Problem Set 10

Due Thursday, April 9

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. Let E be the field extension of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ all four complex roots of the polynomial x^4+5. That is, $E=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ where

$$\alpha_1 = e^{\pi i/4}\sqrt[4]{5}, \quad \alpha_2 = e^{3\pi i/4}\sqrt[4]{5}, \quad \alpha_3 = e^{5\pi i/4}\sqrt[4]{5}, \quad \alpha_4 = e^{7\pi i/4}\sqrt[4]{5}.$$

(a) Prove that there exists[1] a field extension $\mathbb{Q}\subseteq F$ such that $F\subseteq E$, $F\subseteq\mathbb{R}$, and $[F:\mathbb{Q}]=4$.

Proof. Note that

$$\alpha_1 = \sqrt[4]{5}\cdot\frac{\sqrt{2}}{2}(1+i) = \frac{\sqrt[4]{20}}{2}(1+i) \quad \text{and} \quad \alpha_4 = \frac{\sqrt[4]{20}}{2}(1-i)$$

so $\alpha_1+\alpha_4=\sqrt[4]{20}$.

Moreover, $\alpha_1+\alpha_4$ is thus a root of x^4-20, which is irreducible: using Gauss' Lemma, we just need to show it is irreducible over $\mathbb{Z}$, and Eisenstein's Criterion applies with $p=5$ to show that x^4-20 is irreducible over $\mathbb{Z}$. Hence, $m_{\alpha_1+\alpha_2,\mathbb{Q}}(x)=x^4-20$. Set $F=\mathbb{Q}(\alpha_1+\alpha_4)$. Then $F\subseteq E$ and $[F:\mathbb{Q}]=4$, as desired. Moreover, $F\subseteq\mathbb{R}$ since $\alpha_1+\alpha_4\in\mathbb{R}$ and $\mathbb{Q}\subseteq\mathbb{R}$. □

(b) Determine $[E:\mathbb{Q}]$ with justification.

Proof. By the Degree Formula, $[E:\mathbb{Q}]=[E:F][F:\mathbb{Q}]=[E:F]\cdot 4$. We claim that $E=F(i)$. First note that $\frac{\alpha_1}{\alpha_4}=\frac{1+i}{1-i}=i$ so that $i\in E$ and hence $F(i)\subseteq E$.

Since each α_j has the form $\frac{\sqrt[4]{20}}{2}(\pm 1\pm i)$ and both $\sqrt[4]{20}$ and i belong to $F(i)$, we have $\alpha_j\in F(i)$ for all j and thus $E\subseteq F(i)$. We conclude that $E=F(i)$.

Since i is a root of $x^2+1\in F[x]$ we have $[F(i):F]\leqslant 2$. Since $F\subseteq\mathbb{R}$, we have $F\neq F(i)$ and thus $[E:F]=2$. By the Degree Formula, $[E:\mathbb{Q}]=[E:F][F:\mathbb{Q}]=2\cdot 4=8$. □

Problem 2. Let F be a field and $f,g\in F[x]$ be nonzero polynomials. Show that $\gcd(f,g)=1$ in $F[x]$ if and only if f and g have no common roots in an algebraic closure $\overline{F}$ of F.

[1] Note that $\alpha_1+\alpha_4$ is a real number; find it explicitly.

Proof. We prove the contrapositive: 1 is not a gcd for f and g in $F[x]$ if any only if f and g have a common root in an algebraic closure $\overline{F}$ of F.

($\Rightarrow$) If 1 is not a gcd for f and g in $F[x]$, then $\gcd(f,g) = h \in F[x]$ for some polynomial h with $\deg(h) \geqslant 1$. Then since h is nonconstant polynomial, we know h has a root $\alpha \in \overline{F}$. Since $h \mid f$ and $h \mid g$, it follows that α is also a root for both f and g.

