Modern Algebra 2: Midterm 2

April 3, 2014

Name: ____

- Write your answers in the space provided. Continue on the back for more space.
- The last three pages are left blank for scratch work. You may detach them.
- Justify your results.
- You may freely use any result from class or homework, but you must state it correctly. Of course, you may not use the same result that you are being asked to prove.
- The last question is an optional bonus question, which you should attempt if you finish everything else and are bored. Its point value is miniscule.
- *Good luck*!

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
6	0	
Total:	50	

1. (10 points) (a) What does it mean for a polynomial $f(x) \in \mathbf{Z}[x]$ to be *primitive*?

Solution: The polynomial $f(x)$ is primitive if the GCD of all the coefficients is 1. Equivalently, $f(x)$ is primitive if no prime p divides all the coefficients of $f(x)$.

(b) Prove *Gauss's lemma*: the product of two primitive polynomials is primitive.

Solution: Let $f(x)$ and $g(x)$ be two primitive polynomials. Let p be any prime. Then their images $\overline{f}(x)$ and $\overline{g}(x)$ in $\mathbf{Z}/p\mathbf{Z}[x]$ are both nonzero. Since $\mathbf{Z}/p\mathbf{Z}$ is a domain, so is $\mathbf{Z}/p\mathbf{Z}[x]$. Therefore, $\overline{f}(x)\overline{g}(x)$ is nonzero. In other words, the image of $f(x)g(x)$ in $\mathbf{Z}/p\mathbf{Z}[x]$ is nonzero. It follows that no prime p divides all the coefficients of $f(x)g(x)$. Hence $f(x)g(x)$ is primitive.

2. (10 points) Let $F \subset K$ be a field extension and let $\alpha, \beta \in K$ be algebraic over F. Show that $\alpha + \beta$ and $\alpha\beta$ are algebraic over F.

Solution: Consider the inclusions

$$F \subset F(\alpha) \subset F(\alpha, \beta).$$

The first extension $F \subset F(\alpha)$ is a finite extension of degree $\deg_F(\alpha)$. The second extension $F(\alpha) \subset F(\alpha, \beta)$ is also a finite extension of degree at most $\deg_F(\beta)$. Therefore, the extension $F \subset F(\alpha, \beta)$ is also finite (of degree at most $\deg_F(\alpha) \deg_F(\beta)$, but that is not relevant.) Since all finite extensions are algebraic, $F \subset F(\alpha, \beta)$ is an algebraic extension. In other words, all elements of $F(\alpha, \beta)$ are algebraic over F. In particular, $\alpha\beta$ and $\alpha + \beta$ are algebraic over F.

3. (10 points) Let p be a prime. Show that the polynomial

$$f(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^p}{p!}$$

is irreducible in $\mathbf{Q}[x]$. For which p is it possible to construct a root of this equation using ruler and compass?

Solution: Since rational numbers are units of $\mathbf{Q}[x]$, the given polynomial is irreducible if and only if $p!$ times it is irreducible. We have

$$p!f(x) = x^p + px^{p-1} + p(p-1)x^{p-2} + \cdots + (p(p-1)\cdots 2)x + (p(p-1)\cdots 1).$$

This is a polynomial where p does not divide the leading coefficients, divides all the other coefficients, and p^2 does not divide the constant term. By Eisenstein's criterion, it is irreducible in $\mathbf{Q}[x]$.

A root of this equation has degree p over $\mathbf{Q}$. Since constructible numbers must have degree 2^n over $\mathbf{Q}$ for some n, a root of $f(x)$ can be constructible only for $p = 2$. (Actually, for $p = 2$, the polynomial does not have real roots.)

4. (10 points) Let $K = \mathbf{F}_2[x]/(x^4 + x + 1)$.

   (a) Verify that K is a field.

Solution: K is a field if and only if $x^4 + x + 1$ is irreducible over $\mathbf{F}_2$. To check this, we simply check that it is not divisible by any irreducible polynomial of lower degree. It suffices to check degree 1 and degree 2 irreducible polynomials. Since neither 0 or 1 is a root of $x^4 + x + 1$, there are no degree 1 factors. The only irreducible polynomial of degree 2 is $x^2 + x + 1$. Since $x^4 + x + 1$ does not have degree 1 factors, if it factors then it must be $(x^2 + x + 1)^2$. But $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1$. Therefore $x^4 + x + 1$ is irreducible.

   (b) Compute the minimal polynomial of $x^2 \in K$ over $\mathbf{F}_2$.

Solution: We must find an irreducible polynomial equation that x^2 satisfies. Let $\alpha = x^2$. From $x^4 + x + 1 = 0$, we get $x^8 = \alpha^4 = (x+1)^2 = x^2 + 1 = \alpha + 1$. Therefore, x^2 satisfies $X^4 + X + 1 = 0$. Since we have already checked that this is an irreducible polynomial, we are done.

In hindsight, you can arrive at the conclusion without doing any calculation. By construction x satisfies $X^4 + X + 1$. The element x^2 is a Frobenius-conjugate of x. Since the elements of an extension field that are Galois conjugates satisfy the same irreducible polynomial over the base field, we conclude that x^2 also satisfies the same polynomial $X^4 + X + 1$.

5. (10 points) Let

$$\alpha = e^{i\pi/4} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}.$$

Show that $\mathbf{Q}(\alpha) = \mathbf{Q}(i, \sqrt{2})$. Using this, or otherwise, show that $x^4 + 1$ is irreducible in $\mathbf{Q}[x]$.

Solution: Evidently, $\mathbf{Q}(\alpha) \subset \mathbf{Q}(i, \sqrt{2})$. For the reverse inclusion, see that

$$\alpha^{-1} = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}.$$

So $\sqrt{2} = \alpha + \alpha^{-1}$ and $\sqrt{2}i = \alpha - \alpha^{-1}$. Therefore, $\sqrt{2} \in \mathbf{Q}(\alpha)$ and $\sqrt{2}i \in \mathbf{Q}(\alpha)$. That is, $\sqrt{2}, i \in \mathbf{Q}(\alpha)$. Therefore, $\mathbf{Q}(\sqrt{2}, i) \subset \mathbf{Q}(\alpha)$. Together with the other inclusion, we conclude that $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha)$.

Notice that we have a chain of inclusions

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\alpha).$$

The first extension has degree 2, since $\sqrt{2}$ satisfies a quadratic equation $x^2 - 2 = 0$ over $\mathbf{Q}$ and does not lie in $\mathbf{Q}$. The second extension also has degree 2, since i satisfies a quadratic equation $x^2 + 1 = 0$ over $\mathbf{Q}(\sqrt{2})$ and does not lie in $\mathbf{Q}(\sqrt{2})$. Therefore, $\mathbf{Q} \subset \mathbf{Q}(\alpha)$ has degree 4. In other words, the minimal polynomial of α has degree 4. But α satisfies $x^4 + 1 = 0$. Hence, $x^4 + 1$ must be the minimal polynomial of α. In particular, $x^4 + 1$ is irreducible.

6. (Bonus, for ϵ points) Show that $x^4 + 1$ is reducible modulo p for every prime p.

Solution: We have

$$\begin{aligned} x^4 + 1 &= x^4 - (-1) \\ &= x^4 + 2x^2 + 1 - 2x^2 \\ &= x^4 - 2x^2 + 1 + 2x^2. \end{aligned}$$

Note that not all of (-1), 2, and -2 can be nonsquares in $\mathbf{F}_p$. Therefore, one of the above expressions factors as a difference of squares.

Scratch work

Scratch work

Scratch work