Math 113 **Fall 2015**

Homework #13

Nikhil Unni

1. In this problem, we will build an algebraic extension of $\mathbb{Q}$ in a couple differet ways.

   (a) Let $\mathbb{Q}$ be our base field. Build the extension $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ (i.e. the smallest field containing $\mathbb{Q}, \sqrt{5}$, and $\sqrt{7}$) in two steps: first a simple extension field to add in $\sqrt{5}$, and then another simple extension to add in $\sqrt{7}$ to the result. Give a basis for the overall extension from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{5}, \sqrt{7})$, as in the proof of Theorem 31.4.

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} | a, b \in \mathbb{Q}$$
$$\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \{a + b\sqrt{7} | a, b \in \mathbb{Q}(\sqrt{5})\}$$
$$= \{a + b\sqrt{7} + c\sqrt{5} + d\sqrt{35} | a, b \in \mathbb{Q}\}$$

   As shown in the proof of Theorem 31.4, the basis of the entire "tower" is the product (in the sense of every element is multiplied by every other element) of the individual bases in the chain. So from this, the basis of $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ is $\{1, \sqrt{5}\} \times \{1, \sqrt{7}\} = \{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$.

   (b) Next, find the irreducible polynomial $irr(\sqrt{5} - \sqrt{7}, \mathbb{Q})$. Verify that your polynomial is irreducible over $\mathbb{Q}$. Find the obvious basis for $\mathbb{Q}(\sqrt{5} - \sqrt{7})$ over $\mathbb{Q}$.

$$x = \sqrt{5} - \sqrt{7}$$
$$x^2 = 12 - 2\sqrt{35}$$
$$(x^2 - 12)^2 = (-2\sqrt{35})^2$$
$$x^4 - 24x^2 + 144 = 140$$
$$x^4 - 24x^2 + 4 = 0$$

   So we have a valid polynomial where $\sqrt{5} - \sqrt{7}$ is a solution. Now we have to show that the polynomial is indeed irreducible over $\mathbb{Q}$.
   From the Rational Root Theorem, we know that rational roots of a

polynomial must be of the form $\frac{p}{q}$, where the possible values of p are all the integer factors of the constant term, and the possible values of q are all the integers of the highest power coefficient. This means:

$$x = \frac{\{1, 2, 4\}}{\{1\}}$$

But plugging in the values of $1, 2, 4$ into our polynomial, we don't get 0, so there cannot be any roots for our polynomial in $\mathbb{Q}$, meaning we cannot decompose the polynomial into degree 1 and degree 3 terms. But let's suppose that you could decompose it into two degree 2 polynomials. You'd end up with:

$$(ax^2 + bx + c)(dx^2 + ex + f)$$

We know that both $a, d = 1$, since the power 4 term has a coefficient of 1. Similarly, we know that $cf = 4$, so $c, f = 2, 2$ or $c, f = 1, 4$ (the order doesn't matter since they're symmetrical so far). Another thing to note is that there are no degree 3 terms – meaning that $ae + bd = 0$, or $e + b = 0$.
So far, we have either $(x^2 + bx + 2)(x^2 + ex + 2)$ or $(x^2 + bx + 4)(x^2 + ex + 1)$, where $e + b = 0$. To reconstruct the degree 2 term, we must sum all the products of monomials that could lead to a degree 2 term, and that coefficient should be -24. Either:

$$2 + 2 + be = -24$$

or

$$1 + 4 + be = -24$$

So we have either $be = -28$, or $be = -29$. Since b and e are additive inverses, we really just have $b^2 = 28$ or $b^2 = 29$ (or we could use e^2, it doesn't matter). But 29 is prime, so we cannot have $\sqrt{29}$ in $\mathbb{Q}$. Similarly $\sqrt{28} = 2\sqrt{7}$, which is also not in $\mathbb{Q}$. Thus, it is not possible for there to be a decomposition of our polynomial into two degree 2 polynomials.

