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 9, due April 6

Corrections: April 8 (after due date, sorry) The discriminant formula in exercise 1d corrected to $ac - b^2$ from $ac - 4b^2$. The corrected formula takes into account the 2 in $ax^2 + 2bxy + cy^2$.

1. Prove the following facts about polynomial solutions in the finite field $\mathbb{F}_p$ with $p \neq 2$:

   (a) The equation $x^2 = z$ has a solution for exactly half of the $z \neq 0$.

   (b) The equation $x^k = z$ has exactly one solution for all z, if k is odd. (The case $k = p$ is different and simpler than $k \neq p$. If you get stuck for general k, try $x^3 = z$ first.)

   (c) The equation $x^4 = z$ has solutions for exactly half of all $z \neq 0$ or exactly a quarter of all $z \neq 0$ depending on whether $p = 1$ or $p = -1$ mod 4.

   (d) A *binary quadratic form* is a two variable ("binary" means two arguments) homogeneous ("form" means homogeneous polynomial) quadratic polynomial function of the form $f(x, y) = ax^2+2bxy+cy^2$. The coefficients a, b, c, are in $\mathbb{F}_p$. The form is *non-degenerate* if $D = ac-b^2 \neq 0$. The equation $f(x, y) = z$ has a solution for any $z \in \mathbb{F}_p$ if f is non-degenerate. *Hint*: This took me a while to figure out. My approach (hinted at here) may not be the simplest. The hardest things (for me) were the two "(why?)" facts. You can write the equation in matrix form as

   $$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = z \ , \ \ R^t W R = z \ , \ \ R = \begin{pmatrix} x \\ y \end{pmatrix} \ , \ \ W = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \ .$$

   Look for a non-singular $A \in \mathrm{GL}(2, \mathbb{F}_p)$ and consider linear changes of variable $S = AR$ so that f takes the form $S^t \widetilde{W} S$, where $\widetilde{W}$ is as simple as possible (diagonal, ± 1 on the diagonal). ($\mathrm{GL}(n, \mathbb{F})$ is the *general linear group*, which is set of $n \times n$ matrices with entries in the field $\mathbb{F}$ that are invertible. The Michael Artin textbook has material on canonical forms for quadratic forms.) If you can put the equation in the form $x^2 - y^2 = z$, then another linear transformation puts the equation in the form $uv = z$, so there is a solution u for any v and z. The (x, y) for a given z cannot be unique in general, because there are p^2 pairs (x, y) and only p values of z. If $p = -1$ mod 4 then you might have to settle for the form $x^2+y^2 = z$, with a possibly different z. With $y = 0$, you can get the values $Q = \left\{ x^2 \mid x \in \mathbb{F}_p \ , \ x \neq 0 \right\}$

("Quadrat" is German for "square" and gives English "quadratic" for squares). Then you have to get the values $z \notin Q$ using non-zero y. You can see that the set $Q+1 = \{z+1 \mid z \in Q\}$ has $Q \subset \mathbb{F}_p^*$ (i.e., does not contain zero) and therefore $Q+1 \neq Q$ (why?). Therefore there is (x,y) with $z = x^2+y^2 \notin Q$. The pairs tx^2+ty^2 get the rest of Q^c (why?).

2. Suppose K is a finite normal extension of $\mathbb{Q}$. The *algebraic integers* in K are elements $\alpha \in K$ that satisfy equations $f(\alpha) = 0$, where $f \in \mathbb{Z}[x]$ is monic. The set of algebraic integers, $\mathcal{O}_K$, is a ring (assignment 7). This exercise shows that $\mathcal{O}_K$ is a noetherian ring. If the steps here seem too abstract, consider solving exercise 3 as you solve this one.

   (a) Show that for any $x \in K$, there is an integer r so that $rx \in \mathcal{O}_K$. [A special case of this is familiar to me from high school algebra, where we were told to replace expressions like $\frac{1}{\sqrt{2}}$ with $\frac{\sqrt{2}}{2}$ having a "rational integer downstairs". With $r = 2$ and $x = \frac{1}{\sqrt{2}} \in \mathbb{Q}[\sqrt{2}]$, we have $rx = \sqrt{2} \in \mathcal{O}_{\mathbb{Q}[\sqrt{2}]}$. Note that $\alpha = \sqrt{2} \in \mathcal{O}_{\mathbb{Q}[\sqrt{2}]}$ because it satisfies the monic integer polynomial equation $\alpha^2 - 2 = 0$.]

