Math200b, homework 6

Golsefidy

March 2019

Finite fields.

1. (a) Suppose p is a prime. Prove that $\mathbb{F}_{p^m}$ can be embedded into $\mathbb{F}_{p^n}$ if and only if $m|n$. (**Hint**. ($\Rightarrow$) consider $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_{p^m}$. ($\Leftarrow$) show that $x^{p^m} - x | x^{p^n} - x$.)

   (b) Suppose $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree d. Prove that $f(x)|x^{p^d} - x$. (**Hint**. There is a field extension $E/\mathbb{F}_p$ and $\alpha \in E$ such that $E = \mathbb{F}_p[\alpha]$ and $f(\alpha) = 0$.)

   (c) Suppose $f(x) \in \mathbb{F}_p[x]$ is irreducible and $f(x)|x^{p^n} - x$.

Prove that $\deg f | n$. (**Hint**. Argue that there is $\alpha \in \mathbb{F}_{p^n}$ such that $f(\alpha) = 0$; consider $\mathbb{F}_p[\alpha] \subseteq \mathbb{F}_{p^n}$ and use part (a).)

(d) Let $P_d := \{f(x) \in \mathbb{F}_p[x] | \deg f = d, f \text{ is monic irreducible}\}$. Prove that

$$\prod_{d|n} \prod_{f(x) \in P_d} f(x) = x^{p^n} - x.$$

Deduce that $p^n = \sum_{d|n} d|P_d|$. (**Hint**. $x^{p^n} - x$ is square-free.)

Remark. Using Möbius inversion, we can get a closed formula for the number of irreducible monic polynomials of degree n over $\mathbb{F}_p$,

$$|P_n| = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

In particular, we can deduce that $|P_n| > 0$ (why?).

2. Suppose p is prime and $a \in \mathbb{F}_p^\times$. Prove that $x^p - x + a$ is irreducible in $\mathbb{F}_p[x]$. (**Hint**. Suppose E is a splitting field of $x^p - x + a$ over $\mathbb{F}_p$, and $\alpha \in E$ is a zero of $f(x) := x^p - x + a$. Prove that $\alpha + i$ is a zero of $f(x)$ for any

$i \in \mathbb{F}_p$, and deduce that $f(x) = \prod_{i \in \mathbb{F}_p}(x - \alpha - i)$. Suppose $\deg m_{\alpha,\mathbb{F}_p} = d$; consider the coefficient of x^{d-1} of $m_{\alpha,\mathbb{F}_p}(x)$ to deduce $d = p$.)

3. Suppose $p_1(x), \ldots, p_n(x)$ are irreducible in $\mathbb{F}_p[x]$. Suppose E is a splitting field of $\prod_{i=1}^n p_i(x)$ over $\mathbb{F}_p$. Prove that

$$[E : \mathbb{F}_p] = \operatorname{lcm}_{i=1}^n \deg p_i.$$

(**Hint**. Let $m := \operatorname{lcm}_{i=1}^n \deg p_i$. Then $p_i(x) | x^{p^m} - x$; deduce that $\mathbb{F}_{p^m}$ contains a splitting field of $\prod_{i=1}^n p_i(x)$. On the other hand, argue that $\deg p_i | [E : \mathbb{F}_p]$ for any i.)

4. Suppose $m, n \in \mathbb{Z}^+$, $d := \gcd(m, n)$, and $l := \operatorname{lcm}(m, n)$. Identify $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ with certain subfields of $\mathbb{F}_{p^l}$; this can be done because of problem 1 (a).

   (a) Show that $\mathbb{F}_{p^d}$ can be identified with $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}$.

   (b) Prove that $\mathbb{F}_{p^d} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^d} \simeq \bigoplus_{i=1}^d \mathbb{F}_{p^d}$ as $\mathbb{F}_p$-algebras. (**Hint**. Suppose $f(x) \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree d. Prove that $\mathbb{F}_{p^d}$ is a splitting field of $f(x)$ over $\mathbb{F}_p$ and $\mathbb{F}_{p^d} \simeq \mathbb{F}_p[x]/\langle f(x)\rangle$.)

(c) Prove that $\mathbb{F}_{p^m} \otimes_{\mathbb{F}_{p^d}} \mathbb{F}_{p^n} \simeq \mathbb{F}_{p^l}$ as $\mathbb{F}_{p^d}$-algebras. (**Hint.** Show that $\theta : \mathbb{F}_{p^m} \otimes_{\mathbb{F}_{p^d}} \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^l}, \theta(a \otimes b) = ab$ gives us a well-defined $\mathbb{F}_{p^d}$-algebra homomorphism. Show that $\mathrm{Im}(\theta)$ is a field that has copies of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ as subfields. Deduce that θ is onto. Compare the dimension of both sides as $\mathbb{F}_{p^d}$-vector spaces to deduce that θ is injective.)

(d) Prove that $\mathbb{F}_{p^n} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^m} \simeq \bigoplus_{i=1}^{d} \mathbb{F}_{p^l}$ as $\mathbb{F}_p$-algebras. (**Hint.** $\mathbb{F}_{p^n} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^m} \simeq \mathbb{F}_{p^n} \otimes_{\mathbb{F}_{p^d}} \mathbb{F}_{p^d} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^d} \otimes_{\mathbb{F}_{p^d}} \mathbb{F}_{p^m}$.)

Splitting fields.

1. Suppose F is a field, $f(x) \in F[x] \setminus F$, and E is a splitting field of $f(x)$ over E.

   (a) Prove that, if $\gcd(f, f') \neq 1$, then $F[x]/\langle f(x)\rangle \otimes_F E$ has a non-zero nilpotent element.

   (b) Prove that, if $\gcd(f, f') = 1$, then

$$F[x]/\langle f(x)\rangle \otimes_F E \simeq \underbrace{E \oplus \cdots \oplus E}_{\deg f\text{-times}};$$

in particular it has no non-zero nilpotent elements.

2. Suppose $E \subseteq \mathbb{C}$ is a splitting field of $x^p - 2$ over $\mathbb{Q}$ where p is a prime.

   (a) Prove that $E = \mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ where $\zeta_p = e^{\frac{2\pi i}{p}}$.

   (b) Prove that $[E : \mathbb{Q}] = p(p-1)$. (**Hint**. Show that $[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}] = p$ and $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = p - 1$ and use $\gcd(p, p-1) = 1$ to deduce $p(p-1) | [E : \mathbb{Q}]$. Use $[E : \mathbb{Q}] = [E : \mathbb{Q}[\zeta_p]][\mathbb{Q}[\zeta_p] : \mathbb{Q}]$ to deduce $[E : \mathbb{Q}] \leq p(p-1)$.)

Tower of fields.

1. Suppose $a_i \in \mathbb{Q}^\times$. Prove that $\sqrt[3]{2} \notin \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_n}]$.

2. Suppose F is a field and its characteristic is not 2. Let $a, b \in F^\times \setminus F^{\times 2}$. Prove that

$$[F[\sqrt{a}, \sqrt{b}] : F] = 4 \Leftrightarrow ab \notin F^{\times 2}.$$

3. Suppose F is a field and $[F[\alpha] : F]$ is odd. Prove that $F[\alpha] = F[\alpha^2]$.