Because we cannot decompose $x^4 - 24x^2 + 4$ into either a degree 1 and degree 3 or a degree 2 and a degree 2, it is irreducible in $\mathbb{Q}$.

So we know that $\sqrt{5} - \sqrt{7}$ has degree 4 over $\mathbb{Q}$. We get the basis of our extension field over F from the roots of the polynomial. $\sqrt{5} - \sqrt{7}$ is one solution, and $\sqrt{5} + \sqrt{7}$ is another solution. The other two solutions are just negations of these two. So we can let the basis of $\mathbb{Q}(\sqrt{5} - \sqrt{7})$ over $\mathbb{Q}$ be $\{1, \sqrt{5} - \sqrt{7}, \sqrt{5} + \sqrt{7}, \sqrt{35}\}$

(c) Finally, show that the two extension fields you build in parts (a) and (b) are actually the same by using linear algebra – show that every element in the (a) basis can be written as a $\mathbb{Q}$-linear combination of elementsi n the (b) basis and vice versa.

We can show that there is a linear mapping between the two bases both ways with:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & -0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{5}-\sqrt{7} \\ \sqrt{5}+\sqrt{7} \\ \sqrt{35} \end{pmatrix} = \begin{pmatrix} 1 \\ \sqrt{5} \\ \sqrt{7} \\ \sqrt{35} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{5} \\ \sqrt{7} \\ \sqrt{35} \end{pmatrix} = \begin{pmatrix} 1 \\ \sqrt{5}-\sqrt{7} \\ \sqrt{5}+\sqrt{7} \\ \sqrt{35} \end{pmatrix}$$

In general though, even without calculating the mappings between the bases, we know from linear algebra that since we have two vector spaces over the same field, and the two vector spaces have the same dimension (we showed that $\mathbb{Q}(\sqrt{5}-\sqrt{7})$ has dimension 4 in part (b)), that the two vector spaces must be the same. This means that there **has** to exist a linear mapping between the two bases.

2. What degree field extensions can we obtain by successively adjoining to a field F a square root of an element of F not a square in F, then square root of some nonsquare in this new field, and so on? Argue from this that a zero of $x^{14}-3x^2+12$ over $\mathbb{Q}$ can never be expressed as a rational function of square roots of rational functions of square roots, and so on, of elements of $\mathbb{Q}$.

Every time we add a new extension on a square root of an nonsquare element of F, we have a degree 2 extension, as showed in previous problems. So if we had n of these extensions, the degree of the extension we'll obtain has degree 2^n.

With $p=3$, $x^{14}-3x^2+12$ is irreducible over $\mathbb{Q}$ by the Eisenstein Criteria. So by Theorem 29.18, we know that the degree of some α root of our polynomial over $\mathbb{Q}$ is 14. But there is no way to get a power 2 degree with multiples of 14, so we know that there is no possible way to extend F with square roots to solve this polynomial. (We need a seventh-root number

for the extension, perhaps.)

3. Let E be an extension field of F. Let $\alpha \in E$ be algebraic of odd degree over F. Show that α^2 is algebraic of odd degree over F, and $F(\alpha) = F(\alpha^2)$.

   Suppose that $F(\alpha) \neq F(\alpha^2)$. Then, we get a tower of field of extensions – from F to $F(\alpha^2)$ to $F(\alpha)$. As we showed in the previous problems, an extension on a squareroot of a nonsquare element is a degree 2 extension. So we know that $F(\alpha)$ is a degree 2 extension field over $F(\alpha^2)$. But this cannot be, since $F(\alpha)$ is an odd degree extension of F, and by the chain rule of field extensions, the degree of $F(\alpha)$ in this scheme would be $2x$, $x \in \mathbb{Z}$, which cannot be an odd number.

   This shows that $\alpha^2 \in F(\alpha)$, and that $F(\alpha) = F(\alpha^2)$. This means that $F(\alpha^2)$ is an odd degree extension over F, and therefore α^2 is algebraic of odd degree over F (since all finite extensions are algebraic).