MATH 200B WINTER 2021 FINAL –WITH SELECTED SOLUTIONS

1. Let F be a field. Let $A \in M_n(F)$. Let $f = \text{minpoly}_F(A) \in F[x]$.

(a). Let $\overline{F}$ be the algebraic closure of F. Show that $\text{minpoly}_{\overline{F}}(A) = f$.

(b). Show that A is diagonalizable over $\overline{F}$ (that is, A is similar in $M_n(\overline{F})$ to a diagonal matrix) if and only if f is a separable polynomial.

(c). Let $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \in M_3(F)$. Is A diagonalizable over $\overline{F}$? The answer may depend on the properties of F.

Most students did well on this problem. For those that missed part (a), the key is to use that the minpoly is the largest invariant factor, and that invariant factors are unchanged by base field extension (since the rational canonical form must be the same regardless of the field). There is no obvious way to part (a) directly.

2. Let $F \subseteq K$ be a field extension with $[K : F] < \infty$. In this problem, if you find any results from homework problems helpful you can quote them here rather than redoing them. Note that a commutative ring R is called *reduced* if R has no nonzero nilpotent elements.

(a). Suppose that K/F is separable. Prove that the K-algebra $K \otimes_F K$ is reduced, but is not a domain unless $K = F$.

(b). Suppose that K/F is inseparable. Show that the K-algebra $K \otimes_F K$ is not reduced.

Proof. (a). Since K/F is separable, $K = F(\alpha)$ for some $\alpha \in K$, by the theorem of the primitive element. Now we use the result from problem 2 from homework #6. We have $F(\alpha) \cong F[x]/(f)$ where $f = \text{minpoly}_F(\alpha)$. Then $K \otimes_F K \cong K[x]/(f)$ by that problem.

In the special case that $K = F$, of course $K \otimes_F K = F \otimes_F F \cong F$ is a field, and so a domain. Now assume that $K \neq F$, so $\deg f = [K : F] \geq 2$. Now f is irreducible over F, but it is certainly not irreducible over K, as we know that $\alpha \in K$ is a root of f, so that $(x - \alpha)$ is an irreducible factor of f. The rest of the factorization of f into irreducibles in $K[x]$ is unknown, so let us write $f = g_1 g_2 g_3 \dots g_k$ where each g_i is monic and irreducible in $K[x]$. If two of the g_i are associates (and thus scalar multiples), then they will be equal since they are monic. Then f will have multiple roots in a splitting field, which is not the

Date: March 19, 2021.

case. Thus the g_i are pairwise non-associate, and thus generate distinct maximal ideals. This means that the ideals (g_i) are pairwise comaximal. By the Chinese Remainder Theorem, $F[x]/(f) \cong F[x]/(g_1) \times \cdots \times F[x]/(g_k)$. Each $F[x]/(g_i)$ is a factor by a maximal ideal and so is a field K_i. We conclude that $K \otimes K \cong K_1 \times K_2 \times \ldots K_m$ is a product of fields. But it is easy to see that a product of fields has no nilpotents. But since f has at least two irreducible factors in this case where we are assuming that $K \neq F$, then $k \geq 2$ and so as a product of two or more rings $K \otimes K$ cannot be a domain.

Many students did not think about using the Chinese Remainder Theorem and tried to argue the lack of nilpotents directly. This works but some care is required. If $0 \neq h + (f)$ is a nonzero nilpotent element of $K[x]/(f)$, then $(h + (f))^n = h^n + (f) = 0 + (f)$ for some $n \geq 2$ (we cannot have $n = 1$, as then $h + (f) = 0$). Thus $h^n = fg$ for some $g \in K[x]$. The question now is how to use that f is separable. Following the same argument as above, we can write $f = g_1 g_2 \ldots g_k$ where the g_i are monic irreducible, and f separable forces the g_i to be pairwise non-associate. This means that each g_i divides h^n, and since g_i is irreducible, g_i divides h by unique factorization. But then $f = g_1 g_2 \ldots g_k$ divides h, again by unique factorization, and this is a contradiction to $h + (f) \neq 0$. It is also possible to pass to a splitting field L, where f factors as a product of distinct linear factors, and do the same argument there to prove that f divides h in the splitting field, and then noticing that since $f, h \in K[x]$, if $f|h$ in $L[x]$ then $f|h$ in $K[x]$ by the uniqueness in polynomial division with remainder. I think going to the splitting field just makes things more complicated in this case.

(b). Since K/F is not separable, we can find $\alpha \in K$ such that $f = \text{minpoly}_F(\alpha)$ is not separable. Now $F \subseteq F(\alpha) \subseteq K$ and since we are tensoring over a field F, the tensor product $F(\alpha) \otimes_F F(\alpha)$ is naturally a subring of $K \otimes_F K$, as one can see by choosing bases over F. It suffices to show that $F(\alpha) \otimes_F F(\alpha)$ has nonzero nilpotents.

