MA3A6 WEEK 3 ASSIGNMENT : DUE MONDAY 4PM WEEK 3

BILL HART

1. Find two algebraic integers α_1 and α_2 whose sum is -3 and product is 5.

Suppose α_1 and α_2 are roots of the same quadratic polynomial. The polynomial would then be $(x-\alpha_1)(x-\alpha_2) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2 = x^2+3x+5$. Now we can solve this quadratic to find its roots, $x = (-3 \pm \sqrt{3^2 - 4*1*5})/(2*1) = (-3 \pm \sqrt{-11})/2$. As the roots are not rational numbers, the minimum polynomial cannot have degree 1, thus the quadratic polynomial given must be the minimum polynomial. As it is monic with integer coefficients, the roots are algebraic integers.

2. Find the minimum polynomial of the sum of two roots (it doesn't matter which two) of $x^3 - 5x^2 + 2x - 1$. Hint: there may be a link between this and the method you used in the previous question.

The hint suggests we try to use the expression for the coefficients of a polynomial in terms of symmetric combinations of its roots.

For a monic cubic polynomial with roots $\alpha_1, \alpha_2, \alpha_3$ we get the polynomial $x^3 - a_1x^2 + a_2x + a3$ where $a_1 = \alpha_1+\alpha_2+\alpha_3$, $a_2 = \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3$ and $a_3 = \alpha_1\alpha_2\alpha_3$.

We'd like to write the coefficients of the polynomial we are after in terms of the coefficients of the original polynomial. But the latter are symmetric combinations of the roots, and thus the former will be too.

We want $\beta_1 = \alpha_1 + \alpha_2$ say, to be one of the roots of the polynomial we are after. To make the coefficients of the polynomial we are after symmetric in $\alpha_1, \alpha_2, \alpha_3$, we had better make the other two roots of the polynomial we are after $\beta_2 = \alpha_1 + \alpha_3$ and $\beta_3 = \alpha_2 + \alpha_3$.

Thus the a_1 coefficient of the polynomial we are after will be $\beta_1 + \beta_2 + \beta_3 = 2\alpha_1 + 2\alpha_2 + 2\alpha_3 = 2*5 = 10$ (the 5 here is the a_1 coefficient of the original polynomial, which is $\alpha_1 + \alpha_2 + \alpha_3$.

The a_2 coefficient of the polynomial we are after will be $\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = \alpha_1^2+\alpha_2^2+\alpha_3^2+3(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = (\alpha_1+\alpha_2+\alpha_3)^2+(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = 5^2+2 = 27$.

Finally the a_3 coefficient of the polynomial we are after will be $\beta_1\beta_2\beta_3 = \alpha_1^2\alpha_2 + \alpha_1^2\alpha 3 + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_1\alpha_2^2 + \alpha_1\alpha_2\alpha_3 + \alpha_2^2\alpha_3\alpha_2\alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3+\alpha_2\alpha_3) - \alpha_1\alpha_2\alpha_3 = 5*2-1 = 9$.

So the minimum polynomial we are after is $x^3 - 10x^2 + 27x - 9$.

3. Find the ring of integers of $\mathbb{Q}(\zeta_3)$ where ζ_3 is a root of $x^3 - 1$ with $\zeta_3 \neq 1$. (Proof required).

$x^3 - 1 = (x-1)(x^2+x+1)$. A root of this which is not 1 must be a root of the quadratic factor. But the discriminant of this is -3. So we want the ring of integers of $\mathbb{Q}(\sqrt{-3})$. We note that -3 is squarefree and is 1 modulo 4, thus it is a fundamental discriminant, and we know from the proof given in the lectures that the ring of integers is $\mathbb{Z}[(1+\sqrt{-3})/2]$.

4. Find the first 15 negative fundamental discriminants.

We only need to consider values that are 0 or 1 mod 4 and square free (except for a factor of 4).

-3 (see above)

-4 (4*-1 and -1 is 3 mod 4 and squarefree)

-7 (1 mod 4, squarefree)

-8 (4*-2 and -2 is 2 mod 4 and squarefree)

-11 (1 mod 4, squarefree)

-15 (1 mod 4, squarefree)

-19 (1 mod 4, squarefree)

-20 (4*-5 and -5 is 3 mod 4 and squarefree)

-23 (1 mod 4, squarefree)

-24 (4*-6 and -6 is 2 mod 4 and squarefree)

-31 (1 mod 4, squarefree)

-35 (1 mod 4, squarefree)

-39 (1 mod 4, squarefree)

-40 (4*-10 and -10 is 2 mod 4)

-43 (1 mod 4, squarefree)

Revision Exercises (you do not need to hand these in):

Solns will be provided to these some time after Feb 12th to give you plenty of time to work through them.

1. Use the Euclidean algorithm to find the greatest common divisor of $f(x) = x^3 + 3x^2 - 2$ and $g(x) = x^4 + x^3 + x^2 - 1$. Check your answer by checking that the gcd divides both of the original polynomials.

2. How many real and how many complex roots does $x^3 - 3x^2 + 2x + 1$ have. For those who are really inspired, look up Descarte's law of signs and interval arithmetic and see if either of those help.

3. Find all of the roots modulo 3 of $x^3 - 3x^2 + 2x + 3$, i.e. reduce the coefficients modulo 3 and look for roots in $\mathbb{Z}/3\mathbb{Z}$.

4. Factor $x^5 + 3x^4 + x^3 - x^2 - 3x - 1$ modulo 2.

5. Prove that $\mathbb{Z}/3\mathbb{Z}$ is a field and $\mathbb{Z}/6\mathbb{Z}$ is not.

E-mail address: hart_wb@yahoo.com