Honors Algebra II, Courant Institute, Spring 2020

http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2020/HonorsAlgebraII.html

Always check the `classes` message board before doing any work on the assignment.

Assignment 3, due February 17

Corrections: [none yet]

The Gaussian integer questions explore the relation between the fields $\mathbb{Z}/(p)$ and $\mathbb{Z}[i]/(q)$. This is an example of a general theory: If K is a finite degree Galois extension of $\mathbb{Q}$, then there is a ring $O_K \subset K$ of *algebraic integers*. If $K = \mathbb{Q}[i]$, then $O_K = \mathbb{Z}[i]$. A prime ideal $\mathfrak{p}$ "lies over" a *rational prime* (a prime $p \in \mathbb{Z}$) if $\mathfrak{p} \cap \mathbb{Z} = (p)$. (This $\mathfrak{p}$ is in the \mathfrak font, as in $\mathfrak{p}$. This old German font is "fraktur".) The Galois group of K over $\mathbb{Q}$ "acts" on the ideals lying over p. For Gaussian integers, the Galois group is C_2 (cyclic with two elements, corresponding to $z = x + iy \leftrightarrow \overline{z} = x - iy$ (complex conjugation). If there are two Gaussian primes "over" the same rational prime, the Galois group interchanges them. There is also some complementary Galois business going on with the quotient fields mod p and mod $\mathfrak{p}$.

You may assume the following: Suppose $\mathbb{E}$ is a finite field. The multiplicative group (the group of non-zero $x \in \mathbb{E}$ under multiplication) is $\mathbb{E}^*$ and is cyclic. In particular, there is a *generator* $g \in \mathbb{E}$ so that every $x \in \mathbb{E}$ may be written as $x = g^k$ for some integer k. If $\mathbb{E}^*$ has n elements, then these are $\left\{1, g, \ldots, g^{n-1}\right\}$. This is sometimes called the "little Fermat theorem", but I think Fermat only knew that $x^p = x \bmod p$ and not that the multiplicative group is cyclic.

1. Let q be a Gaussian prime. Show that $\mathbb{Z}[i]/(q)$ is a field by showing that (q) is a maximal ideal.

2. Let q be a Gaussian prime. Show that $\mathbb{Z}[i]/(q)$ has $|q|^2$ elements. *Hint*: The euclidean domain construction may help.

3. List the five elements of $\mathbb{Z}[i]/(2+i)$ and construct an explicit isomorphism (say who goes where) to $\mathbb{F}_5 = \mathbb{Z}/(5) = \{0, 1, 2, 3, 4\}$. There are many ways to list the elements but the isomorphism is unique.

4. Suppose q is a Gaussian prime that is not a rational prime. We know (Assignment 2) that $|q|^2 = p$, where p is a rational prime. Show that the principal ideals (q) and $(\overline{q})$ lie over $(p) \subset \mathbb{Z}$. Here $\overline{q}$ is the complex conjugate of q.

5. Let $p \neq 2$ be a rational prime (i.e., $p \in \mathbb{Z}$) that is also a Gaussian prime. Let $\mathbb{E} = \mathbb{Z}[i]/(p)$, be the quotient field.

   (a) Show that $\mathbb{E}$ has p^2 elements, using a geometric argument like that from exercise (2).

(b) Show that $\mathbb{E}$ has *characteristic* p, which means that if $x \in \mathbb{E}$, then $p.x = x + x + \cdots + x = 0$ (p copies of x in the sum). (People (e.g., Serre) write $p.x$ instead of px to indicate the integer p multiplying the field element x, because in $\mathbb{E}$, $p = 1 + \cdots + 1 \equiv 0$.)

(c) Explain the natural embedding $\mathbb{F}_p \subset \mathbb{E}$ and show that $\mathbb{E}/\mathbb{F}_p$ is a field extension.

(d) Show that if $p \neq 2$ is a rational and Gaussian prime, then $x^2 + 1$ is irreducible in $\mathbb{F}_p$. *Hint*: From assignment 2, what is p mod 4? When is there a k so that $g^k = -1$ in $\mathbb{F}_p$?

