MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 11
Model Solutions

Basic Questions

1. *Calculate the dimension of $Q[\sqrt[5]{7}]$ as a vector space over Q.*

   A basis for this vector space is $\{1, \sqrt[5]{7}, \sqrt[5]{7^2}, \sqrt[5]{7^3}, \sqrt[5]{7^4}\}$, so the dimension is 5.

2. *Give a basis of $Q[\frac{1}{2} + \frac{\sqrt{3}}{2}i]$ over Q.*

   One basis is $\{1, \sqrt{3}i\}$.

3. *What is $\mathrm{Irr}(\sqrt{3+\sqrt[3]{3}}, \mathbb{Q})$?*

   Let $t = \sqrt{3+\sqrt[3]{3}}$. Let $s = t^2 = 3 + \sqrt[3]{3}$. We get that $(s-3)^3 = 3$, so that $(s-3)^3 - 3 = 0$. So s is a zero of $x^3 - 9x^2 + 27x - 30$, and t is a zero of $x^6 - 9x^4 + 27x^2 - 30$. This is irreducible over $\mathbb{Z}$ by Eisenstein's criterion with $p = 3$, and therefore irreducible over $\mathbb{Q}$. Therefore, this polynomial is $\mathrm{Irr}(\sqrt{3+\sqrt[3]{3}}, \mathbb{Q})$.

4. *The polynomial $f(x) = x^2 + 2x + 2$ is irreducible over $\mathbb{Z}_3$. Let α be a zero of f, and factorise f over $\mathbb{Z}_3(\alpha)$. [Hint: use long division.]*

   We know that $(x - \alpha)$ is a factor of f in $\mathbb{Z}_3(\alpha)$. Applying long division, we get $f(x) = (x-\alpha)(x+\alpha+2)$. [So the other zero of f is $1 + 2\alpha$.

5. *Let α be a zero of $f(x) = x^3 + x + 1$ over $\mathbb{Z}_2$. Compute the multiplication table of $\mathbb{Z}_2(\alpha)$. [Hint: $\mathbb{Z}_2(\alpha)$ has 8 elements: 0, 1, α, $\alpha+1$, α^2, α^2+1, $\alpha^2+\alpha$, and $\alpha^2+\alpha+1$.]*

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Theoretical Questions

5. *Let V be a vector space of dimension n over a field F.*

   (a) Show that if $v_1, \ldots, v_n$ is a linearly independent set, then it is a basis.

   We know that any linearly independent set extends to a basis. Therefore, we can extend $v_1, \ldots, v_n$ to a basis $\{v_1, \ldots, v_n, w_1, \ldots, w_k\}$. Since V has dimension n, this basis has cardinality n, so we must have $k = 0$, i.e. $\{v_1, \ldots, v_n\}$ is a basis.

   (b) Show that if $v_1, \ldots, v_n$ is a spanning set, then it is a basis.

   If $\{v_1, \ldots, v_n\}$ is a linearly independent set, then it must be a basis. Suppose it is not linearly independent, then we can take a maximal linearly independent subset $\{v_{i_1}, \ldots, v_{i_k}\}$. We claim that this is a spanning set, and therefore, a basis. Let $x \in V$ be any vector. We know that x is a linear combination $\lambda_1 v_1 + \cdots + \lambda_n v_n$. Now for any $v_j \notin \{v_{i_1}, \ldots, v_{i_k}\}$, we know that $\{v_j, v_{i_1}, \ldots, v_{i_k}\}$ is not linearly independent (by maximality). This means that we have some $\alpha v_j + \beta_1 v_{i_1} + \cdots + \beta_k v_{i_k} = 0$. If $\alpha = 0$, then we have a contradiction to the assumption that $\{v_{i_1}, \ldots, v_{i_k}\}$ is linearly independent. Therefore $\alpha \neq 0$, and since F is a field, this means that α has an inverse. We therefore get $v_j = -\alpha^{-1}\beta_1 v_{i_1} - \cdots - \alpha^{-1}\beta_k v_{i_k}$, so v_j is a linear combination of $\{v_{i_1}, \ldots, v_{i_k}\}$. Therefore, replacing each v_j by this linear combination, we can express x as a linear combination of $\{v_{i_1}, \ldots, v_{i_k}\}$. This proves that $\{v_{i_1}, \ldots, v_{i_k}\}$ is a basis, so $k = n$. Therefore, $\{v_1, \ldots, v_n\}$ is a basis.

6. *If F is a finite field with q elements, and V is a vector space of dimension d over F, show that V has q^d elements.*

   Let $\{v_1, \ldots, v_d\}$ be a basis for V over F. The elements of F are uniquely represented in the form $\lambda_1 v_1 + \cdots + \lambda_d v_d$, where each $\lambda_i \in F$, so there are q possibilities for each λ_i. Therefore the total number of elements is q^d.

7. *Show that if E is a finite extension field of F, and if $[E : F]$ is prime, then E is a simple extension of F. [Hint: in fact $E = F(\alpha)$ for any α in $E \setminus F$.]*

   Let $\alpha \in E \setminus F$. We know that $[E : F] = [E : F(\alpha)][F(\alpha) : F]$. Since $[E : F]$ is prime, one of $[E : F(\alpha)]$ and $[F(\alpha) : F]$ must be 1. Since $\alpha \notin F$, we can't have $[F(\alpha) : F] = 1$, so we must have $[E : F(\alpha)] = 1$. This means that $E = F(\alpha)$ is a simple extension of F.

8. *Let F be a field, let $F(\alpha)$ be algebraic over F, and let $[F(\alpha) : F]$ be odd. Show that $F(\alpha^2) = F(\alpha)$.*

   Since $\alpha^2 \in F(\alpha)$, we know that $F(\alpha^2)$ is a subfield of $F(\alpha)$. Furthermore, it is easy to see that $\{1, \alpha\}$ is a spanning set for $F(\alpha)$ over $F(\alpha^2)$, so $[F(\alpha) : F(\alpha^2)] \leqslant 2$. Since $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$ is odd, so is $[F(\alpha) : F(\alpha)]$, so it must be 1, i.e. $F(\alpha) = F(\alpha^2)$.