Math 505 HW6

Rohan Mukherjee

February 12, 2024

1. We first show that $f(x) = x^4 - 4x^2 - 1$ is irreducible. Clearly, the rational root theorem shows that this has no roots over $\mathbb{Q}$. Notice that by just explicitly checking, the only irreducible polynomials of degree 2 in $\mathbb{F}_3$ are

$$x^2 + 1$$
$$x^2 + x + 2$$
$$x^2 + 2x + 2$$

Clearly $\overline{f}(x) = x^4 + 2x^2 - 1$ has no roots in $\mathbb{F}_3$ (checked by plugging in all possibilities). Next, dividing $\overline{f} \in \mathbb{F}_3[x]$ by each polynomial results in a remainder of 1, x, and 1 respectively, so f is irreducible in $\mathbb{F}_3$ thus also in $\mathbb{Q}$.

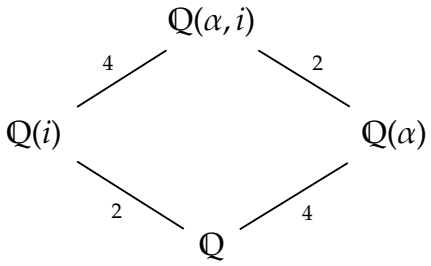
Now we explicitly find the roots. Let $y = x^2$. Then our polynomial becomes

$$y^2 - 4y^2 - 1$$

Which has solutions $y = \frac{4 \pm \sqrt{16+4}}{2} = 2 \pm \sqrt{5}$. Thus our original polynomial has solutions $x = \pm\sqrt{2 \pm \sqrt{5}}$ (4 distinct solutions). Notice that

$$\sqrt{2 + \sqrt{5}} \cdot \sqrt{2 - \sqrt{5}} = \sqrt{4 - 5} = i$$

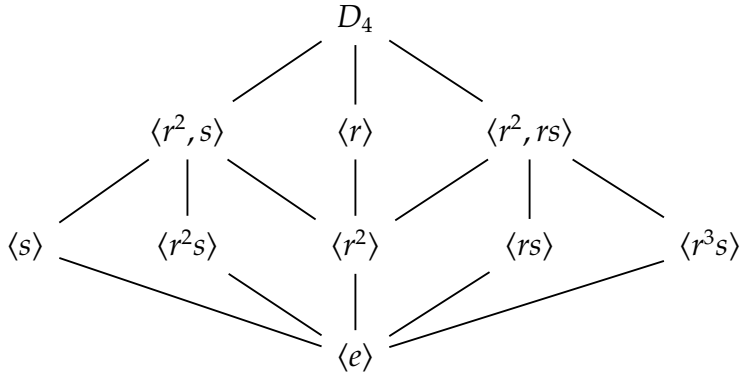
We abstract away the specific value of the root by letting $\alpha = \sqrt{2 + \sqrt{5}}$. Then the other roots are $-\alpha, i\alpha^{-1}$ and $-i\alpha^{-1}$ by our above calculation. Thus the splitting field is just $\mathbb{Q}(\alpha, i)$. Clearly $|\mathbb{Q}(i)/\mathbb{Q}| = 2$, and since we showed irreducibility, we also have $|\mathbb{Q}(\alpha)/\mathbb{Q}| = 4$. Since $i \notin \mathbb{Q}(\alpha)$, and $x^2 + 1 = 0$ is a polynomial of degree 2 that has i as a root over $\mathbb{Q}(\alpha)$, it must be that $|\mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)| = 2$. We have the following diagram:



In particular, letting $G = \mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$, $|G| = 8$. Define the following maps:

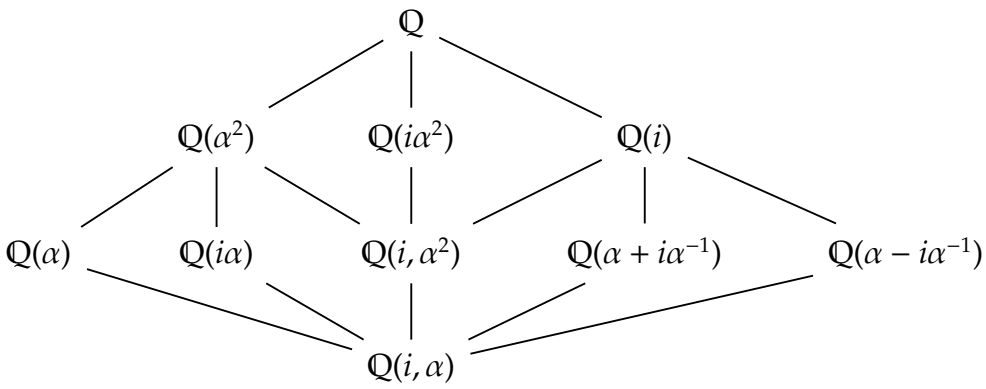
$$\gamma : i \mapsto -i$$
$$\sigma : \alpha \to -\alpha$$
$$\varphi : \alpha \mapsto i\alpha^{-1}$$
$$\tau : \alpha \mapsto -i\alpha^{-1}$$

