Problem Set 11

Due Thursday, April 16

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Classification of finite fields:

(a) Let F be a finite field; i.e., a field with finitely many elements. Show that $|F| = p^n$ for some prime number p and integer $n \geq 1$.

Proof. Note that every field contains a prime field, which is $\mathbb{Q}$ if F has characteristic 0 and is $\mathbb{F}_p$ if F has characteristic p. Since $\mathbb{Q}$ is infinite, the prime field must be $\mathbb{F}_p$ for some prime number p. Note that $F/\mathbb{F}_p$ must be finite, since otherwise F is an infinite-dimensional vector space, and infinite as a set. If $[F : \mathbb{F}_p] = n$, then $F \cong \mathbb{F}_p^n$ as vector spaces, so $|F| = p^n$. □

(b) Let p be a prime number and $n \geq 1$. Show that the polynomial $f(x) = x^{p^n} - x$ has p^n distinct roots in $\overline{\mathbb{F}_p}$, and that the set of roots of f in $\overline{\mathbb{F}_p}$ forms a subfield of $\overline{\mathbb{F}_p}$. Deduce that there exists a field with p^n elements.

Proof. Let $f(x) = x^{p^n} - x$. Then $f'(x) = -1 \neq 0$, so $\gcd(f, f') = 1$. Thus, f is separable, so it has exactly p^n roots in the algebraic closure $\overline{\mathbb{F}_p}$.

Let E denote the roots of f in $\overline{\mathbb{F}_p}$. Since $\mathbb{F}_p[x]$ has prime characteristic p, the Frobenius map $h_n \colon \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ defined by $h_n(a) := a^{p^n}$ for all $a \in \overline{\mathbb{F}_p}$ is a ring homomorphism. Then

- $f(0) = 0^{p^n} - 0 = 0$ and $f(1) = 1^{p^n} - 1 = 0$, so $0, 1 \in E$.
- If $a, b \in E$, then $h_n(a - b) = h_n(a) - h_n(b)$, so

$$f(a-b) = h_n(a-b) - (a-b) = h_n(a) - a - h_n(b) + b = f(a) - f(b) = 0 - 0 = 0,$$

  so $a - b \in E$.
- If $a, b \in E$, then $h_n(ab) = h_n(a)h_n(b)$, so

$$f(ab) = h_n(ab) - (ab) = h_n(a)h_n(b) - ab = (h_n(a) - a)h_n(b) - a(h_n(b) - b) = f(a)h_n(b) - af(b) = 0,$$

  so $ab \in E$.

Thus, E is a subring of $\overline{\mathbb{F}_p}$. In particular, E is a domain, and is finite, so E is a field. In particular E is a field with p^n elements. □

(c) Show that[1] if K is any field with p^n elements, then K is a splitting field for $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$. Deduce that all fields with p^n elements are isomorphic.

Proof. Let K be a field with p^n elements. From part (a), we note that $\mathbb{F}_p$ is a subfield of K. Then $K^\times$ is a group with $p^n - 1$ elements, and we showed in an earlier problem set that a finite subgroup of the multiplicative group of a field is cyclic, so $K^\times \cong \mathbb{Z}/(p^n - 1)$. In particular, for every $k \in K^\times$, we have $k^{p^n} = k^{p^n - 1}k = k$; also $0^{p^n} - 0 = 0$. Thus, every element of K is a root of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Thus, the roots of f generate K, so K is a splitting field for f. Since all splitting fields for a polynomial are isomorphic, all fields with p^n elements are isomorphic. □

Problem 2. Let p be an odd prime integer and let L be the splitting field of $x^p - 2$ in $\mathbb{C}$. Determine $[L : \mathbb{Q}]$.

Proof. We have $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$ since $x^p - 2$ is irreducible (over $\mathbb{Z}$ by Eisenstein's Criterion applied to the prime p, over $\mathbb{Q}$ by Gauss' Lemma; complete the details as we have done in many similar problems). By the degree formula, it follows that p divides $[L : \mathbb{Q}]$. We have

$$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1$$

since $x^{p-1} + x^{p-2} + \cdots + x + 1$ has $e^{2\pi i/p}$ as a root and is irreducible over $\mathbb{Q}$ by Problem 3, so it must be the minimal polynomial of $e^{2\pi i/p}$. By the degree formula, it follows that $p - 1$ divides $[L : \mathbb{Q}]$. Since p and $p - 1$ are relatively prime, we conclude that $p(p - 1)$ divides $[L : \mathbb{Q}]$. On the other hand, we have

$$L = \mathbb{Q}(\sqrt[p]{2}, e^{2\pi i/p}) \quad \text{and} \quad [L : \mathbb{Q}(e^{2\pi ip})] \leqslant p - 1,$$

since $\sqrt[p]{2}$ is a root of $x^{p-1} + x^{p-2} + \cdots + x + 1$. By the Degree Formula, we conclude that

$$[L : \mathbb{Q}] \leqslant (p - 1)p.$$

Thus

$$[L : \mathbb{Q}] = p(p - 1).$$

□

Problem 3. Let F be a field and let $f \in F[x]$.