($\Leftarrow$) Suppose that f and g have a common root $\alpha \in \overline{F}$, that is $f(\alpha) = g(\alpha) = 0$. Then α is algebraic over F and hence it has a minimal polynomial $m_{\alpha,F} \in F[x]$. Furthermore, by properties of the minimal polynomial it follows that since $f(\alpha) = 0$ then $m_{\alpha,F} \mid f$ and since $g(\alpha) = 0$ then $m_{\alpha,F} \mid g$. Thus $m_{\alpha,F}$ is a common divisor for f, g in $F[x]$ and therefore by properties of the gcd $m_{\alpha,F} \mid \gcd(f,g)$. This shows that, since $\deg(m_{\alpha,F}) \geqslant 1$, $\deg(\gcd(f,g)) \neq 0$, therefore no unit of F can be a gcd for f, g in $F[x]$. □

Problem 3. Let $F \subseteq L$ be a field extension and let $S \subseteq L$ be an arbitrary subset of L whose elements are all algebraic over F. Show[2] that $F \subseteq F(S)$ is algebraic.

Proof. Given $\alpha \in F(S)$, we want to show that α is algebraic over F. By the hint, α can be written as a rational function in S with coefficients in F, which means it uses only finitely many elements $\alpha_1, \ldots, \alpha_n \in S$, so $\alpha \in F(\alpha_1, \ldots, \alpha_n)$. Since $\alpha_1, \ldots, \alpha_n \in S$ are all algebraic over F, the extensions $F \subseteq F(\alpha_1)$, $F(\alpha_1) \subseteq F(\alpha_1, \alpha_2), \ldots, F(\alpha_1, \ldots, \alpha_{n-1}) \subseteq F(\alpha_1, \ldots, \alpha_n)$ are all algebraic. We showed in class that the composition of algebraic extensions is algebraic; thus the tower of algebraic extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2), \ldots, F(\alpha_1, \ldots, \alpha_{n-1}) \subseteq F(\alpha_1, \ldots, \alpha_n)$$

implies that $F \subseteq F(\alpha_1, \ldots, \alpha_n)$ is algebraic. In particular, $\alpha \in F(\alpha_1, \ldots, \alpha_n)$ is algebraic over F. We conclude that $F \subseteq F(S)$ is algebraic. □

Proof. We prove the contrapositive: 1 is not a gcd for f and g in $F[x]$ if any only if f and g have a common root in an algebraic closure $\overline{F}$ of F.

($\Rightarrow$) If 1 is not a gcd for f and g in $F[x]$, then $\gcd(f,g) = h \in F[x]$ for some polynomial h with $\deg(h) \geqslant 1$. Then since h is nonconstant polynomial, we know h has a root $\alpha \in \overline{F}$. Since $h \mid f$ and $h \mid g$, it follows that α is also a root for both f and g.

($\Leftarrow$) Suppose that f and g have a common root $\alpha \in \overline{F}$, that is $f(\alpha) = g(\alpha) = 0$. Then α is algebraic over F and hence it has a minimal polynomial $m_{\alpha,F} \in F[x]$. Furthermore, by properties of the minimal polynomial it follows that since $f(\alpha) = 0$ then $m_{\alpha,F} \mid f$ and since $g(\alpha) = 0$ then $m_{\alpha,F} \mid g$. Thus $m_{\alpha,F}$ is a common divisor for f, g in $F[x]$ and therefore by properties of the gcd $m_{\alpha,F} \mid \gcd(f,g)$. This shows that, since $\deg(m_{\alpha,F}) \geqslant 1$, $\deg(\gcd(f,g)) \neq 0$, therefore no unit of F can be a gcd for f, g in $F[x]$. □

Problem 4. Let L be the splitting field of $f = x^5 - 11 \in \mathbb{Q}[x]$.

(a) Find the degree[3] of $[L : \mathbb{Q}]$.

(b) Let $F = \mathbb{Q}(\xi)$, where $\xi = e^{\frac{2\pi i}{5}}$ is a primitive fifth root of unity. Show that f is irreducible over F.