Clearly γ, σ have order 2, and $\varphi^{(2)}(\alpha) = \varphi(i\alpha^{-1}) = i\varphi(\alpha)^{-1} = ii^{-1}\alpha = \alpha$, so φ has order 2 and similarly τ has order 2. Notice that $\gamma\varphi\gamma^{-1}(\alpha) = \gamma(i\alpha^{-1}) = -i\alpha^{-1}$. Thus, G is nonabelian. Hence G is either Q_8 or D_4. We see that $(\varphi\gamma)^{(2)}(\alpha) = (\varphi\gamma)(i\alpha^{-1}) = -i\varphi(\alpha)^{-1} = -\alpha$, so in particular $\varphi\gamma$ has order 4. Similarly, $\tau\gamma$ has order 4. Thus our group has precisely 2 elements of order 4: $\varphi\gamma$ and $\tau\gamma$, 5 elements of order 2: $\gamma, \sigma, \varphi, \tau, \sigma\gamma$, and one element of order 1: e. Q_8 has 6 elements of order 4, thus we have determined that $G = D_4$. Identifying $\varphi\gamma$ with r, and γ with s, we have the following lattice:



The reader can clearly see that under the identification above, $\sigma = r^2$, $\varphi = rs$, $\tau = sr = r^3 s$, and thus $\sigma\gamma = r^2 s$, and finally $\tau\gamma = r^3$. This identification and some (omitted) calculations

yields the following lattice:

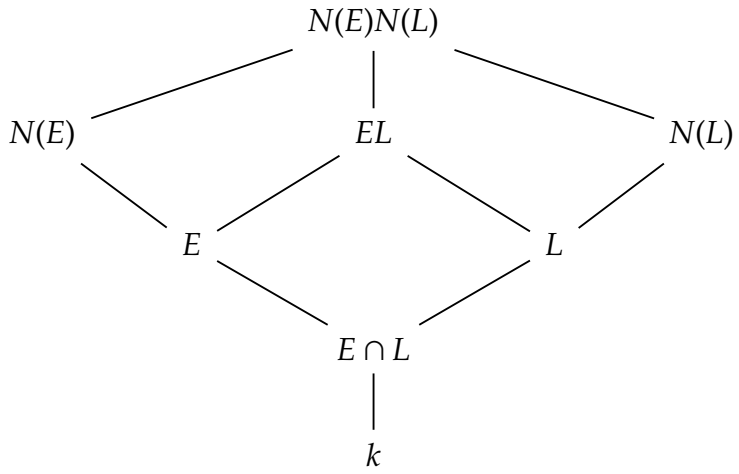


We shall go over only the nontrivial ones for completness. The ones I found difficult were finding the fixed field of $\langle rs \rangle$, $\langle r^2 s \rangle$ and $\langle r^3 s \rangle$. Recall that $\varphi = rs$. The technique I had in mind is to build the middle field from the two side fields–importantly, noticing that $\varphi(i\alpha^{-1}) = \alpha$, and since φ has order 2, we have that $\varphi(\alpha + i\alpha^{-1}) = i\alpha^{-1} + \alpha$. Now we need to argue this extension has degree 4 over $\mathbb{Q}$. Since it is fixed by φ, it must either contain or be contained in $\mathbb{Q}(i)$ by Galois correspondence. Since it is clearly not contained in $\mathbb{Q}(i)$ (by matching real and imaginary parts), it must be that it contains it (strictly), which shows it has dimension 4. The same argument applies for $\langle r^3 s \rangle$. The intuition about the fixed field of $\langle rs \rangle$ is noticing that a field that contains α would be a square root of α–but we already used one so let's use the other.

