MATH 895, Assignment 3, Summer 2011

Instructor: Michael Monagan

Please hand in the assignment by 9:30am Wednesday June 22nd.
Late Penalty -20% off for up to two days 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 linear algebra, find the minimal polynomial $m(x) \in \mathbb{Q}[x]$ for

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

Question 2: Norms.

Prove that the norm is multiplicative, i.e., $N(ab) = N(a)N(b)$ in $\mathbb{Q}[\alpha]$ 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 in $\mathbb{C}$. Determine the minimal polynomial $m(z)$ for ω and Compute ω^{-1} in $\mathbb{Q}[z]/m(z)$ using the extended Euclidean algorithm and use this to solve the following linear system for x and y.

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

Now represent ω in Maple using the RootOf representation for algebraic numbers and solve the linear system using the `solve` command.

Question 4: Trager's algorithm

Let ω be a primitive 4th root of unity.
Using Trager's algorithm, factor $f(x) = x^5 - 1$ over $\mathbb{Q}(\omega)$.
Use Maple's RootOf notation for representing elements of $\mathbb{Q}(\omega)$ and the `gcd` command.

Study the proof of Theorem 8.16 and write out your own version of the proof.

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.