(a) Assume $\text{char}(F) = 0$. Prove that f is not separable if and only if the prime factorization of f in $F[x]$ admits a repeated factor.

(b) Give a counterexample to the previous part when the assumption $\text{char}(F) = 0$ is omitted.

Proof.

(a) Suppose f is not separable; say $\alpha \in \overline{F}$ is a repeated root of f. Then $m_{\alpha,F}$ is irreducible and $m_{\alpha,F} \mid f$, so that $f = gh$ for some $h \in F[x]$. Moreover, since $\text{char}(F) = 0$ and $m_{\alpha,F}$ is irreducible, we know that $m_{\alpha,F}$ is separable and hence α is not a repeated root of $m_{\alpha,F}$. That is, in $\overline{F}[x]$ we have $g = (x - \alpha)l$ with $l(\alpha) \neq 0$. Since $f = (x - \alpha)^2 j$, we must have that $x - \alpha$ divides h in $\overline{F}[x]$. That is, we must have $h(\alpha) = 0$. But then g divides h too and so $f = g^2 q$ for some q. So g is a repeated prime (irreducible) factor of f.

Assume now that $f = g^2 m$ for some prime (irreducible) g. Then for any root α of g in $\overline{F}$, we have that $f = (x - \alpha)^2 l$ in $\overline{F}[x]$ and hence f is not separable.

[1] Hint: Show the stronger claim that every element of K is a root of $f(x)$. You might find it helpful to recall something you proved earlier about the group $K^\times$.

(b) Let $F = (\mathbb{Z}/p)(y)$, the field of fractions of the polynomial ring $(\mathbb{Z}/p)[y]$, and let $f(x) = x^p - y$. Since $(\mathbb{Z}/p)[y]$ is a PID and y is a prime element, then f is irreducible by Eisenstein's Criterion. If α is any root of f in $\overline{F}$, then $f(x) = (x-\alpha)^p$ by the Freshman's Dream. Since $p \geqslant 2$, f is not separable. But since f is irreducible over F, it doesn't have a repeated factor in its prime factorization over F. □

Problem 4. Let $F \subseteq L$ is a field extension and $S \subseteq L$. Show that

$$F(S) = \left\{ \frac{f(s_1,\dots,s_t)}{g(s_1,\dots,s_t)} \;\middle|\; t \geq 0,\ s_1,\dots,s_t \in S,\ f(x_1,\dots,x_t), g(x_1,\dots,x_t) \in F[x_1,\dots,x_t],\ g(s_1,\dots,s_t) \neq 0 \right\}.$$

Proof. Let K denote the right hand side. We will show that K is the unique smallest subfield of L containing $F \cup S$. Clearly K contains $F \cup S$. We claim that K is a subfield of L. Clearly, $0, 1 \in K$. Given two elements f/g and f'/g' of K, by taking the union, we can assume without loss of generality that f, g, f', g' are polynomial expressions in the same finite subset $s_1, \dots, s_t \in S$. Then

$$\frac{f(s_1,\dots,s_t)}{g(s_1,\dots,s_t)} - \frac{f'(s_1,\dots,s_t)}{g'(s_1,\dots,s_t)} = \frac{f(s_1,\dots,s_t)g'(s_1,\dots,s_t) - g(s_1,\dots,s_t)f'(s_1,\dots,s_t)}{g(s_1,\dots,s_t)} g'(s_1,\dots,s_t) \in K,$$

$$\frac{f(s_1,\dots,s_t)}{g(s_1,\dots,s_t)} \frac{f'(s_1,\dots,s_t)}{g'(s_1,\dots,s_t)} = \frac{f(s_1,\dots,s_t)f'(s_1,\dots,s_t)}{g(s_1,\dots,s_t)} g'(s_1,\dots,s_t) \in K,$$

and if $f/g \neq 0$, then $f(s_1,\dots,s_t) \neq 0$, and

$$\frac{f(s_1,\dots,s_t)}{g(s_1,\dots,s_t)}^{-1} = \frac{g(s_1,\dots,s_t)}{f(s_1,\dots,s_t)} \in K.$$

This shows that K is a subfield of L.

It remains to show that any subfield E of L containing $F \cup S$ contains K. But since E is closed under addition, subtraction, mutliplication, and division, any rational function expression in S with coefficients in F must also be in E. That is, $E \subseteq K$.

This shows that $F(S) = K$. □