Math 505 HW2

Rohan Mukherjee

February 7, 2024

1. Applying the Eisenstein criterion to $f(x)$ with $p = 3$ shows that f is irreducible. Next, notice that $\alpha^3 + 9\alpha + 7 = 1$. Thus,

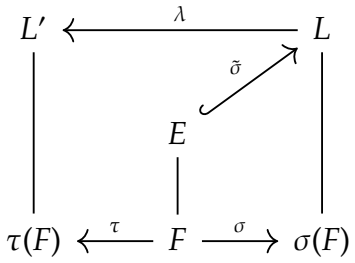
$$\frac{1}{1+\alpha} = \frac{\alpha^3 + 9\alpha + 7}{1+\alpha}$$

Replacing α with an indeterminate x and applying polynomial long division to the RHS (in $\mathbb{Z}[x]$), will give us that $(x+1)(x^2 - x + 10) = (x^3 + 9x + 7) + 3 = 1$. Plugging in α to both sides will show that $(\alpha + 1)(\alpha^2 - \alpha + 10) = 1 + 3 = 4$. We conclude that $(1+\alpha)^{-1} = \frac{1}{4}(\alpha^2 - \alpha + 10)$.

2. Notice that $\mathbb{Q}(1+i) = \mathbb{Q}(i)$, since $i = (1+i) - 1$, and vice versa. Clearly $\mathbb{Q}(i)/\mathbb{Q}$ is a degree 2 extension, since $x^2 + 1$ is the minimal polynomial of i (it is clearly irreducible, or else it would split as a product of linear factors, but $\mathbb{Q}$ contains none of it's roots). Thus $(x-1)^2 + 1 = x^2 - 2x + 2$ is the minimal polynomial of $1 + i$ (it is again irreducible for the same reasons–it's other root being $1 - i$).

3. (1) Recall that if $p(x) = \mathrm{Irr}_F(\alpha)$, and β is any root of $p(x)$, the map sending F identically to F and sending α to β determines a homomorphism $\sigma : F(\alpha) \to \overline{F}$. Since sending α to a different root determines a different homomorphism, we have immediately that $[F(\alpha) : F]_{\mathrm{sep}} \geq n_0(p)$, where $n_0(f)$ is the number of distinct roots of a polynomial f (We have stolen this notation from the wonderous Mason-Stothers theorem, which the author has written a paper about). Similarly, let $\sigma : F(\alpha) \to \overline{F}$ be a homomorphism sending F identically to F, and $p(x) = \mathrm{Irr}_F(\alpha)$. We see that $0 = \sigma(p(\alpha)) = p(\sigma(\alpha))$ since σ is a homomorphism, thus $\sigma(\alpha)$ is another root of $p(x)$. Specifying where α goes uniquely determines σ (since F is sent identically to F), so we have that $[F(\alpha) : F]_{\mathrm{sep}} \leq n_0(p)$, which completes the proof.

(2) Let $\sigma : F \to \overline{L}$ be an embedding of F into an algebraically closed field L, and $\tau : F \to \overline{L}'$ be an embedding of F into a (possibly different) algebraically closed field L', E/F an algebraic extension, and $\tilde{\sigma}$ an extension of σ to an embedding of E into L. By the extension theorem, we can extend $\tau \circ \sigma^{-1} : \sigma(F) \to L'$ to an embedding λ of L into L', which is an isomorphism of fields by the corollary to the extension theorem. Now let $\tilde{\sigma}$ be an extension of σ to an embedding of E into L, giving us the following commutative diagram:



$\lambda \circ \tilde{\sigma}$ is now an extension of τ to an embedding of E into L', since λ was chosen to make the above diagram commute (By this we mean that the path from F to $\tau(F)$ to L' is the same as the path from F to E to L to L'). Notice also that if $\tilde{\sigma}_2$ is a different extension of F to an embedding $E \to L$, then $\lambda \circ \tilde{\sigma}_2 \neq \lambda \circ \tilde{\sigma}$ since λ is injective. This yields an injection from extensions of σ to extensions of τ. Similarly, by considering λ^{-1} and using the exact same arguments, we get the reverse injection, which shows that

$$\left| \left\{ \begin{array}{l} \text{extensions of } \tau \text{ to} \\ \text{embeddings } E \hookrightarrow L' \end{array} \right\} \right| = \left| \left\{ \begin{array}{l} \text{extensions of } \sigma \text{ to} \\ \text{embeddings } E \hookrightarrow L \end{array} \right\} \right|$$

