Honors Algebra II, Courant Institute, Spring 2021

http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2021/HonorsAlgebraII.html

Check the class forum for corrections and hints

Practice questions for the Midterm Exa,m, March 25.

Quiz Instructions and information

- You must do the midterm exam while on zoom with your camera on at all times. Upload your answers at the end of the quiz.
- The quiz will be closed book, closed notes, etc. You may not use any resources during the quiz, except ...
- You may prepare and use a "cheat sheet", which is one US standard size ($8\frac{1}{2}'' \times 11''$) piece of paper, front and back. Please upload the cheat sheet with your quiz answers, if you use one.
- 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.
- If you have a question during the quiz, please communicate with me on chat in the zoom session. Make sure the chat goes only to me and not the everyone in the session.

Questions

The actual midterm exam will be much shorter than this. The exam covers all material in Chapters 12, 15, and 16 that we covered in class or in homework, up to Section 16.5. The practice questions here do not cover material that was on the quiz, but the midterm exam itself may.

1. Let p be a rational prime and $\psi_p \colon \mathbb{Z}[t] \to \mathbb{F}_p[t]$ be the map $a_n t^n + \cdots a_0 \to \overline{a}_n t^n + \cdots + \overline{a}_0$, where $\overline{a} \in \mathbb{F}_p$ is the equivalence of integer a mod p. Take $f \in \mathbb{Z}[t]$ and $g_p = \psi_p(f)$. In each case, back your claim with a proof or a counterexample.

   (a) Is it possible that f is irreducible but g_p is not.

(b) Is it possible that g_p is irreducible but f is not?

(c) Is it possible that f has distinct roots in $\mathbb{C}$ but g_p does not have distinct roots in $\overline{F}_p$ (an algebraic closure of $\mathbb{F}_p$).

(d) Let l be a distinct rational prime. Is it possible that g_p is irreducible but g_l has nontrivial factors?

(e) Is it possible that f is irreducible in $\mathbb{Z}[t]$ but has non-trivial factors in $\mathbb{Q}[t]$?

2. Prove that if neither x nor y is a square mod p (p a rational prime), then xy is a square mod p. You may assume that neither x nor y is a multiple of p. You may assume that there is a generator g for $\mathbb{F}_p^*$.

3. Show that the polynomial $f(x) = x^{10} + x^9 + 1$ has distinct roots in any extension field of $\mathbb{Q}$. You may use the fact (which is easy to verify, but not on an exam) that $.9^9 < \frac{1}{2}$.

4. Show that the polynomial $f(t) = t^4 - 2$ factors but does not split in $\mathbb{F}_7$ and that f splits in $\mathbb{F}_{49}$.

5. Let f be a polynomial over $\mathbb{F}_p$ with $\deg(f) > p$ and so that f and f' are relatively prime. Show that f does not split in $\mathbb{F}_p$.

6. Consider the quotient $\mathbb{K} = \mathbb{Z}[i]/(p)$, where p is a rational prime with $p \equiv 3 \mod 4$.

(a) Show that $\mathbb{K}$ is a finite field and identify $|\mathbb{K}|$.

(b) Let a and b be rational integers in the range $\{0, 1, \cdots, p-1\}$. Show that every $x \in \mathbb{K}$ is uniquely a coset of the form $\overline{a + bi}$ in $\mathbb{Z}[i]/(p)$.

(c) Which of these are primitive elements for the extension $\mathbb{K}/\mathbb{F}_p$? *Hint.* If $b \neq 0$, find an irreducible quadratic $t^2 + ct_d$ with x as a root and c, d rational integers. Show that $a - ib$ is the other root. To check whether $a + ib$ and $a - ib$ are linearly independent over $\mathbb{F}_p$, check whether the ratio $(a + ib)/(a - ib)$ is in $\mathbb{F}_p$.

7. Use the quadratic reciprocity theorem to determine whether 113 is a square mod 127. *Hint.* To see whether n is prime it suffices to check possible prime factors $p \leq \sqrt{n}$.

8. Let $\mathbb{K}/\mathbb{Q}$ be a splitting field of $f(t) = t^3 - 2$. Let $\alpha \in \mathbb{K}$ have $\alpha^3 = 2$.

(a) Show that there is an $\omega \in \mathbb{K}$ with $\omega^3 = 1$ but $\omega \neq 1$.

(b) Show that any such ω satisfies $\omega^2 + \omega + 1 = 0$.

(c) Show that there is a unique automorphism automorphism, σ, of $\mathbb{K}$ over $\mathbb{Q}$ with $\sigma(\alpha) = \omega\alpha$ and $\sigma(\omega) = \omega$.

(d) Show that there is a unique automorphism, τ, of $\mathbb{K}$ over $\mathbb{Q}$ with $\tau(\omega) = -\omega$ and $\tau(\alpha) = \alpha$.

(e) In any group, the *commutator* of elements g, h is $[g, h] = g^{-1}h^{-1}gh$. The commutator is a measure of how non-abelian a group is. Calculate $[\sigma, tau]$.