MATH 895, Assignment 3, Summer 2009

Instructor: Michael Monagan

Please hand in the assignment by 3:30pm Monday June 29thh.
Late Penalty -20% off for up to one day late. Zero after that.

Question 1: Minimal polynomials.

Let α be an algebraic number with minimal polynomial $m(z) \in \mathbb{Q}[z]$.
Prove that $m(z)$ is irreducible over $\mathbb{Q}$.

Using the method suggested in class, find the minimal polynomial for

$$\alpha = 1 + \sqrt{2} + \sqrt{3}.$$

Question 2: Norms.

Prove that the norm is multiplicative, i.e., $N(ab) = N(a)N(b)$, by showing that for A, B, C non-zero in $\mathbb{Q}[z]$,

$$\operatorname{res}(A, BC) = \operatorname{res}(A, B) \operatorname{res}(A, C).$$

Question 3: Computing with algebraic numbers.

Let ω be a primitive 4th root of unity with minimal polynomial $m(z) = z^4 + z^3 + z^2 + z + 1$.
Compute ω^{-1} in $\mathbb{Q}[z]/m(z)$ and use this to solve the following linear system for x and y.

$$\{ \ \omega x + \omega y = 1, \ \omega^3 x + \omega^4 y = -1 \ \}$$

Question 4: Trager's algorithm

Let α be a primitive 4th root of unity with minimal polynomial $m(z) = z^4 + z^3 + z^2 + z + 1$. Using Trager's algorithm, factor $f(x) = x^5 - 1$ over $\mathbb{Q}(\alpha)$.

Question 5: Square-free norms.

To factor $f(x)$ over $\mathbb{Q}(\alpha)$, Trager's algorithm chooses $s \in \mathbb{Q}$ such that the norm $N(f(x-s\alpha))$ is square-free. Theorem 8.18 states that only finitely many s do not satisfy this requirement. Give a characterization for which s satisfy this requirement in terms of resultants.
Hint: $n(x)$ is square-free iff $\gcd(n(x), n'(x)) = 1$ where $n(x) = N(f(x - s\alpha))$.

Using your characterization, for $\alpha = \sqrt{2}$ and $f(x) = x^2 - 2$, find all $s \in \mathbb{Q}$ for which the $n(x)$ is not square-free. Repeat this for the factorization problem in question 4.

Question 6: Cyclotomic polynomials.

The n'th cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial for the primitive n'th root of unity. For $n = 2, 3, ..., 12$, factor the polynomial $x^n - 1$ over $\mathbb{Q}$ using the factor command and identify the cyclotomic polynomials $\Phi_n(x)$ for $n = 7, 8, ..., 12$. Now determine an algorithm for computing $\Phi_n(x)$ that does not do any polynomial factorization. Using your algorithm, find the first n such that the largest coefficient of $\Phi_n(x)$ is 3 in magnitude.

Note: if α is an n'th root of unity, but NOT a primitive n'th root of unity, that is, $\alpha^m = 1$ for some $m < n$ and $m|n$, then $\gcd(\Phi_n(x), x^m - 1) = 1$ so $\Phi_n(x)$ divides the polynomial

$$\frac{(x^n - 1)}{(x^m - 1)}.$$