To go one step further, the author conjectures that replacing the -4 in our polynomial with any other number congruent to 2 mod 3 would yield the same Galois group via the same arguments (in particular, the irreducibility argument would still work). In particular, given any $a \equiv 2 \bmod 3$, $g_a(x) = x^4 + ax^2 - 1$ would yield the same Galois group with a similar picture once the correct α has been picked (namely, the positive real one). Perhaps $g_a(x)$ being irreducible is even sufficient for $a \equiv 2 \bmod 3$, which would give quite the incredible divisibility rule.

2. We first prove extension of scalars. Let E, L sit inside some algebraic closure of k and denote the normal closure of E as $N(E)$ (the intersection of all normal extensions of E). We

then have the following diagram:



Since $N(E)$ is the splitting field of some polynomial f, and $N(L)$ is the splitting field of some polynomial g, we see clearly that $N(E)N(L)$ is the splitting field of fg, thus $N(E)N(L)$ is Galois over EL. But why does a field extension of L that is normal over k exist? Since L is finite, we can take elements $\alpha_1, \ldots, \alpha_n$ that generate it, then just take the splitting field over the product of the minimal polynomials of each α_i. Notice finally that $N(E)N(L)/N(L)$ is separable since separable extensions form a distinguished class. Thus $N(E)N(L)/N(L)$ is Galois, so we may reduce to the case where E, L are normal over k. In that case,

$$\mathrm{Gal}(EL/L) \cong \mathrm{Gal}(E/E \cap L) \trianglelefteq \mathrm{Gal}(E/k)$$

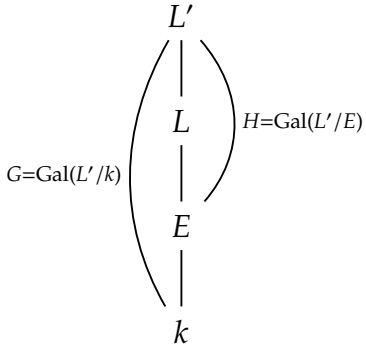
Where the last inclusion is by Galois correspondence (notably it is a normal subgroup since the intersection of two normal extensions is also normal). Since $\mathrm{Gal}(E/k)$ is solvable, and since normal subgroups of solvable groups are solvable, $\mathrm{Gal}(E/E \cap L)$ is solvable, and thus so is $\mathrm{Gal}(EL/L)$.

We prove the more general result that any subgroup of a solvable group is solvable. Let G be a solvable group and $H \leq G$. By solvability, the derived series terminates at $\langle e \rangle$, i.e.

$$G \trianglerighteq [G, G] = G^{(1)} \trianglerighteq [G^{(1)}, G^{(1)}] = G^{(2)} \trianglerighteq \cdots \trianglerighteq \langle e \rangle$$

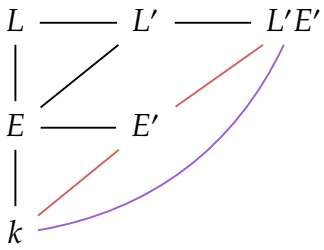
Clearly, $[H, H] \leq [G, G]$ since $H \leq G$. By applying this fact inductively, we can see that $H^{(i)} \leq G^{(i)}$. Thus, since G's derived series terminates, we have that H's does too. Let $L/E/k$ be a tower of extensions, and assume that L is solvable. Then there exists an extension L'

of L such that L'/k is solvable. Pictorially,



Since $H \leq G$, by the previous lemma H is solvable. Since $E \subset L'$ and $\mathrm{Gal}(L'/k)$ is solvable, taking $E = L'$ in our definition of a solvable field extension shows that E/k is solvable.

The converse is, morally speaking, citing the forward direction twice and a picture. Let $L/E/k$ be a tower of extensions such that L/E is solvable and E/k is solvable. Let L' be the field extension of L such that $\mathrm{Gal}(L'/E)$ is solvable and E' defined similarly. We then have the following diagram:



