6 making a coordinate transformation of $x - 1$ might be a good choice. $f(x-1) = 2 - 4x + 2x^3 + x^4$ Now we can use Eisenstein's Criterion more easily. Recall Eisenstein's Criterion says that if you have a polynomial $g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, and a prime p dividing each a_i for $0 \leq i < n$, but p doesn't divide a_n and p^2 doesn't divide a_0, then $g(x)$ is irreducible in $\mathbb{Q}[x]$. Using Eisenstein's criterion on $f(x - 1)$, we can see that

a prime $p = 2$ divides each a_i for $0 \leq i < n$ $(2|2, -4, 2)$, $p = 2$ doesn't divide $a_n = 1$, and $p^2 = 4$ doesn't divide $a_0 = 2$; therefore, $f(x-1)$ is irreducible in $\mathbb{Q}[x]$ and so $f(x)$ is irreducible in $\mathbb{Q}[x]$.