ALGEBRAIC NUMBER THEORY W4043

1. Homework, week 1, due September 17

1. (Linear diophantine equations) Let $a, b, c \in \mathbb{Z}$. Give necessary and sufficient conditions for the existence of a solution to the diophantine equation

$$ax + by = c$$

with $x, y \in \mathbb{Z}$.

2. A *quadratic field* is an extension of $\mathbb{Q}$ of degree 2. Let $d \in \mathbb{Z}$ and assume d is not a square in $\mathbb{Q}$. Let $\sqrt{d} \in \mathbb{C}$ be a square root of d, and define $\mathbb{Q}(\sqrt{d})$ to be the subfield of $\mathbb{C}$ consisting of elements of the form $\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ (you may want to verify that $\mathbb{Q}(\sqrt{d})$ is a field if you haven't seen this previously).

(a) Prove that $\mathbb{Q}(\sqrt{d})$ is a quadratic field. Show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some integer d. Show that $\mathbb{Q}(\sqrt{d})$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group, indicating the action of non-trivial elements of $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ on the typical element $a + b\sqrt{d}$.

(b) Let d and d' be two integers that are not squares in $\mathbb{Q}$. Show that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ if and only if d/d' is a square in $\mathbb{Q}$. Use this result to give a complete (infinite) list of all quadratic fields.

(c) Let $P(x) = ax^2+bx+c \in \mathbb{Z}[x]$, with $a \neq 0$, and assume P is irreducible in $\mathbb{Q}[x]$. Let $\Delta = b^2 - 4ac$ be the discriminant of P. Show that $\mathbb{Q}(\sqrt{\Delta})$ is a splitting field for P. What are the possible values of Δ modulo 4?

(d) Conversely, let $d \in \mathbb{Z}$ be a square-free integer (in other words, if p is a prime dividing d then p^2 does not divide d). Find a monic polynomial $Q \in \mathbb{Z}[x]$ with splitting field $\mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \pmod 4$ show that Q can be taken to have discriminant d; if $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$ show that Q can be taken to have discriminant $4d$.

3. Consider the polynomial $P(x) = x^{68} + x^{51} + x^{34} + x^{17} + 1 \in \mathbb{Z}[x]$.

(a) Show that $P(x)$ is a product of a two irreducible polynomials P_4 and P_{64} in $\mathbb{Q}[x]$ of degrees 4 and 64, respectively. There is no need to determine the factors explicitly. (Hint: let $y = x^{17}$; use Galois theory.)

(b) Let p be a prime number and let $\mathbb{F}_p$ be the finite field with p elements. We write $\bar{P}_{64}$ for the reduction of P_{64} modulo p; i.e., if $P_{64} = \sum_{i=0}^{64} a_i x^i$, $\bar{P}_{64} \in \mathbb{F}_p[x]$ is the polynomial whose ith coefficient is $\bar{a}_i$, where $\bar{a}_i$ is the residue of a_i modulo p. Give necessary and sufficient conditions for $\bar{P}_{64}$ to factor as a product of linear terms in $\mathbb{F}_p[X]$.

(c) Let k be a splitting field for $\bar{P}_{64}$ over $\mathbb{F}_p$. What is the maximal possible degree $[k : \mathbb{F}_p]$? What is the Galois group in that case?