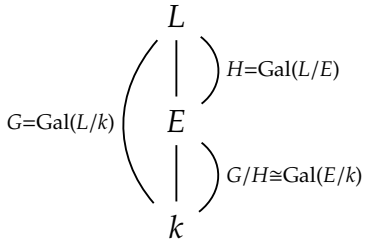
We claim that $L'E'$ is Galois over k. Since E'/k is separable, E/k is separable. Since separable extensions form a distinguished class, and since L'/E is separable (since L/E and E/k are separable), $L'E'/E'$ is separable. This tells us that $L'E'/k$ is separable. Let $\sigma : L'E' \to \overline{k} = \overline{E}$ be an embedding into the algebraic closure of k. Clearly,

$$\sigma(l'e') = \sigma(l')\sigma(e')$$

Since L'/E is normal, L' will get mapped to itself under any embedding of L' into $\overline{E} = \overline{k}$, thus $\sigma(l') \in L'$. Similarly, $\sigma(e') \in E'$, Thus $\sigma(L'E') = L'E'$, which shows normality. Since L'/E is solvable, by extension of scalars $L'E'/E'$ is solvable too. Clearly $L'E'/E'$ is Galois, so by the forward direction, $L'E'/E'$ is solvable.

We have shown the red path in the above diagram is a tower of solvable Galois extensions,

thus we can reduce to the case where L and E are Galois. We draw the final diagram:



Our hypothesis is that H and G/H are solvable, which shows that G is solvable.

3. (1)

Lemma 1. *Let $f(x) \in k[x]$ be inseparable and irreducible. Then there exists an irreducible separable polynomial $g(x) \in k[x]$ and $k > 0$ so that $f(x) = g(x^{p^k})$.*

Proof. By induction. Clearly the theorem is true for monic polynomials. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be as above. Let $d(x) = \gcd(f(x), f'(x))$ (where d is monic). If $f'(x) \not\equiv 0$, $d(x) \equiv 1$, otherwise $d(x) \mid f(x)$ but $f(x)$ is irreducible. Then by Bezout, there are $a(x), b(x)$ such that

$$a(x)f(x) + b(x)f'(x) = 1$$

Since $f(x)$ has a repeat root α, we could plug α into the above equation to get that $0 = 1$, a contradiction. Thus $f' \equiv 0$. Now let $1 \leq i \leq n$. It follows that $ia_i = 0$ in k. If $a_i \neq 0$, we have that $i \cdot 1 = 0$ so $p \mid i$. Thus p divides the power of term in $f(x)$, so we can write

$$f(x) = \sum_{i=0}^{n/p} a_i x^{pi}$$

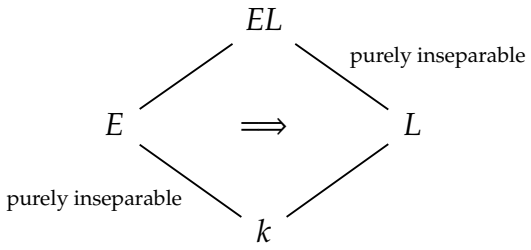
Taking $g(x) = \sum_{i=0}^{n/p} a_i x^i$ yields $f(x) = g(x^p)$. If g is separable we are done, otherwise we must show that g is irreducible to complete the inductive step. If g had a reduction $g(x) = h(x)k(x)$, then $f(x) = h(x^p)k(x^p)$ would be a reduction of f, which cannot be. □

Now let $\alpha \in K \setminus k$ and $f(x) = \mathrm{Irr}_k(\alpha)$. Find $g(x) \in k[x], k > 0$ as per the previous lemma. We claim, of course, that $\alpha^{p^k} \in k$. By construction $g(\alpha^{p^k}) = f(\alpha) = 0$. Thus α^{p^k} is the root of an irreducible separable polynomial, and since K is purely inseparable, this forces $\alpha^{p^k} \in k$.

(2) Let $k(\alpha)/k$ be a simple purely inseparable extension with $\alpha \notin k$. Via part (1), there

exists $n > 0$ so that $\alpha^{p^n} \in k$ and $f(x)$ so that $\mathrm{Irr}_k(\alpha) = f(x^{p^n})$. We claim that f is linear. Indeed, if $f(x) = g(x)h(x)$ was a reduction of g, then $f(x^{p^n}) = g(x^{p^n})h(x^{p^n})$ would be a reduction of $\mathrm{Irr}_k(\alpha)$, so f is irreducible. It follows then that $(x - \alpha^{p^n}) \mid f$. The only way that f could be irreducible then is if $f(x) = x - \alpha^{p^n}$ (note that f is monic). From here we see that $\mathrm{Irr}_\alpha(k) = x^{p^n} - \alpha^{p^n}$, thus $|k(\alpha) : k| = p^n$.