Proof.

[2] You can use without proof the analogue of Lemma 15.1.12 for larger generating sets: if $F \subseteq L$ is a field extension and $S \subseteq L$, then $F(S) = \{\frac{f(s_1,\ldots,s_t)}{g(s_1,\ldots,s_t)} \mid s_1, \ldots, s_t \in S,\ f(x_1, \ldots, x_t), g(x_1, \ldots, x_t) \in F[x_1, \ldots, x_t],\ g(s_1, \ldots, s_t) \neq 0\}$.

[3] Consider the chains $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{11}) \subseteq L$ and $\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq L$.

a) First, we claim that $L = \mathbb{Q}(\xi, \sqrt[5]{11})$. On the one hand, the roots of f are $\sqrt[5]{11}\xi^i$ for $i = 0, 1, 2, 3, 4$, so $L = \mathbb{Q}(\sqrt[5]{11}\xi^i \mid 0 \leqslant i \leqslant 4) \subseteq \mathbb{Q}(\xi, \sqrt[5]{11})$. On the other hand,

$$\xi = \frac{\sqrt[5]{11}\xi}{\sqrt[5]{11}} \in L,$$

so $L = \mathbb{Q}(\xi, \sqrt[5]{11})$.

We claim that f is irreducible over $\mathbb{Q}$: indeed, 11 divides all the coefficients of f of nonmaximal degree but the coefficient of maximal degree, 11^2 does not divide the degree 0 coefficient of f, and 11 is prime, so Eisenstein's Criterion says that f is irreducible over $\mathbb{Z}$. By Gauss' Lemma, f is irreducible over $\mathbb{Q}$. Since $\sqrt[5]{11}$ is a root of the monic irreducible polynomial f, we conclude that f is the minimal polynomial of $\sqrt[5]{11}$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5$.

By Problem Set 10, $g = x^4 + x^3 + x^2 + x + 1$ is irreducible, since 5 is prime. Note that ξ is a root of $(x-1)g = x^5 - 1$ but not a root of $x - 1$, so $g(\xi) = 0$. Since g is irreducible, we conclude that g is the minimal polynomial of ξ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$.

By the Degree Formula,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = 4[L : \mathbb{Q}(\xi)]$$

and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[5]{11})][\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5[L : \mathbb{Q}(\sqrt[5]{11})].$$

Thus $4|[L : \mathbb{Q}]$ and $5|[L : \mathbb{Q}]$. Since $\gcd(4, 5) = 1$, we conclude that $20|[L : \mathbb{Q}]$.

Now ξ still satisfies g over $F = \mathbb{Q}(\sqrt[5]{11})$, so $m_{\xi,F}|g$. Thus the degree of $m_{\xi,F}$ is at most 4, and $[L : \mathbb{Q}(\sqrt[5]{11})] \leqslant 4$. Therefore,

$$[L : \mathbb{Q}] = 5[L : \mathbb{Q}(\sqrt[5]{11})] \leqslant 20.$$

But $20|[L : \mathbb{Q}]$, so $[L : \mathbb{Q}] = 20$.

b) In the proof of part a) we showed that $[\mathbb{Q}(\sqrt[5]{11}) : \mathbb{Q}] = 5$, $[F : \mathbb{Q}] = [\mathbb{Q}(\xi) : \mathbb{Q}] = 4$, and $[L : \mathbb{Q}] = 20$. Moreover, $L = F(\sqrt[5]{2}$. By the Degree Formula,

$$[F(\sqrt[5]{2} : F][F : \mathbb{Q}] = [L : \mathbb{Q}] = 20.$$

Thus $[F(\sqrt[5]{2} : F] = 4$, so $m_{\sqrt[5]{2},F}$ has degree 5. Since $f(\sqrt[5]{2}) = 0$ and $f \in F[x]$ is monic, we conclude that f is the minimal polynomial of $\sqrt[5]{2}$ over F. In particular, f must be irreducible over F. □