(e) Show that $\mathbb{E}/\mathbb{F}_p$ is the splitting field of $x^2 + 1$. Use this to give a different proof that $|\mathbb{E}| = p^2$.

6. Let $\mathbb{E}$ be a field with $|\mathbb{E}| = p^2$. Let $F \subset \mathbb{E}$ be defined by $x \in F \iff x^p = x$. Show that $F = \mathbb{F}_p$ (with the operations in $\mathbb{E}$). *Hint*: How many solutions of $x^p = x$ can there be in $\mathbb{E}$? How are they related to $1 \in \mathbb{E}$?

7. (*You know how to do this if you went to the first recitation.*) Let $A \subset \mathbb{C}$ be the set of all complex numbers of the form $x = a + bi\sqrt{5}$, with a and b being rational integers.

(a) Show that A is isomorphic to $\mathbb{Z}[x]/(x^2 + 5)$.

(b) An element $x \in A$ is *irreducible* if $x = yz$ implies that either y or z (or both) is a unit. Show that 2, 3, $1 + i\sqrt{5}$ and $1 - i\sqrt{5}$ are all irreducible.

(c) The definition of a *unique factorization domain* is that for any x there are irreducible elements $p_i \in A$ so that $x = p_1 p_2 \cdots p_n$, and if $x = q_1 \cdots q_m$ with q_i irreducible, then $m = n$ and there are units u_i and a permutation j_i so that $q_i = u_i p_{j_i}$. Find two non-equivalent factorizations of $6 \in \mathbb{Z}[i\sqrt{5}]$ to show that $\mathbb{Z}[i\sqrt{5}]$ is not a unique factorization domain. In particular, $\mathbb{Z}[i\sqrt{5}]$ is not a euclidean domain.

8. Let $\mathbb{E} \subset \mathbb{C}$ be a splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let $\alpha \in \mathbb{R}$ be the real solution of $x^3 = 2$. Let $\omega = e^{2\pi i/3} \in \mathbb{C}$.

(a) Show that $\left\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\right\}$ is a basis for $\mathbb{E}$ over $\mathbb{Q}$.

(b) Let $\xi_1 = \alpha$, $\xi_2 = \omega\alpha$, and $\xi_3 = \omega^2\alpha$ be the three roots of $x^3 = 2$ in $\mathbb{E}$. Let S_3 be the group of permutations of $\{\xi_1, \xi_2, \xi_3\}$. Show that for any $\pi \in S_3$, there is a unique automorphism σ on $\mathbb{E}$ that fixes $\mathbb{Q}$ with $\sigma(\xi_j) = \xi_{\pi_j}$. *Warning*: Do not give six proofs for the six elements of S_3.

(c) Find the fixed field, $\mathbb{F}$, for the subgroup $H \subset S_3$ generated by the transposition $\xi_2 \leftrightarrow \xi_3$. Show that there are no non-trivial isomorphisms of $\mathbb{F}$ that fix $\mathbb{Q}$.

(d) Find the fixed field for the subgroup $H \subset S_3$ generated by the transposition $\xi_1 \leftrightarrow \xi_2$.

(e) Find the fixed field, $\mathbb{K}$, of the cyclic permutation $(\xi_1, \xi_2, \xi_3) \to (\xi_2, \xi_3, \xi_1)$.

(f) Show that there is one non-trivial isomorphism of $\mathbb{K}$ that fixes $\mathbb{Q}$.

9. Find the formula for the polynomial

$$f(x_1, \ldots, x_n) = \sum_{k=1}^{n} x_k^3$$

in terms of elementary symmetric polynomials.

10. Find the formula for $f(x, y) = x^4 + y^4$ in terms of elementary symmetric polynomials in x and y. You may start by checking

$$(x + y)^4 = x^4 + y^4 + 6(xy)^2 + 3(xy)(x^2 + y^2) \ .$$