In particular, if $\tau = \mathrm{id}_F : F \to \overline{F}$, this shows that $[E : F]_{\text{sep}} = \left| \left\{ \begin{array}{l} \text{extensions of } \sigma \text{ to} \\ \text{embeddings } E \hookrightarrow \overline{F} \end{array} \right\} \right|$ for any embedding $\sigma : F \to L$. Now we can use a simple counting argument. Let $L/E/F$ be a tower of finite extensions and let $\{ \sigma_i \}_{i \in I}$ be the set of embeddings $\sigma_i : E \to \overline{F}$ with $\sigma_i|_F = \mathrm{id}_F$, and to each σ_i assign the set $\left\{ \tau_{ij} \right\}_{j \in J}$ which is extensions of σ_i to embeddings $\tau_{ij} : L \hookrightarrow \overline{F}$. We know that $\left| \left\{ \tau_{ij} \right\}_{j \in J} \right| = [L : E]_{\text{sep}}$ for any j by the lemma, and clearly $|\{ \sigma_i \}_{i \in I}| = [E : F]_{\text{sep}}$. Now, since

$$\coprod_{i \in I} \left\{ \tau_{ij} \right\}_{j \in J} = [L : F]_{\text{sep}}$$

(we can restrict any extension $\sigma : L \to F$ to E to see this, and this is clearly a disjoint union), we have that $[L : F]_{\text{sep}} = [L : E]_{\text{sep}}[E : F]_{\text{sep}}$.

4. (1) We claim that every finite extension is of the form $F(\alpha_1, \ldots, \alpha_n)$ for algebraic α and $n \geq 0$. Let E be a finite extension of F. If $E = F$ we are done, otherwise find $\alpha_1 \in E \setminus F$. We see that the minimal polynomial of α_1 has degree at least 2 (otherwise $\alpha_1 \in F$), so $[F(\alpha_1) : F] \geq 2$. We may now repeat the process: if $E = F(\alpha_1)$, we are done, otherwise find $\alpha_2 \in E \setminus F(\alpha_1)$. Again the minimal polynomial (now with coefficients in $F(\alpha_1)$) has degree at least 2, so $[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_1)] \cdot [F(\alpha_1) : F] \geq 2^2$. We may continue this process finitely many steps until $F(\alpha_1, \ldots, \alpha_n) = E$, since $F(\alpha_1, \ldots, \alpha_n)$ is always a subfield of E, and we can make it larger unless $F(\alpha_1, \ldots, \alpha_n) = E$, and since the degree of E is finite, this process is finite.

   Remark. This process takes $\leq \log_2(d)$ steps to complete, where $d = [E : F]$.

   Now we can prove the claim by induction on the number of adjoined elements. The base case was part (1), since $[F(\alpha) : F] =$ the degree of $\mathrm{Irr}_F(\alpha) \geq$ the number of it's distinct roots. Suppose the claim is true for n adjoined elements for some $n \geq 1$. Then

$$\begin{aligned}
[F(\alpha_1, \cdots, \alpha_{n+1}) : F]_{\text{sep}} &= [F(\alpha_1, \ldots, \alpha_n) : F]_{\text{sep}} \cdot [F(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1}) : F(\alpha_1, \ldots, \alpha_n)]_{\text{sep}} \\
&\leq [F(\alpha_1, \ldots, \alpha_n) : F] \cdot [F(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1}) : F(\alpha_1, \ldots, \alpha_n)] \\
&= [F(\alpha_1, \ldots, \alpha_{n+1}) : F]
\end{aligned}$$

   (2) First we prove that if $\alpha \in F(\alpha)/F$ is not separable, then $[F(\alpha) : F]_{\text{sep}} < [F(\alpha) : F]$. Indeed, if α is not separable then it's minimal polynomial $\mathrm{Irr}_F(\alpha)$ has repeat roots, and so the number of distinct roots is strictly less than it's degree. This is fully equivalent (by 2.1) to the above (strict) inequality, proving this subclaim.

