Mathematics 404 Exam Name: Answers

April 27, 2005

Instructions: This is a closed book exam, no notes or calculators allowed. Justify all of your answers. You may refer to and use any result from the book, homework, or portfolio problems, but for full credit, do not use results from practice problems – if you need one of those results, you should prove it.

This is a timed exam, so you may use abbreviations and symbols (such as "$\forall$"): as long as I can make sense of what you write without struggling too much, it's okay.

1. (10 points) Let $\mathbf{F}_q$ be a field with q elements and fix $n \geq 1$. What is the order of the group $GL_n(\mathbf{F}_q)$? [One of your homework problems asked you to establish a bijection between $GL_n(F)$ and the set of ordered bases of F^n, for any field F. Use that result. You can get some partial credit by answering this question for small values of n.]

Solution: By the homework problem, the order of the group is equal to the number of ordered bases of $(\mathbf{F}_q)^n$. Note that there are q^n vectors in $(\mathbf{F}_q)^n$.

To construct a basis of this space, choose the first vector: this can be any nonzero vector, so there are $q^n - 1$ choices for it. Choose the second vector. This can be anything which is not a scalar multiple of the first one, and there are q scalar multiples of it, so there are $q^n - q$ choices. Continue like this. After having chosen $v_1, v_2, \ldots, v_i$, the basis vector v_{i+1} can be any vector which is not in the span of the first i vectors. The span of the first i vectors is of the form

$$c_1 v_1 + c_2 v_2 + \cdots + c_i v_i$$

where each c_j is an arbitrary element of $\mathbf{F}_q$, and thus this span has q^i elements. So there are $q^n - q^i$ choices for the $(i+1)$st vector. Therefore the total number of bases, which equals the order of $GL_n(\mathbf{F}_q)$ is

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

2. Let p be a prime number and j and k positive integers.

   (a) (6 points) What conditions on j and k guarantee that $\mathbf{F}_{p^j}$ an extension of $\mathbf{F}_{p^k}$? (I'm looking for an answer of the form "$\mathbf{F}_{p^j}$ is an extension of $\mathbf{F}_{p^k}$ if and only if ...")

   Solution: According to the main theorem on finite fields, $\mathbf{F}_{p^j}$ is an extension of $\mathbf{F}_{p^k}$ if and only if k divides j.

   (b) (4 points) When it is an extension, what is its degree: what is $[\mathbf{F}_{p^j} : \mathbf{F}_{p^k}]$?

   Solution: The answer is j/k. To determine this, let d denote the degree. Then as a vector space over $\mathbf{F}_{p^k}$, the field $\mathbf{F}_{p^j}$ has dimension d, and so there is a vector space isomorphism

   $$\mathbf{F}_{p^j} \equiv (\mathbf{F}_{p^k})^d.$$

   The left side has p^j elements, and the right side has $(p^k)^d = p^{kd}$ elements. Thus $j = kd$, so $d = j/k$.
   Alternatively, according to the main theorem, $[\mathbf{F}_{p^i} : \mathbf{F}_p] = i$ for any i, so you can solve for $[\mathbf{F}_{p^j} : \mathbf{F}_{p^k}]$ in the following:

   $$[\mathbf{F}_{p^j} : \mathbf{F}_p] = [\mathbf{F}_{p^j} : \mathbf{F}_{p^k}][\mathbf{F}_{p^k} : \mathbf{F}_p].$$

3. This problem deals with construction with straight-edge and compass.

   (a) (6 points) We proved a theorem describing the field K of constructible numbers; state that theorem. (No justification required.)

   Solution: For every α in K, there is a tower of field extensions

   $$\mathbf{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

   such that $\alpha \in F_n$, and such that for each $i \geq 1$, F_i is equal to $F_{i-1}(\sqrt{\beta_{i-1}})$ for some $\beta_{i-1} \in F_{i-1}$. Conversely, every element γ in such a field extension F_n is contained in K.

(b) (4 points) Let K denote the field of constructible numbers. Give two different examples of irrational numbers which are in K, and give two different examples of irrational (real) numbers which are not in K. (If you explain why some number α is not in K, then $-\alpha$ is not a "different" example of a number not in K, for instance.)

