MATH 800, Assignment 6, Fall 2023

Instructor: Michael Monagan

Please hand in the assignment by 11pm Monday November 27th.
Late Penalty -20% off for up to 24 hours late. Zero after that.
Use Maple as needed for all questions.

Question 1: Minimal polynomials. [14 marks]

(a) Let $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i$. Find the minimal polynomial $m(z) \in \mathbb{Q}[z]$ for ω.
Calculate ω^3 via calculating z^3 in $\mathbb{Q}[z]/m(z)$.

(b) Using linear algebra, find the minimal polynomial $m(z) \in \mathbb{Q}[x]$ for $\alpha = 1 + \sqrt{2} + \sqrt{3}$.
Using the extended Euclidean algorithm compute the inverse of α i.e. $[z]^{-1}$ in $\mathbb{Q}[z]/(m)$.

(c) Let α be an algebraic number and $m(z)$ be a non-zero monic polynomial in $\mathbb{Q}[z]$ of least degree such that $m(\alpha) = 0$.
Prove that $m(z)$ is (i) unique and (ii) irreducible over $\mathbb{Q}$.

Question 2: Algebraic numbers in Maple. [6 marks]

Let ω be a primitive 5th root of unity in $\mathbb{C}$.

(a) What is the minimal polynomial for ω?
What is the minimal polynomial for ω^2?

(b) Consider the following linear system

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

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

(c) Consider the polynomials $a, b \in \mathbb{Q}(\omega)[x]$

$$a = x^2 + \left(\omega^3 + \omega^2 + 2\omega\right) x - \omega \quad \text{and} \quad b = x^2 + \left(-\omega^2 + \omega\right) x + \omega^2.$$

Use Maple to compute their gcd and to factor them over $\mathbb{Q}(\omega)$.

Question 3: Resultants [6 marks]

(a) For $a, b, c \in k[x]$, k a field show that $\mathrm{res}(a, b \cdot c, x) = \mathrm{res}(a, b, x) \cdot \mathrm{res}(a, c, x)$.

(b) For $a = x^4 + x^3 + x^2 + x + 1$, $b = x^2 - 2$, $c = x^2 - 3$ use Maple's resultant command to verify that $\mathrm{res}(a, b \cdot c, x) = \mathrm{res}(a, b, x) \cdot \mathrm{res}(a, c, x)$.

Question 4: Primitive elements [14 marks]

(a) Let α_1 have minimal polynomial $z_1^2 - 3$ and α_2 have minimal polynomial $z_2^2 + z_2 + 1$. Use Maple to show that $z_2^2 + z_2 + 1$ is irreducible over $\mathbb{Q}(\alpha_1)$. Hence $\dim(\mathbb{Q}(\alpha_1, \alpha_2)) = \deg(m_1, z_1) \times \deg(m_2, z_2) = 4$ and $B = [1, z_1, z_2, z_1 z_2]$ is the standard basis for the quotient ring $R = \mathbb{Q}[z_1, z_2]/\langle m_1, m_2 \rangle$.

Let $C_B : R \to \mathbb{Q}^4$ be the co-ordinate vector operation. E.g. $C_B(2 + 3z_1 + 4z_1 z_2) = [2, 3, 0, 4]^T$. Let $\gamma = z_1 + z_2$. Compute the matrix A whose ith column is $C_B(\gamma^{i-1})$. Now calculate A^{-1} and find the minimal polynomial for γ in $\mathbb{Q}[z]$.

(b) We have R is isomorphic to the quotient ring $S = \mathbb{Q}[z]/m(z)$ and let $B' = [1, z, z^2, z^3]$ be a basis for S and $C_{B'} : S \to \mathbb{Q}^4$ be the co-ordinate vector operation. Let $\phi : R \to S$ be the isomorphism and ϕ^{-1} it's inverse. We have $\phi(a) = C_{B'}^{-1}(A^{-1} C_B(a))$. Code ϕ and ϕ^{-1} in Maple as procedures `phi` and `phiinv`. Compute $\phi(z_1)$ and $\phi(z_2)$. Verify your code by checking that $\phi^{-1}(\phi(z_1)) = z_1$ and $\phi^{-1}(\phi(z_2)) = z_2$. Now use the isomorphism between R and S to compute $g = \gcd(a, b)$ in $R[x]$ for

$$
\begin{aligned}
a &= x^4 + 2x^3 z_1 + (-z_1 z_2 + 3z_2 + 1)\, x^2 + (2z_1 - 6z_2)\, x + 3z_1 z_2 + 3z_1 + 3z_2 \\
b &= x^4 z_1 - 2x^3 z_2 + (z_1 - 3z_2 - 3)\, x^2 + (-2z_1 z_2 - 2z_1 - 2z_2)\, x + 3z_1 z_2 - 3
\end{aligned}
$$

You should get $g = x^2 - z_1 z_2 + 1$. Do this two ways. First do the gcd comptuation in $R[x]$. Use Maple to do this by using RootOfs for α_1 and α_2. For the second way apply the isomorphism to do the gcd computation in $S[x]$. then invert the isomorphism to recover the gcd in $R[x]$. Use Maple for the gcd computation in $S[x]$ using a RootOf for γ. To apply ϕ to the coefficients of a in $R[x]$ use

```
> collect(a,x,phi); # maps a in R[x] to a in S[x]
```

Question 5: Trager's factorization algorithm. [10 marks]

(a) Let ω be a primitive **4**'th root of unity. Using Trager's algorithm, factor $f(x) = x^4 + x^2 + 2x + 1$ and $f(x) = x^4 + 2\omega x^3 - x^2 + 1$ over $\mathbb{Q}(\omega)$. Use Maple's RootOf notation for representing elements of $\mathbb{Q}(\omega)$ and Maple's `gcd(...)` command to compute gcds in $\mathbb{Q}(\omega)[x]$.

(b) 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. You are given that a polynomial $n(x) \in k[x]$ for any field k is square-free iff $\gcd(f(x), f'(x)) = 1$ iff $\mathrm{res}(f(x), f'(x), x) \neq 0$. Using this, find all $s \in \mathbb{Q}$ such that if $N(f(x - s\alpha))$ is NOT square-free for the two polynomials $f(x)$ in part (a).