MATH 210 PROBLEM SET 4

RAVI VAKIL

This problem set is due on Friday, February 23 at Jarod Alper's office door.

In this problem set, you'll compute an interesting Galois group, prove a famous theorem (Hilbert's "Theorem 90"), use it to cheaply get Pythagorean triples, and work through a useful construction (the resultant).

1. *(Dummit and Foote, p. 562, problem 16)*
(a) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.
(b) Show that the roots of this quartic are $\alpha_1 = \sqrt{1+\sqrt{3}}$, $\alpha_2 = \sqrt{1-\sqrt{3}}$, $\alpha_3 = -\sqrt{1+\sqrt{3}}$, $\alpha_4 = -\sqrt{1-\sqrt{3}}$.
(c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
(d) Prove that K_1, K_2, and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.
(e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

2. *(This is basically Dummit and Foote, p. 563, problem 23: Hilbert's Theorem 90)* If K is a Galois extension of F, define the *norm* of an element $\alpha \in K$ to F by

$$N_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha).$$

(See problem 17 on p. 563.) Now let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that α is of the form $\alpha = \beta/(\sigma\beta)$ for some nonzero $\beta \in K$. (Hint: By the linear independence of characters show there exists some $\theta \in K$ such that

$$\beta = \theta + \alpha\sigma(\theta) + (\alpha\sigma\alpha)\sigma^2(\theta) + \cdots + (\alpha\sigma\alpha\cdots\sigma^{n-2}\alpha)\sigma^{n-1}(\theta)$$

is nonzero. Compute $\beta/\sigma\beta$ using the fact that α has norm 1 to F.)

3. *(This is basically Dummit and Foote, p. 564, problem 24.)* Prove that the rational solutions $a, b \in \mathbb{Q}$ of Pythagoras' equation $a^2 + b^2 = 1$ are of the form $a = \frac{s^2-t^2}{s^2+t^2}$ and $b = \frac{2st}{s^2+t^2}$ for some $s, t \in \mathbb{Q}$ and hence show that any right triangle with relatively prime integer sides has sides of lengths $(m^2 - n^2, 2mn, m^2 + n^2)$ for some integers m, n. Do this as follows: note that $a^2 + b^2 = 1$ is equivalent to $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = 1$, then use Hilbert's Theorem 90 in the previous problem with $\beta = s + it$.

4. *(This is basically Dummit and Foote, p. 600, problem 29.)* This exercise gives an effective method of seeing whether two polynomials have a common factor. In particular, this can be used to check if a polynomial and its derivative have a common factor. Let F be a field

Date: Friday, February 16, 2007.

and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be two polynomials in $F[x]$.

(a) Prove that a necessary and sufficient condition for $f(x)$ and $g(x)$ to have a common root (in the splitting field, or, equivalently, a common divisor in $F[x]$) is the existence of a polynomial $a(x) \in F[x]$ of degree at most $m-1$ and a polynomial $b(x) \in F[x]$ of degree at most $n-1$ with $a(x)f(x) = b(x)g(x)$.

(b) Writing $a(x)$ and $b(x)$ explicitly as polynomials show that equating coefficients in the equation $a(x)f(x) = b(x)g(x)$ gives a system of $n+m$ linear equations for the coefficients of $a(x)$ and $b(x)$. Prove that this system has a nontrivial solution (hence $f(x)$ and $g(x)$ have a common zero) if and only if the determinant

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & & \\ & & a_n & a_{n-1} & \cdots & a_0 & & \\ & & & \ddots & & & & \\ & & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & & & \\ & b_m & b_{m-1} & \cdots & b_0 & & & \\ & & b_m & b_{m-1} & \cdots & b_0 & & \\ & & & \ddots & & & & \\ & & & & b_m & b_{m-1} & \cdots & b_0 \end{vmatrix}$$

is zero. Here $R(f,g)$, called the *resultant* of the two polynomials, is the determinant of an $(n+m) \times (n+m)$ matrix R with m rows involving the coefficients of $f(x)$ and n rows involving the coefficients of $g(x)$. As baby cases, find the resultant of the quadratic $ax^2 + bx + c$ and its derivative; and of the cubic $x^3 + bx + c$ and its derivative.