Solution: There are of course lots of examples. According to the theorem, numbers like $\sqrt{5}$ and $\sqrt[4]{7}$ are in K (and are not rational). Numbers like $\sqrt[3]{2}$ and π are not in K, because their degree is not a power of 2 (in the case of $\sqrt[3]{2}$) or they are transcendental (in the case of π).

4. (10 points) Let $\zeta_8 = e^{2\pi i/8}$. Compute the irreducible polynomial

(a) for ζ_8 over $\mathbf{Q}(i)$

Solution: $x^2 - i$. $\zeta_8 = e^{2\pi i/8} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ certainly satisfies this polynomial, so its degree is at most 2 over $\mathbf{Q}(i)$. Also ζ_8 is not in $\mathbf{Q}(i)$: the elements of $\mathbf{Q}(i)$ have the form $a+bi$ where a and b are rational, and ζ_8 does not have this form. Therefore its degree is bigger than 1: its degree is at least 2. Therefore its degree must be exactly 2, and $x^2 - i$ is its irreducible polynomial.

(b) for ζ_8 over $\mathbf{Q}$

Solution: $x^4 + 1$. ζ_8 satisfies this polynomial; can it satisfy one of smaller degree? Consider the extensions $\mathbf{Q} \subseteq \mathbf{Q}(i) \subseteq \mathbf{Q}(\zeta_8)$. These are all of degree 2, so ζ_8 has degree 4 over $\mathbf{Q}$. Therefore its irreducible polynomial over $\mathbf{Q}$ has degree 4, and we've found it.

5. (10 points) Consider the number $\alpha = \sqrt{2}+\sqrt{3}$.

(a) True or false: the irreducible polynomial for α over $\mathbf{Q}$ is the same as the irreducible polynomial for α over $\mathbf{Q}(\sqrt{6})$.

Solution: False. Note that α has degree at most 2 over $\mathbf{Q}(\sqrt{6})$: since $\alpha^2 = 5+\sqrt{6}$, then α is a root of the polynomial $x^2-(5+\sqrt{6})$.
I claim that α has degree 4 over $\mathbf{Q}$. Indeed, I claim that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$, and the right side is a degree 4 extension over $\mathbf{Q}$. I should verify both of these claims.
The first claim is that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$. It is clear that the left side is contained in the right. What about the other inclusion? By the form of α^2, $\sqrt{6}$ is contained in the left side, so $\sqrt{6}\alpha = 2\sqrt{3}+3\sqrt{2}$ is as well. Therefore

$$\sqrt{6}\alpha - 2\alpha = \sqrt{2}$$

is contained in the left side, as is $\alpha - \sqrt{2} = \sqrt{3}$. Therefore the right side is contained in the left, and the two fields are equal.
The second claim was that $[\mathbf{Q}(\sqrt{2},\sqrt{3}) : \mathbf{Q}] = 4$. Consider the tower of extensions

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt{2},\sqrt{3}).$$

The first of these is degree 2 and the second is degree 1 or 2. It is degree 1 if and only if $\sqrt{3} \in \mathbf{Q}(\sqrt{2})$, which I claim is not true. If it were, then $\sqrt{3} = a+b\sqrt{2}$ for some rational numbers a and b. Squaring both sides leads to the conclusion that $\sqrt{2}$ is rational, which is nonsense.

(b) True or false: the irreducible polynomial for α over $\mathbf{Q}$ is the same as the irreducible polynomial for α over $\mathbf{Q}(\sqrt[3]{5})$.

Solution: True. According to the computation in part (a), α has degree 4 over $\mathbf{Q}$. The extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{5})$ has degree 3: $\sqrt[3]{5}$ is a root of the polynomial x^3-5 which is irreducible by Eisenstein's criterion (with $p=5$). Consider the extensions

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{5}) \subseteq \mathbf{Q}(\sqrt[3]{5},\alpha)$$

and

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\sqrt[3]{5},\alpha)$$

The degree $[\mathbf{Q}(\sqrt[3]{5},\alpha) : \mathbf{Q}]$ is divisible by 3 by the first tower of extensions, and is divisible by 4 by the second tower of extensions. Thus it's divisible by 12, so α must have degree at least 4 over $\mathbf{Q}(\sqrt[3]{5})$. I know that it satisfies a degree 4 polynomial, so its degree is at most 4. Thus its degree is exactly 4, and its irreducible polynomial over $\mathbf{Q}$ is the same as its irreducible polynomial over $\mathbf{Q}(\sqrt[3]{5})$.