MA3A6 WEEK 4 ASSIGNMENT : DUE MONDAY 4PM WEEK 4

BILL HART

1. Find a single generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. What degree is the resulting number field?

$K = \mathbb{Q}(\sqrt{2})$ is a degree 2 number field and we are adjoining $\sqrt{3}$ to it. This cannot give us more than a degree 4 extension of $\mathbb{Q}$ (see the final solution below for hint as to how to prove this). Thus we just need to look for an element in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ of degree 4 and it must then be a generator. We can easily guess such an element and check it has the required degree.

Alternatively, if we examine the proof of the theorem which tells us that a number field has a single generator, we see that it explicitly tells us how to construct a generator. In particular we could choose $\sqrt{2} + \sqrt{3}$ as a generator (there is only a finite number of things to check to ensure that this generator is ok).

We can easily compute the degree of $a = \sqrt{2} + \sqrt{3}$ by computing its minimum polynomial. $a^2 = 2 + 3 + 2\sqrt{6}$, i.e. $(a^2 - 5)^2 = 24$, i.e. $a^4 - 10a^2 + 1 = 0$. We easily check that $f(x) = x^4 - 10x^2 + 1$ does not factor over $\mathbb{Q}$, thus it is the minimum polynomial of our generator, and thus the degree is 4.

2. Determine if $\mathbb{Q}(\alpha)$ is Galois if α is a root of $f(x) = x^3 - 3x^2 + 2x + 1$.

We compute the derivative $f'(x) = 3x^2 - 6x + 2$. This has zeroes at $(3 \pm \sqrt{3})/3$. At both these turning points, $f(x)$ is positive. Plotting the graph of $f(x)$ one sees that it starts below the axis, crosses the axis, passes through a turning point, heads back down to the axis, but before it gets there, turns again and heads up. Thus there is only a single real zero.

If α is this real zero, then $\mathbb{Q}(\alpha)$ contains only real numbers. The other two roots of $f(x)$ are complex however, so cannot be in $\mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\alpha)$ cannot be Galois.

3. Let α be a root of $f(x) = x^3 - 3x^2 + 2x + 1$. Write each of the following in the form $a_1\alpha^2 + a_2\alpha + a_3, \ \text{ for } \ a_i \in \mathbb{Q}$

(i) $\frac{1}{\alpha - 1}$

We have $\alpha^3 - 3\alpha^2 + 2\alpha + 1 = 0$. Thus $(\alpha - 1)(\alpha^2 - 2\alpha) = -1$. Thus $1/(\alpha - 1) = -\alpha^2 + 2\alpha$.

(ii) $\frac{\alpha^2 - 1}{\alpha}$

We have $\alpha^3 - 3\alpha^2 + 2\alpha + 1 = 0$, thus $\alpha(\alpha^2 - 3\alpha + 2) = -1$, thus $1/\alpha = -\alpha^2 + 3\alpha - 2$.

Therefore $\frac{\alpha^2 - 1}{\alpha} = (\alpha^2 - 1)(-\alpha^2 + 3\alpha - 2) = -\alpha^4 + 3\alpha^3 - \alpha^2 - 3\alpha + 2$.

We can replace α^3 with $3\alpha^2 - 2\alpha - 1$. Then $\alpha^4 = \alpha(3\alpha^2 - 2\alpha - 1) = 3\alpha^3 - 2\alpha^2 - \alpha = 3(3\alpha^2 - 2\alpha - 1) - 2\alpha^2 - \alpha = 7\alpha^2 - 7\alpha - 3$.

Thus $\frac{\alpha^2 - 1}{\alpha} = -7\alpha^2 + 7\alpha + 3 + 3(3\alpha^2 - 2\alpha - 1) - \alpha^2 - 3\alpha + 2 = \alpha^2 - 2\alpha + 2$.

(iii) $\alpha^4 + \alpha^2 + 1$.

We already computed that $\alpha^4 = 7\alpha^2 - 7\alpha - 3$, so we get $8\alpha^2 - 7\alpha - 2$.

4. Prove that if $K = \mathbb{Q}(\alpha)$ is a degree n number field then for any $\beta \in K$, the degree of β divides n.

$\mathbb{Q}(\beta)$ is a vector space over $\mathbb{Q}$ of degree m_1 say. Let $\{s_1, s_2, \ldots, s_{m_1}\}$ be a basis.

But $\beta \in K$, thus $\mathbb{Q}(\beta)$ is contained in $\mathbb{Q}(\alpha)$ meaning that K is a field extension of $\mathbb{Q}(\beta)$. Thus it is a vector space over $\mathbb{Q}(\beta)$ of dimension m_2 say. Let $\{t_1, t_2, \ldots, t_{m_2}\}$ be a basis.

Clearly $\{s_1t_1, s_1t_2, \ldots, s_{m_1}t_{m_2}\}$ is a basis of K/Q. But this is a dimension n vector space over $\mathbb{Q}$, thus $m_1m_2 = n$, i.e. $m_1|n$. However $\mathbb{Q}(\beta)$ is a dimension m_1 vector space over $\mathbb{Q}$. But the dimension m_1 is also the degree of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$ (and the degree of β), thus the degree of β divides n.

E-mail address: hart_wb@yahoo.com