   Now, suppose that E/F is a finite extension, $[E : F]_{\text{sep}} = [E : F]$, but that there is an $\alpha \in E$ such that α is not separable. Using the procedure in part (1), we can write $E = F(\alpha, \beta_1, \ldots, \beta_n)$ for some $n \geq 0$. By our multiplicative property, we have that,

$$\begin{aligned}
[E : F]_{\text{sep}} &= [F(\alpha) : F]_{\text{sep}} [F(\alpha, \beta_1, \ldots, \beta_n) : F(\alpha)]_{\text{sep}} \\
&< [F(\alpha) : F] \cdot [F(\alpha, \beta_1, \ldots, \beta_n) : F(\alpha)] = [E : F]
\end{aligned}$$

   By the lemma, a contradiction. We prove the converse by induction on the number of adjoined variables. Problem 3.1 is the base case, so assume the converse is true for $n \geq 1$ adjoined variables, and let $E = F(\alpha_1, \ldots, \alpha_{n+1})$. Clearly $F(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1})/F(\alpha_1, \ldots, \alpha_n)$ is a finite separable extension, so the base case applies and we see that $[E : F(\alpha_1, \ldots, \alpha_n)]_{\text{sep}} = [E : F(\alpha_1, \ldots, \alpha_n)]$. By the induction hypothesis $[F(\alpha_1, \ldots, \alpha_n) : F]_{\text{sep}} = [F(\alpha_1, \ldots, \alpha_n) : F]$, so putting these together gives

us,

$$\begin{aligned}[E : F]_{\text{sep}} &= [E : F(\alpha_1, \ldots, \alpha_n)]_{\text{sep}} \cdot [F(\alpha_1, \ldots, \alpha_n) : F]_{\text{sep}} \\ &= [E : F(\alpha_1, \ldots, \alpha_n)] \cdot [F(\alpha_1, \ldots, \alpha_n) : F] = [E : F]\end{aligned}$$

which completes the proof.

(3) Recall from 3.1 that $[F(\alpha) : F]_{\text{sep}}$ = the number of distinct roots of $\text{Irr}_F(\alpha)$. If α is separable, this polynomial has all distinct roots, so this number is just the degree of $\text{Irr}_F(\alpha)$. This is precisely equal to $[F(\alpha) : F]$, which completes the proof.

5. (a) We showed that $f(x)$ is irreducible over $\mathbb{Z}$ on the last homework, which, by Lemma 4 on that same homework shows that $f(x)$ is irreducible over $\mathbb{Q}$.

(b) We need only show that $f(x)$ factors in $\mathbb{Q}(\rho)$. Notice once again that $f(x)(x-1) = x^p - 1$, and let $\zeta = e^{\frac{2\pi i}{p}}$. Notice that $f(\zeta^n) = 0$ for every $n \in \{0, \ldots, p-1\}$, and that $\zeta^n = \zeta^m$ iff $p \mid n - m$. In particular ζ^n for $n \in \{0, \ldots, p-1\}$ are all the p distinct roots of $f(x)(x-1)$ (recall that f has at most p roots), so $f(x)(x-1)$ factors as $f(x)(x-1) = \prod_{k=0}^{p-1}(x - \zeta^k) = (x-1)\prod_{k=1}^{p-1}(x - \zeta^k)$. Since ρ is another pth root of unity we have that $\rho = \zeta^k$ for some $k \in \{1, \ldots, p-1\}$ (0 being obviously excluded). Since $k \in (\mathbb{Z}/p)^\times$, k has an inverse (mod p), say a, with $k \cdot a = 1 + p\ell$. Notice then that

$$\rho^a = e^{\frac{2\pi i(1+p\ell)}{p}} = e^{\frac{2\pi i}{p}} \cdot e^{2\pi i\ell} = \zeta$$

Which shows that $f(x)$ also factors as $\prod_{k=1}^{p-1}(x - \rho^{ak})$, completing the proof that $\mathbb{Q}(\rho)$ is a splitting field of f.