Algebra II Homework 8 Commentary

Zachary Gardner

Unless otherwise stated, k denotes a field and Fr the Frobenius map on k (which is defined if k has prime characteristic $p > 0$).

General Commentary

- Given a polynomial $f(x) \in k[x]$ and a field extension L/k in which $f(x)$ splits, if we know all of the roots of $f(x)$ in L (including their multiplicities) then we **almost** know $f(x)$. The issue is that $f(x)$ may not be monic and so we may need to multiply by some nonzero scalar. This matters, for instance, when trying to say two polynomials are equal. Namely, if two polynomials each divide the other then we can only be certain they are the same if both polynomials are monic.
- It's true that being separable means having no repeated roots, but it's important to note where these roots live. As an extreme example, irreducible polynomials over perfect fields are separable but also obviously have no roots at all over the ground field (since otherwise they would be reducible).
- Be careful that polynomials in $\mathbb{F}_p[x]$ and the functions $\mathbb{F}_p \to \mathbb{F}_p$ they induce are not one and the same thing. In particular, there are plenty of nonzero polynomials that vanish at every point of $\mathbb{F}_p$ upon evaluating. In fact, all such polynomials are multiples of $x^p - 1$.

Problem 1

Part (a)

- Remember that if and only if two statements have two directions. Some people only proved one direction.
- This is a comment for people who prefer to think of separability in terms of having no repeated roots. In the case that $p \nmid n$, how do you know that $x^n - 1$ will not have some "non-obvious" factorization in $\mathbb{F}_p[x]$?
- Note that the roots of the polynomial $x^n - 1 \in \mathbb{F}_p[x]$ need not be contained in $\mathbb{F}_p$. Note also that $x^n - 1$ need not have n distinct roots – indeed, this problem shows that holds if and only if $p \nmid n$. In the case $p \mid n$, how many distinct roots does $x^n - 1$ have?

Part (b)

- If a polynomial $g(x) \in \mathbb{Q}[x]$ is reducible over $\mathbb{Q}(\zeta_3)$ then it is not necessarily true that x^2+x+1 (the minimal polynomial of ζ_3 over $\mathbb{Q}$) divides $g(x)$. For instance, consider $x^2 - x + 1$, which is the minimal polynomial of $\zeta_3 + 1$ over $\mathbb{Q}$.

- Let α be a root of $f(x)$ (which lives in some field extension of $\mathbb{Q}$). Some work is needed to see why $\mathbb{Q}(\alpha, \zeta_3)$ has degree 6 over $\mathbb{Q}$ (namely, the result of this problem). By the same token, the minimal polynomial of α over $\mathbb{Q}(\zeta_3)$ cannot just be assumed to have degree 3 since this is equivalent to the statement of the problem.
- One way to view this problem is in terms of the extremely useful trick of exchanging the order of quotients. We are given $f(x) \in \mathbb{Q}[x]$ irreducible of degree 3. Letting α be as above, the field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$ is a degree 3 extension of $\mathbb{Q}$. At the same time, $\mathbb{Q}(\zeta_3) \cong \mathbb{Q}[y]/(y^2+y+1)$ is a degree 2 extension of $\mathbb{Q}$. We then have

$$\begin{aligned}\mathbb{Q}(\zeta_3)[x]/(f(x)) &\cong (\mathbb{Q}[y]/(y^2+y+1))[x]/(f(x)) \\ &\cong (\mathbb{Q}[x]/(f(x)))[y]/(y^2+y+1) \\ &\cong \mathbb{Q}(\alpha)[y]/(y^2+y+1)\end{aligned}$$

  upon switching the order of the quotients.[1] If we call all of these fields L (which we can do since they are all isomorphic) then we see that L contains (copies of) both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta_3)$. Thus, $[L : \mathbb{Q}]$ is divisible by both $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ hence divisible by 6 since $\gcd(2, 3) = 1$. This shows that L is "bigger than" both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta_3)$. Hence, $f(x)$ is irreducible over $\mathbb{Q}(\zeta_3)$ (and, as a bonus, $y^2 + y + 1$ is also irreducible over $\mathbb{Q}(\alpha)$).

Parts (c)-(e)

- For part (c), be careful that $\mathbb{F}_9$ is not the same ring as $\mathbb{Z}/9\mathbb{Z}$. In particular, writing things like 4 and 7 for elements of $\mathbb{F}_9$ doesn't make sense.
- For part (d), several people tried to do this by arguing in terms of gcd. Remember that before you can say anything about gcd you need to know something about dividing polynomials. The argument some people had in mind relies on knowing the result of this problem to work (which is an issue because of circular reasoning).
- For part (d), don't confuse this statement with that of Gauss's Lemma (which is a much stronger result).
- For part (e), simply stating the definition of Galois (in terms of automorphisms) did not get any points for justification. The same goes for any equivalent definition of Galois.

