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 2, due February 10

Corrections: [none yet]

The first five exercises are about Gaussian integers. They are closely related there is a lot of overlap in the answers. Please read all of them before starting to work on them. The next few are taken from the Michael Artin text problems on Section 3 of Chapter 15. These are beautiful problems. I urge you to look at the rest of them. The last three exercises are not about field theory, but are about the fact that row rank equals column rank.

1. An element $x \in R$ is *composite* if it is not a unit or a prime. Show that if $x \in \mathbb{Z}[i]$ is composite, then $|x|^2$ factors as a product of powers of $|p_i|^2$, where the p_i are Gaussian primes. Give an example (see the table below) showing that the converse is false. Explain how a factorization of $|x|$ limits the possible factors of x. *Hint*: $|x|^2 = x\overline{x}$ ($\overline{x}$ is the complex conjugate of x).

2. Fill in the table below to include all $x \in \mathbb{Z}[i]$ with $|x|^2 \leq 49$ to identify the first few primes in $\mathbb{Z}[i]$. Explain that the rows of the table really should be arranged in order of increasing $|x|$.

x family	$\|x\|^2$	factorization in $\mathbb{Z}$	factorization of x in $\mathbb{Z}[i]$
• $1+i$	• 2	prime	prime
2	4	$= 2^2$	$= -i \cdot (1+i)^2$
• $2+i,\ 1+2i$	• 5	prime	prime
$2+2i$	8	$= 2^3$	$= i \cdot (1+i)^3$
• 3	• 9	$= 3^2$ (3 is new)	prime
$3+i,\ 1+3i$	10	$= 2 \cdot 5$	$= (1+i)(2+i)$
• $3+2i$	• 13	prime	prime
$3+3i$	18	$= 2 \cdot 9$	
4			
⋮		⋮	
7			

3. If $p \in \mathbb{Z}$ is prime in $\mathbb{Z}$, we call p an integral prime. If $q \in \mathbb{Z}[i]$ and q prime in $\mathbb{Z}[i]$, we call q a Gaussian prime. For example, 3 and 5 are integral primes, 3 is a Gaussian prime but 5 is not a Gaussian prime. Let p be an integral prime. The element $1+i$ is a Gaussian prime. Any Gaussian prime that is in $\mathbb{Z}$ is an integral prime. Show that p factors in $\mathbb{Z}[i]$ if

$p = |q|^2$ for some Gaussian prime q. Use this and the table above to help decide which of the integral primes up to 29 are Gaussian primes.

4. Show that if p is an odd integral prime and $p \equiv 3 \bmod 4$, then p is a Gaussian prime. *Hint*: If p factors in $\mathbb{Z}[i]$ but not in $\mathbb{Z}$, then $p = a^2 + b^2$ with a and b integers. One of a or b must be even. Reduce $p = a^2 + b^2$ mod 4. Note that this does not prove the converse, that integral primes equal to 1 mod 4 are not Gaussian primes.

5. Show that if $q \notin \mathbb{Z}$ is a Gaussian prime, then $|q|^2 = \overline{q}q$ ($\overline{q}$ is the complex conjugate) then $p = |q|^2$ is an integral prime. *Hint*: $\mathbb{Z}[i]$ is a unique factorization domain (why?).

6. Show that if $\mathbb{F}$ is a field, and $\mathbb{E} = \mathbb{F}[\alpha]$ is an extension field of degree 5, then $\mathbb{E} = \mathbb{F}[\alpha^2]$.

7. Let $\zeta_n = e^{2\pi i/n}$ be a primitive $n-$th root of unity in $\mathbb{C} : \mathbb{Q}$. Show that if $x \in \mathbb{Q}[\zeta_7]$ and $x \neq 1$, then $x^5 \neq 1$ (reworded for emphasis).

8. We call $\alpha \in \mathbb{C}$ *algebraic* if α is algebraic over $\mathbb{Q}$. Show that if $\alpha \in \mathbb{C}$ and $\beta \in \mathbb{C}$, and if $\alpha + \beta$ and $\alpha\beta$ are algebraic, then α and β are algebraic.

9. An extension E/K is *algebraic* if every $x \in E$ is algebraic over K.

   (a) Give an example of an algebraic extension over $\mathbb{Q}$ that does not have finite degree.

