Math 5320: Bonus Problem Set

This set of problems is meant to help you with final exam prep and is mostly focused on the material we covered in the last part of the course, after the last midterm (although the exam itself will be comprehensive).

If you would like to turn in a set of solutions to these, it is due at the start of the final exam, which is Monday April 30 at 1 pm. This is totally optional. If your grade on this write-up is higher than any of your homework grades, it will replace your lowest homework grade.

1. Let R be a ring and consider the ideal (x) of $R[x]$. The ideal (x) has a natural R-module structure. Find a generating set for (x) as an R-module. Find a generating set for (x) as an $R[x]$-module. Why can you choose them to be different from one another? What is a generating set for (x) as an ideal of $R[x]$? How does it compare with the other generating sets you've found?

2. Let R be a ring and let M and N be R-modules.

   (a) Suppose that M is finitely generated and there is an R-module surjection $\varphi : M \to N$. Show that N is finitely generated.

   (b) Let $R^{\oplus n}$ be the free R-module given by the direct sum of n copies of R. Let $e_1, \dots e_n$ be the standard "basis" of $R^{\oplus n}$. Show that for any choice of n elements $\{m_i\}_{i=1}^{n}$ of M there is a unique R-module homomorphism sending e_i to m_i. (Does this result remind you of another result we proved about polynomial rings?)

3. Let p be a prime and $n \in \mathbb{N}$. At the end of the last lecture, we discussed how to show that there is a unique (up to isomorphism) field with p^n elements. Finish the proof: Let K be a splitting field for the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Show that the set of roots of $x^{p^n} - x$ inside K has p^n distinct elements and includes the elements of $\mathbb{F}_p$ and show they are a subfield of K (and hence all of K). Therefore, K is the field we're looking for.

4. Show that $\mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^r}$ if and only if $k|r$.

Here's some exposition to help us do the last few problems and complete our picture of finite fields (don't worry I won't make you read such long paragraphs on the exam!).

Theorem 0.1. *Let $\mathbb{F}$ be a finite field. Then its group of units $\mathbb{F}^\times$ is cyclic.*

Proof. We know $|\mathbb{F}|$ will be some prime power p^n and so $|\mathbb{F}^\times| = p^n - 1$. By the structure theorem for finite abelian groups, we can write $\mathbb{F}^\times$ as a product of cyclic groups of prime-power order. By the Chinese remainder theorem, we can change the way we've written the product of cyclic groups so that $\mathbb{F}^\times \cong C_{d_1} \times \cdots \times C_{d_r}$ where $d_1 | \cdots | d_r$ (e.g. $C_2 \times C_2 \times C_5 \cong C_2 \times C_{10}$). Then, we can see that any element of $\mathbb{F}^\times$ will have order dividing d_r. So, every element of $\mathbb{F}^\times$ must be a root of $x^{d_r} - 1$, but we already know every element of $\mathbb{F}^\times$ is a root of $x^{p^n - 1} - 1$, so $p^n - 1 \leq d_r$. But $|\mathbb{F}^\times| = p^n - 1 = d_1 \cdots d_r$, so $d_r = p^n - 1$ and so the product $C_{d_1} \times \cdots \times C_{d_r}$ must have only one factor, therefore $\mathbb{F}^\times$ is cyclic. □

5. Now let's decide what the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is:

   (a) Why do we know the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois?

   (b) Consider the homomorphism $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ that sends elements to their p-th powers (this is called the Frobenius morphism). Show that φ is an $\mathbb{F}_p$-automorphism and show that it generates $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

   (c) So, what is $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$?

6. Given the previous theorem, why is $\mathbb{F}_{p^n}$ a primitive field extension of $\mathbb{F}_p$?

7. Finally, we will prove that the 17-gon is constructible. Let $\zeta = e^{2\pi i/17}$. By the above theorem and our discussion of primitive roots of unity in class, $G := G(\mathbb{Q}(\zeta)/\mathbb{Q}$ is isomorphic to C_{16}, the cyclic group with 16 elements. One can check (but you are not required to) that the automorphism σ sending ζ to ζ^3 is a generator.

   (a) How many possible intermediate field extensions are there between $\mathbb{Q}(\zeta)$ and $\mathbb{Q}$?

   (b) We decided that an n-gon is constructible if the angle $\frac{2\pi}{n}$ is. Let $\theta = \frac{2\pi}{17}$. Show that $\mathbb{Q}(\cos(\theta)) \subseteq \mathbb{Q}(\zeta)$ is a field extension of degree 2. (Hint: $\zeta + \zeta^{-1} = 2\cos(\theta)$).

   (c) By the last problem, $\mathbb{Q}(\cos(\theta))$ is an intermediate field between $\mathbb{Q}(\zeta)$ and $\mathbb{Q}$. Which subgroup of G is it the fixed field of?

   (d) Using your knowledge of the intermediate field extensions between $\mathbb{Q}(\zeta)$ and $\mathbb{Q}$, show that there is a succession of (real) field extensions of $\mathbb{Q}$ that are degree 2 that ends with $\mathbb{Q}(\cos(\theta))$.

   We know that any degree 2 extension comes from taking a square root, and square roots of constructible numbers are constructible, therefore we've shown that $\cos(\theta)$ is constructible, and hence that the 17-gon is constructible.