Let $E = F(\alpha)$. Now similar to above, $E \otimes_F E \cong E[x]/(f)$. In this case, because f is not separable, when we factor it into monic irreducibles in $E[x]$, we get $f = g_1^{e_1} \ldots g_k^{e_k}$ where the g_i are distinct but where at least one $e_i \geq 1$. This is because two different monic irreducibles cannot have a common root (else both would be the minimal polynomial for that root). Without loss of generality, suppose that $e_1 \geq 2$. Again using the chinese remainder theorem we have $E[x]/(f) \cong E[x]/(g_1^{e_1}) \times \cdots \times E[x]/(g_k^{e_k})$. But now $E[x]/(g_1^{e_1})$ has a nonzero nilpotent element $g_1 + (g_1^{e_1})$, which is nonzero because $e_1 \geq 2$. Then $(g_1, 0, \ldots, 0)$ is a nonzero nilpotent element of the product.

We can avoid the Chinese remainder theorem here as well if we wish— one can prove directly that $g_1 g_2^{e_2} \ldots g_k^{e_k} + (f)$ is nilpotent and nonzero in $E[x]/(f)$.

□

3. Let $f(x) = x^{12} - 3 \in \mathbb{Q}[x]$. Let K be the splitting field of f over $\mathbb{Q}$.

(a). Show that $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to D_{24}, a dihedral group of order 24. (Hint: a primitive 12th root of 1 is given by $e^{2\pi i/12} = \cos(\pi/6) + i\sin(\pi/6)$.)

(b). Let Z be the center of G. Let $E = \mathrm{Fix}(Z)$. Show that E is a splitting field over $\mathbb{Q}$ of some polynomial $g \in \mathbb{Q}[x]$. Find such a g.

Solution:

This problem had an unfortunate error—the Galois group is not D_{24} as claimed. Many of the students on the exam gave in fact the same (incorrect) solution I had in mind when I wrote the problem. I graded the solutions only on whether they correctly proved that the extension $K/\mathbb{Q}$ had degree 24; that 24 automorphisms were written down and justified why these were automorphisms; and that a reasonable attempt was made in part (b), in particular showing that D_{24} has center of order 2 and/or justifying that $\mathrm{Fix}(Z)/Q$ would be Galois (normal) by the fundamental theorem. Since the group is not D_{24} I couldn't grade part (b) too closely.

Let K be the splitting field of $f = x^{12} - 3$ over $\mathbb{Q}$. Let $\alpha = \sqrt[12]{3}$ be the positive real 12th root of 3, and let $\zeta = e^{2\pi i/12}$ be a primitive 12th root of 1. Now $\zeta = (\cos\pi/6) + i(\sin\pi/6) = \sqrt{3}/2 + (1/2)i$. Thus $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt{3}, i)$. On the the other hand, $\sqrt{3} = \zeta + \overline{\zeta} = \zeta + \zeta^{-1}$ and $i = \zeta + \zeta^5$ are both in $\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{3}, i)$.

Similar to other examples of these type we did in class and in the notes, the roots of f in $\mathbb{C}$ are $\{\alpha, \alpha\zeta, \ldots \alpha\zeta^{11}\}$ and so $K = \mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\sqrt[12]{3}, \sqrt{3}, i) = \mathbb{Q}(\sqrt[12]{3}, i)$ since $\sqrt{3} = \sqrt[12]{3}^6$ is already contained in the field generated by $\sqrt[12]{3}$. Now f is irreducible over $\mathbb{Q}$ by the Eisenstein criterion applied with the prime 3. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 12$. Since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, clearly $i \notin \mathbb{Q}(\alpha)$; also i satisfies $x^2 + 1 \in \mathbb{Q}[x]$. This forces $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ and hence $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 24$. Since K is the splitting field of a separable polynomial f over $\mathbb{Q}$, $K/\mathbb{Q}$ is Galois. So $|\mathrm{Gal}(K/\mathbb{Q})| = 24$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$.

If $\sigma \in G$, then $\sigma(\alpha)$ is another root of $x^{12} - 3$ and $\sigma(i)$ is another root of $x^2 + 1$. There are 12 choices in the first case and 2 in the second, so 24 choices total. On the other hand, an element in G is determined by its action on α and i and $|G| = 24$. It follows that all choices occur.

It is important to realize that some argument has to be made here. Given a Galois extension $F(\alpha_1, \ldots, \alpha_m)$, each element of the Galois group must send each α_i to another root of $f_i = \mathrm{minpoly}_F(\alpha_i)$. Also, if we fix i, then there exists some automorphism which sends α_i to any other root of f_i we please (and does something unknown to the other α_j); this is what our results on splitting fields said. However, we cannot necessarily find an automorphism which

sends every α_i to any other root of f_i we please, simultaneously for all i at once. The reason is that there may be "hidden relationships" among the elements α_i.