We now claim the following.



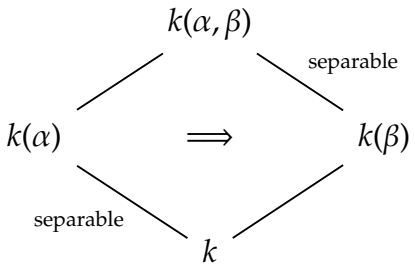
Let $\alpha \in EL \setminus L$, let $q(x) = \mathrm{Irr}_L(\alpha)$, and finally $p(x) = \mathrm{Irr}_k(\alpha)$. First we claim that $q(x) \mid p(x)$ in $L[x]$. Let $d(x) = \gcd(p(x), q(x))$. Clearly $d(x) \neq 1$, otherwise we could find $a(x), b(x)$ so that $a(x)p(x) + b(x)q(x) = 1$ but plugging α in shows that $0 = 1$, a contradiction. Thus, $d(x) = q(x)$ as the only divisors of $q(x)$ are 1 and associates of $q(x)$. Since $\alpha \notin k$, the previous paragraph shows that $p(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$ for some $n \geq 1$. Thus $q(x)$ is of the form $(x - \alpha)^{p^m}$ for some $m \leq n$. m cannot be 0, as this would say that $\alpha \in L$. Hence $q(x)$ is inseparable, which completes the proof of the claim. We now complete the proof by induction. Let $K = k(\alpha_1, \ldots, \alpha_n)$. Then $|K : k| = |k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : k(\alpha_1, \ldots, \alpha_{n-1})| \cdot |k(\alpha_1, \ldots, \alpha_{n-1}) : k|$. By the previous paragraph $K/k(\alpha_1, \ldots, \alpha_{n-1})$ is a simple inseparable extension, thus has order p^m for some m. By induction the right hand side does too, thus $|K : k|$ is a power of p, completing the proof.

(3) Let

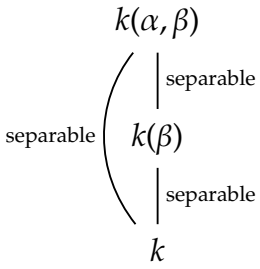
$$E = \{\, x \in k \mid x \text{ separable over } k \,\}$$

We need to show that E is indeed a field. Let $\alpha, \beta \in E$.

Since separable extensions form a distinguished class,



Which tells us that,



So $k(\alpha,\beta)/k$ is a separable extension. Thus $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta$, and α/β are separable over k, so E is indeed a field (note that E is nonempty since $0 \in E$). By construction every element of E is separable thus E/k is a separable extension. Now let $\alpha \in E$. Carefully considering the claims proven in part (2), all we need to conclude that α is inseparable over E is that α is inseparable over k, thus K/E is purely inseparable.

Now we prove that $|K:E| = |K:k|_{\text{sep}}$. Recall that

$$|K:k|_{\text{sep}} = |\Sigma_{\text{id}}(K/k)| = \left|\left\{\, \sigma : K \to \overline{k} \;\middle|\; \sigma|_k = \text{id}_k \,\right\}\right|$$

We can obviously define a surjection from $\Sigma_{\text{id}}(K/k)$ to $\Sigma_{\text{id}}(E/k)$ by $\sigma \mapsto \sigma|_E$. We claim that we can extend a $\sigma \in \Sigma_{\text{id}}(E/k)$ uniquely to a $\tilde{\sigma} \in \Sigma_{\text{id}}(K/k)$. Let $\alpha \in K \setminus E$. Once again the minimal polynomial of α over k is of the form $x^{p^n} - \alpha^{p^n} = (x-\alpha)^{p^n}$. Since $\tilde{\sigma}$ (any extension of σ) must send α to another root of its minimal polynomial over k, we can see clearly that α must be sent to α, as it's minimal polynomial has no other roots. Thus $|K:k|_{\text{sep}} = |E:k|_{\text{sep}} = |E:k|$, completing this step. For the sake of completness the author notes that this argument is more general as it also yields an equality for extensions of infinite degree.

Finally, we have the equality $|K:k| = |K:E|\cdot|E:k| = |K:E|\cdot|K:k|_{\text{sep}}$ by the previous paragraph. Since K/E is a purely inseparable finite extension, $|K:E| = p^n$ for some n. Thus $|K:k| = p^n|K:k|_{\text{sep}}$ as required.