Problem 2

- This doesn't need to be done by contradiction since all of the proofs I know of are directly constructive.
- Let $f(x) \in k[x]$ be separable and $g(x)$ be a monic factor. What you should do here is pass to a field over which $f(x)$ splits completely. Then, $g(x)$ must also split completely since it is a factor of $f(x)$. Finally, $g(x)$ must have no repeated roots (hence be separable) since $f(x)$ has no repeated roots (since it is separable).
- Continuing with the above comment, if you first try to work with a field over which $g(x)$ splits and then pass to some possibly larger field for accommodate $f(x)$ then you will have to

[1] Note that we can also write these double quotients in terms of a single quotient, namely $\mathbb{Q}[x, y]/(f(x), y^2+y+1)$.

deal with compatibility issues. This illustrates one key difference between the "bottom-up" and "top-down" approaches to field extensions that I described on a previous homework.

- There is a difference between a splitting field for $f(x)$ and a field over which $f(x)$ splits since the former is minimal in a precise sense.

Problem 3

- Since the things here are just sets (without extra structure) the word bijection should be probably be used in place of isomorphism.
- I was looking for people to explicitly state that there is a bijective correspondence between $\mathrm{Emb}_k(k[x]/(f(x)), L)$ and the set of roots of $f(x)$ in L. Note that the result of Homework 7 Problem 7(a) being used here is only stated for monogenic (also called primitive) extensions. This is why it is extremely important that $f(x)$ is irreducible.

Problem 4

Most of the comments for this problem have to do with (a) $\implies$ (b), so let me first briefly state the remainder of the comments.

- For (b) $\implies$ (a), don't forget the $g'(x)$ part of the chain rule computation.
- Many people forgot to do the very last part of the problem.

Now to discuss (a) $\implies$ (b). For convenience, let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$.

- Many people correctly stated that $f'(x) = na_n x^{n-1} + \cdots + a_1$ and then used the fact that $f'(x) = 0$ to deduce that $ia_i = 0$ for each $1 \leq i \leq n$. However, this is where some people then went astray. What this equation tells us is that either $p \mid i$ or $a_i = 0$ for each i. This is not something uniform in i in the sense that which one of these two statements is true depends on the value of i. In the case that $p \nmid i$ we can cancel the i from ia_i to deduce that $a_i = 0$. So, all of the coefficients of $f(x)$ whose index is not divisible by p must vanish. In the case that $p \mid i$ we automatically have $ia_i = 0$ and so a_i can be arbitrary.
- Another common mistake I saw was claiming that Fr will be the identity on k. The fact that k is perfect means only that Fr is an automorphism. In fact, Fr is the identity map if and only if $k = \mathbb{F}_p$ (in characteristic p, anyway). Even for a perfect field as simple as $\mathbb{F}_{p^2}$ the map Fr will act in a nontrivial way. You can figure out what this looks like explicitly by writing $\mathbb{F}_{p^2}$ as the quotient of $\mathbb{F}_p[x]$ by an irreducible quadratic.
- Note that $f'(x) = 0$ tells us nothing about the constant term a_0. This is not a problem since we can still write $a_0 = b_0^p$ for some $b_0 \in \mathbb{F}_p$.

Problem 5

- Since this problem asks for separable minimal polynomials, you need to offer some explanation for why the proposed minimal polynomials are separable. In particular, you need to say that irreducible polyonomials over $\mathbb{F}_3$ are automatically separable (since $\mathbb{F}_3$ is perfect).

- Most people failed to give a line of explanation for why $\min_A(x)$ cannot just be an irreducible quadratic. Perhaps it was too harsh of me to expect this.
- Remember that conjugacy classes are uniquely and completely represented by matrices in rational canonical form, which generally have more than one invariant factor. Writing down just the minimal or characteristic polynomial is in general not enough information to determine a class.
- Did you know there is a relatively quick and painless formula to compute the number of irreducible monics of a given degree in $\mathbb{F}_p[x]$? If you've never heard of Móbius inversion then you should check it out. If you're really looking for a challenge then you should check out the Möbius function ring.

Problem 6

- Many people failed to check the necessary hypotheses of Gauss's Lemma. In particular, Gauss's Lemma only applies once you know that $f(x)$ and $g(x)$ are both monic (which many people neglected to justify or even state).
- The polynomial $\Phi_n(x)$ only looks "nice" for n relatively simple (e.g., for n prime). In particular, it is **not** true that $\Phi_n(x) = (x^n - 1)/(x - 1)$ for general n. As an illustration of the fact that $\Phi_n(x)$ can be complicated (and perhaps going against what you might expect), $\Phi_n(x)$ need not always have coefficients $0, \pm 1$. Can you find the smallest n that verifies this?

Problem 7

The crux of this problem is that factorizations in $\mathbb{Z}[x]$ give rise to factorizations in $\mathbb{F}_p[x]$. It is somewhat miraculous that $\Phi_n(x) \in \mathbb{Z}[x]$ since it is defined in terms of a big product of complex numbers. Being able to convert information in $\mathbb{Z}$ to information "mod p" is a powerful tool.