In particular, we can find an automorphism $\sigma \in G$ such that $\sigma(\alpha) = \alpha\zeta$ and $\sigma(i) = i$; and an automorphism $\tau \in G$ such that $\tau(\alpha) = \alpha$ and $\tau(i) = -i$. The place where almost all of you missed a subtlety at this point (and I did too when I was designing the problem!) was to claim that $\sigma(\alpha\zeta^i) = \alpha\zeta^{i+1}$ for all i, and so σ has order 12. The problem is that we have not determined what σ does to ζ, only what it does to i. And in fact σ does not fix ζ. Note that $\sigma(\sqrt{3}) = \sigma(\alpha^6) = \alpha^6\zeta^6 = -\alpha^6 = -\sqrt{3}$. Thus $\sigma(\zeta) = \sigma(\sqrt{3}/2 + (1/2)i) = -\sqrt{3}/2 + (1/2)i = \zeta^5$. Similarly, τ does not fix ζ but rather $\tau(\zeta) = \zeta^{11} = \zeta^{-1}$. In particular this means that $\sigma(\alpha\zeta) = \alpha\zeta^6 = -\alpha$. Using this you can check that $|\sigma| = 4$ and so this σ and τ do not even generate G.

Some students instead attempted to define an automorphism by $\sigma'(\alpha) = \alpha\zeta$, $\sigma'(\zeta) = \zeta$. Such a σ' would satisfy the formula $\sigma'(\alpha\zeta^i) = \alpha\zeta^{i+1}$ for all i, but in fact you can check that no such σ' exists. Here $\deg \operatorname{minpoly}_{\mathbb{Q}}(\zeta) = 4$ *so we run exactly into the problem mentioned above, that we cannot necessarily define an automorphism that moves α and ζ simultaneously to any roots of their minimal polynomials we please, as that would lead to 48 different automorphisms.*

In fact we get a more complicated group of order 24 for G, which has no elements of order 12. For each $0 \leq j \leq 11$ there is an automorphism σ_j such that $\sigma_j(\alpha) = \alpha\zeta^j$ and $\sigma_j(i) = i$. The collection of these, $H = \{\sigma_j | 0 \leq j \leq 11\}$, is clearly a subgroup of G, and in fact must be equal to $\mathrm{Gal}(K/\mathbb{Q}(i))$ since these are 12 automorphisms that fix $\mathbb{Q}(i)$. So which group of order 12 is it? Unfortunately it is the least familiar of the nonabelian groups of order 12, sometimes called T, which can be described as the semidirect product $\mathbb{Z}_3 \rtimes_\psi \mathbb{Z}_4$ where $\psi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) = \mathbb{Z}_3^* \cong \mathbb{Z}_2$ is the only nontrivial homomorphism. (There are only three nonabelian groups of order 12; the others are D_{12} and A_4). The group T also has presentation $\langle a, b | a^4 = 1 = b^3, a^{-1}ba = b^2 \rangle$. We can match up H with this presentation by sending σ_1 to a and σ_4 to b. Now we can calculate that $\tau^{-1}\sigma_j\tau = \sigma_{12-j}$. Thus G can be described as a further semidirect product $H \rtimes_\theta \mathbb{Z}_2$ where $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(H)$ sends the generator to the order 2 automorphism of H given by $b \mapsto b^2$, $a \mapsto ba^3$. So G has presentation $\langle a, b, c | a^4 = b^3 = c^2 = 1, a^{-1}ba = b^2, c^{-1}bc = b^2, c^{-1}ac = ba^3 \rangle$ (if I haven't made a calculation error). I'm not sure if there is a simpler way to describe this group.

(b). It turns out that the answer in part (b) is not affected too much by the error in part (a), and many students' solutions to part (b) were essentially correct as written. One can show that it is still true that the presentation above has a center of order 2, generated by a^2. So the center Z of G is generated by σ_6, which is the automorphism sending α to $-\alpha$ and fixing i (also fixing ζ). So this fixes α^2. Thus $\mathbb{Q}(\alpha^2, i) \subseteq \mathrm{Fix}(Z)$. Since α^2 is a root of the irreducible polynomial $x^6 - 3$, one shows in a similar way as above that $[\mathbb{Q}(\alpha^2, i) : \mathbb{Q}] = 12$ and thus $E = \mathrm{Fix}(Z) = \mathbb{Q}(\alpha^2, i)$. The fact that $E/\mathbb{Q}$ is Galois comes right from the fundamental

theorem, since Z is a normal subgroup of G. Now one can take $g = x^6 - 3$ and show that E is the splitting field of g over $\mathbb{Q}$, similarly to the way we showed that $K = \mathbb{Q}(\alpha, i)$ is the splitting field of $x^{12} - 3$ over $\mathbb{Q}$. Other g's are possible of course.