Math 128B, problem set 09
CORRECTED MON APR 26
Outline due: Fri Apr 23
Due: Wed Apr 28
Last revision due: Mon May 17

Problems to be done, but not turned in: (Ch. 22) 1–49 odd; (Ch. 23) 1–21 odd.

Problems to be turned in:

1. Let $E = \mathbf{Z}_2(\alpha)$, where α is a root of $x^4 + x^3 + 1$ (i.e., $\alpha^4 + \alpha^3 + 1 = 0$).
   (a) What are the possible orders of elements of E^*?
   (b) Find a primitive element $\beta \in E^*$, where β is a polynomial in α of degree ≤ 3.
   (c) Make a table of all elements of E^*, with each row corresponding to an element $\gamma \in E^*$, containing the following information:
      - In the first column, describe γ as a polynomial in α of degree ≤ 3.
      - In the second column, describe γ as a power of β.
      - In the third column, write the order of γ.
2. Draw the subfield lattices of $GF(7^{105})$ and $GF(11^{50})$.
3. Let $f(x) \in \mathbf{Z}_5[x]$ be a cubic polynomial that is irreducible over $\mathbf{Z}_5$, and let $E = \mathbf{Z}_5[x]/\langle f(x)\rangle$. Suppose we have $a \in E^*$ such that a is **not** a zero of $x^5 - x$.
   (a) Prove that $E = \mathbf{Z}_5(a)$.
   (b) What are all possible orders of a as an element of E^*? Prove your answer.
4. Let E be a finite field of characteristic 2. For this problem, you may assume that the map $\rho : E \to E$ defined by $\rho(x) = x^2$ is an automorphism of E.
   (a) Prove that $\rho(x) = x$ if and only if $x \in \mathbf{Z}_2$ (i.e., if and only if $x = 0, 1$).
   (b) Suppose $f(x) \in \mathbf{Z}_2[x]$, $\alpha \in E$, and $f(\alpha) = 0$. Prove that $f(\rho(\alpha)) = 0$.
   (c) Let $E = \mathbf{Z}_2(\alpha)$, where α is a root of the irreducible polynomial $x^5+x^2+1 \in \mathbf{Z}_2[x]$. Use ρ to factor $x^5 + x^2 + 1$ into linear factors over E.
5. Let p be prime and $e \geq 1$.
   (a) Let $m(x) \in \mathbf{Z}_p[x]$ be irreducible of degree d, where d divides e. Use the field $\mathbf{Z}_p[x]/\langle m(x)\rangle$ to prove that $m(x)$ divides $x^{p^d} - x$, and therefore, that $m(x)$ divides $x^{p^e} - x$.
   (b) Conversely, suppose $m(x) \in \mathbf{Z}_p[x]$ is irreducible over $\mathbf{Z}_p$, $m(x)$ divides $x^{p^e} - x$ in $\mathbf{Z}_p[x]$, and $d = \deg m(x)$. Prove that there exists some $\alpha \in GF(p^e)$ such that $m(\alpha) = 0$, and use $\mathbf{Z}_p(\alpha)$ to prove that d divides e.
6. Suppose α is a positive real root of $x^5 - 27x + 12$. Prove that α is not constructible (in the sense of Ch. 23).