Practice questions for the Final Exam, May 14-15.

Quiz Instructions and information

- This is a take-home exam. It will be posted on Friday, May 14 at 2pm New York time. Answers must be uploaded to the NYUClasses web site for the class by 2pm on Saturday, May 15.
- You may consult the textbook and your notes, but you may not consult any other sources, online or print.
- You may not communicate with anyone other than the TA (Juma) or me regarding the exam. This includes fellow students, other math majors, or anyone else. If you have a question, please email me.
- Please write as clearly and neatly as possible in a quiz situation. If you scan or photograph a handwritten paper (the most common mode), please do that as well as possible in the quiz setting.
- You will be graded on clarity as well as mathematical correctness. You don't have to use full sentences in each case, but what you write should be grammatical and use mathematical terms and notation correctly. You may use scratch paper that you don't hand in to organize your thoughts. Reasoning is as important as the answer in a theory class like abstract algebra.
- You will get 25% credit for any question or question part that you leave blank. You may lose points for a wrong answer, even if you also give a correct answer. Cross out anything you think is wrong.
- The following questions are only from the last part of the class, but the exam will cover the whole class. Please look at the practice quiz, the quiz, the practice midterm, and the midterm for questions about other parts of the class. Some of the questions ask you to reproduce material from the book. Others ask you to solve problems. Some of the problems are more challenging than others. Nobody is expected to "get" everything.

Corrected May 11, Exercise 1, part (c), and Exercise 2 ($\zeta = e^{\cdots}$)
Questions

1. A field extension $\mathbb{K}/\mathbb{L}$ is Galois if L is the fixed field or the set of automorphisms of $\mathbb{K}$ that fix $\mathbb{L}$.

   (a) Let $\mathbb{K}/\mathbb{F}_p$ be a finite degree extension. Show that it is a Galois extension.

(b) (Related to part (a)) Let $f \in \mathbb{F}_p[t]$ be an irreducible polynomial of degree n. Show that an extension $\mathbb{K} = \mathbb{F}_p[\alpha]$ where $f(\alpha) = 0$ is a splitting field for f.

(c) Let $\mathbb{L} = \mathbb{C}(x)$ be the field of rational functions in one variable with complex coefficients. Some elements of $\mathbb{L}$ are $u(x) = x^2 - 1$ and $v(x) = (x-3)^2/(x+1)$. Let $f \in \mathbb{L}[w]$ have the form $f(w) = w^3 - v$ with $v \in \mathbb{L}$. Give an example of such an f that is irreducible. Show that if α is a root of such a polynomial in an extension field of $\mathbb{L}$, then f splits in $\mathbb{L}[\alpha]$ and the extension is Galois.

2. Let $\zeta = e^{2\pi i/3} \in \mathbb{C}$ be a primitive third root of unity. Let R be the ring of algebraic integers in $\mathbb{Q}[\zeta]$.

   (a) Find the degree $[\,\mathbb{Q}[\zeta] : \mathbb{Q}]$ and the irreducible monic polynomial, ζ satisfies, $\phi(t)$.

   (b) Show that $\zeta - 1$ and $\zeta^2 - 1$ are the roots of $\psi(t) = \phi(t+1)$. Use this to show that $(\zeta - 1)(\zeta^2 - 1) = 3$.

   (c) Show that $R = \mathbb{Z}[\zeta]$ and that this is a euclidean domain. One way to do the first part is to show that $\mathbb{Q}[\zeta] = \mathbb{Q}[i\sqrt{3}]$ and then use the description of R for that field from the book.

   (d) Let $A = (\zeta - 1) \subset R$ be the principal ideal. Show that A is a prime ideal.

   (e) Show that $A = (\zeta^2 - 1)$ also.

   (f) Show that the ideal $(3) \subset R$ factors as $(3) = A^2$ (ideal multiplication).

   (g) Show that if $l \in \mathbb{Z}$ is a rational prime so that the equation $t^2 = -3$ has no solution mod l, then the ideal $(l) \subset R$ is a prime ideal.

3. Show that if f is an irreducible polynomial of degree 5 over $\mathbb{Q}$, then the Galois group of f (more properly, the Galois group of a splitting field of f) has an element of order 5. Show that this cannot happen if f is reducible.

4. Let $f \in \mathbb{F}[t]$ be an irreducible polynomial over a general field $[f]$. Define a tower of fields $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$, where f splits in $\mathbb{L}$ and $\mathbb{K} = \mathbb{F}[\alpha]$, where α is a root of f in $\mathbb{L}$.

   (a) Show that $\mathbb{K}$ is isomorphic to the abstract field $\mathbb{F}/(f)$. Show that $\mathbb{K}$ is isomorphic to any field of the form $\mathbb{F}[\beta]$, where β is a root of f.

   (b) State the primitive element theorem over fields of characteristic zero and use it to show that if $\mathbb{F}$ has characteristic zero, then any splitting fields of f are isomorphic.

5. Here is a proof of a fact from the last class. Suppose $\mathbb{K}/\mathbb{F}$ is a finite degree Galois extension of degree n. Let $\alpha_1, \cdots, \alpha_n$ be a basis of $\mathbb{K}$ as a vector space over $\mathbb{F}$. Show that there is a *dual basis* of elements $\beta_1 \cdots, \beta_n$ so that $\mathrm{Tr}(\alpha_j \beta_k) = \delta_{jk}$. For any $\gamma \in \mathbb{K}$,

$$\mathrm{Tr}(\gamma) = \sum_{\sigma \in G} \sigma(\gamma) \ .$$

(a) Show that $S(\alpha,\beta) = \mathrm{Tr}(\alpha\beta)$ is a *bilinear form* over $\mathbb{F}$. *Bilinear* means that it is linear in each argument separately. If $a \in \mathbb{F}$, then

$$\begin{aligned} S(\alpha_1 + a\alpha_2, \beta) &= S(\alpha_1,\beta) + aS(\alpha_2,\beta) \\ S(\alpha, \beta_1 + a\beta_2) &= S(\alpha,\beta_1) + aS(\alpha,\beta_2)\ . \end{aligned}$$

Note that S is *symmetric*, which means $S(\alpha,\beta) = S(\beta,\alpha)$, so you need only check one part of bilinearity.

(b) Let R be the $n \times n$ matrix that represents S is the α_j basis, which means that the elements of R are $r_{jk} = S(\alpha_j,\alpha_k)$. Suppose two elements of $\mathbb{K}$ are $\gamma = \sum c_j\alpha_j$ and $\delta = \sum d_k\alpha_k$, where c_j and d_k are in $\mathbb{F}$. Let c be the column vector with components c_j, and similarly for d. Show that $S(\gamma\delta) = c^t\, R\, d$.

(c) A quadratic form is *non-degenerate* if $S(\gamma,\delta) = 0$ for all δ implies that $\gamma = 0$. Show that this S is not non-degenerate. (This is a simple but clever trick. If you don't find the trick, just move on.)

(d) Show that this S has R with $\det(R) \neq 0$.

(e) If a dual basis β_k does exist, the elements may be expressed in the form (why?)

$$\beta_k = \sum_{j=1}^{n} m_{kj}\alpha_j\ .$$

The elements $m_{jk} \in \mathbb{F}$ may be organized into an $n \times n$ matrix. Find a matrix equation involving R that M can satisfy to imply that the β_k are a dual basis. Does this equation have a solution?

6. Let R be the ring of elements of the form $a/2^n$ with $a \in \mathbb{Z}$ and $n \in \mathbb{Z}$ (so n may be negative). Show that this is a ring. Show that R is a principal ideal domain. What are the units of u (invertible elements)? What are the prime elements of R?