   (b) Let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. For any $x \in K$, the trace is

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

   Show that $\mathrm{Tr}(x) \in \mathbb{Q}$ for any $x \in K$.

   (c) A *bilinear form* is a function $f(x,y)$ that is linear in x for every y and linear in y for every x. Show that $f(x,y) = \mathrm{Tr}(xy)$ is a bilinear form on K with values in $\mathbb{Q}$.

   (d) A bilinear form is *non-degenerate* if the linear map $x \to f(x,y)$ is not the zero map unless $y = 0$, and the map $y \to f(x,y)$ is not the zero map unless $x = 0$. Show that $f(x,y) = \mathrm{Tr}(xy)$ is non-degenerate.

   (e) Suppose $\xi_1, \ldots, \xi_n$ form a basis for an n dimensional vector space V over a field $\mathbb{F}$. A *dual basis* with respect to a non-degenerate quadratic form $f\colon V \times V \to \mathbb{F}$ is a set of elements $\eta_k \in V$ so that $f(\xi_j, \eta_k) = \delta_{jk}$. This δ is the *Kronecker delta symbol*, with $\delta_{jk} = 0$ if $j \neq k$ and $\delta_{kk} = 1$, for all j and k. Show that for every basis and non-degenerate bilinear form there is a dual basis. *Hint*: This can be done, among other ways, using Emil Artin (*Galois Theory* book) style linear algebra. The matrix that "represents" f in the ξ_k basis is non-singular if f is non-degenerate. Suppose $u \in V$ has representation

   $$u = \sum_{k=1}^{n} a_k \xi_k \ .$$

Show that if η_k is the dual basis, then the "expansion coefficients" are given by

$$a_j = f(u, \eta_j) \; .$$

(f) Let elements $\xi_j \in K$ be a basis of K over $\mathbb{Q}$. Use part (a) to show that there is a basis with $\xi_j \in \mathcal{O}_K$ for all j. Let r be a rational integer. Let M_r be the set of elements $x \in K$ so that

$$x = \frac{1}{r} \sum_{j=1}^{n} a_j \xi_j \; , \quad \text{all } a_j \in \mathbb{Z} \; .$$

Show that M_r is a noetherian module over $\mathbb{Z}$.

(g) Show that if $x \in \mathcal{O}_K$ and $y \in \mathcal{O}_K$, then $\mathrm{Tr}(xy) \in \mathcal{O}_K$.

(h) Let η_j be the elements of the dual basis to the basis $\xi_j \in K$, with respect to the bilinear form $\mathrm{Tr}(x, y)$. Show that Show that there is a rational integer r so that $r\eta_j \in \mathcal{O}_K$ for all j. Use this to show that there is a fixed r so that if $\alpha \in \mathcal{O}_K$, then $\alpha \in M_r$ for some r.

(i) Show that $\mathcal{O}_K$, as a module over $\mathbb{Z}$ is a noetherian module. Use this to show that $\mathcal{O}_K$ is a noetherian ring.

3. Go through exercise 2 for the specific field $K = \mathbb{Q}[i\sqrt{d}]$. Show that $\xi_1 = 1$ and $\xi_2 = i\sqrt{d}$ is a basis. If $x = \alpha\xi_1 + \beta\xi_2$ and $y = \gamma\xi_1 + \delta\xi_2$, find a formula for $\mathrm{Tr}(xy)$ in terms of α, β, γ, and δ. Find the dual basis, η_1, and η_2. Find r so that $r\eta_1$ and $r\eta_2$ are in $\mathcal{O}_{\mathbb{Q}[i\sqrt{d}]}$. Show that if $x \in \mathcal{O}_{\mathbb{Q}[i\sqrt{d}]}$, then $x = \frac{1}{2}\left(a + i\sqrt{d}\, b\right)$, with rational integers a and b. (Note, it may be that $r \neq 2$, so this may require working out formulas in more detail.)