   (b) Suppose L/E is algebraic and E/K is algebraic, show that L/K is algebraic. *Hint*: This is equivalent to showing that for every $x \in L$, $K[x]/K$ is an algebraic field extension (why?).

10. (*This exercise is explained in both Artin books in different ways. I would like you to write it up as practice summarizing for yourself an important argument.*) Let A be a matrix with n rows and m columns. The *row space* of A is the linear subspace of $\mathbb{R}^m$ spanned by the rows of A. Here, $r \in \mathbb{R}^m$ is thought of as an $m-$component row vector. The *column space* of A is the subspace of $\mathbb{R}^n$ spanned by the columns of A. Here $c \in \mathbb{R}^n$ is thought of as an $n-$component column vector.

    (a) Let $L : \mathbb{R}^n \to \mathbb{R}^n$ be a linear map. Let $S \subseteq \mathbb{R}^n$ be a linear subspace. Let $S' = LS$ be the image of S under L. Show that if L is invertible then $\dim(S) = \dim(S')$.

    (b) Let A' be the matrix you get from A when you add a multiple of column j to column $k \neq j$. Show that this generates an invertible linear map on $\mathbb{R}^m$ (the row space) and on $\mathbb{R}^n$ (the column space). Be careful, as the two proofs are a little different. Show that this is also true if A' comes from A by interchanging two rows or two columns.

    (c) Show that the dimension of the row or column space of A is the same as the dimension of the row or column space of A'.

(d) Explain that after a sequence of operations of the type described in part (b), you can get an *upper triangular* matrix A'' that has entries $a''_{jk} = 0$ if $j > k$.

(e) Explain how the row rank and column rank of A'' may be determined from the number of rows at the bottom or columns on the right that are all zero.

(f) Finish the proof that the row and columns spaces of A have the same dimension.

(g) Suppose that A is a square matrix. Use the row/column rank thing to show that $\dim[\ker(A)] = \dim[\ker(A^t)]$, where A^t is the transpose of A.

11. (*This the hard part of the Perron Frobenius theorem, which plays a central role in the theory of Markov chains (a kind of random process).*) An $n \times n$ matrix P with entries $p_{jk} \in \mathbb{R}$ is called *stochastic* if the entries are non-negative and each row sum is equal to 1. That is

$$p_{jk} \geq 0 \text{ for all } j \text{ and } k, \text{ and } \sum_{k=1}^{n} p_{jk} = 1 \text{ for all } j .$$

(a) Show that a stochastic matrix has a right eigenvector (a column vector) $\mathbf{1}$ with all entries equal to 1

$$\mathbf{1} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

and eigenvalue $\lambda = 1$. That is $P\mathbf{1} = \mathbf{1}$.

(b) Show that a stochastic matrix has a left eigenvector (a row vector) π that satisfies $\pi P = \pi$. *Hint:* Apply the previous problem with $A = P - I$.

12. (*This application of "no kernel implies onto" has impressed a chain of mathematicians over a century. It is well known in my field (numerical methods for solving PDE) and was used by E. Artin (wbo probably got it from R. Courant) as an exercise. Peter Lax put it in his linear algebra book with an acknowledgement to E. Artin. M. Artin put it in his book with an acknowledgement to P. Lax.*) Consider the system of linear equations over $\mathbb{R}$ for unknowns $x_1, \ldots, x_n$ with $n \geq 3$.

$$\begin{aligned} 2x_1 - x_2 &= f_1 \\ -x_{j-1} + 2x_j - x_{j+1} &= f_k \ , \quad \text{for } 2 \leq j \leq n-1 \\ -x_{n-1} + 2x_n &= f_n \ . \end{aligned}$$

These equations may be expressed in terms of an $n \times n$ matrix A with entries a_{jk}. These are $a_{jj} = 2$ for all j, $a_{j,j+1} = -1$ for $1 \leq j \leq n-1$, and $a_{j,j-1} = -1$ for $2 \leq j \leq n$.

(a) Prove the identity

$$x^t A x = x_1^2 + \sum_{j=1}^{n-1} (x_j - x_{j+1})^2 + x_n^2 \ .$$

(b) Show that if $x \neq 0$ (in $\mathbb{R}^n$), then $Ax \neq 0$.

(c) Show that the equations above have a solution, which is unique, for any numbers $f_1, \ldots, f_n$.