Homework 21 - MATH 791

Will Thomas

Problem 1:
Prove that 1, $\sqrt[3]{2}$, $\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ are linearly independent over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
Solution:
Let us start with 1, $\sqrt[3]{2}$ and assume for contradiction that they are not linearly independent.
That would mean that $\exists \lambda_1, \lambda_2 \in \mathbb{Q}$ such that $\lambda_1 * 1 + \lambda_2 * \sqrt[3]{2} = 0$. We can reduce this to $\lambda_1 + \lambda_2 * \sqrt[3]{2} = 0$, and since both $\lambda_1, \lambda_2 \in \mathbb{Q}$, we can factor out λ_2 from both to get.

$$\lambda_2 * (\lambda_1' + \sqrt[3]{2}) = 0$$

$$\implies \sqrt[3]{2} = -\lambda_1' \implies 2 = -(\lambda_1')^3$$

This would mean that there exists a $\lambda_1' \in \mathbb{Q}, \lambda_1' = \sqrt[3]{-2}$ which is a contradiction.

$$\therefore 1, \sqrt[3]{2} \text{ are linearly independent}$$

A very similar argument can be made when adding $\sqrt[3]{4}$ to the mix

$$\therefore 1, \sqrt[3]{2}, \sqrt[3]{4} \text{ are linearly independent over } \mathbb{Q}$$

Now to conclude that $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, we need only realize that any element in $\mathbb{Q}[\sqrt[3]{2}]$ can be made of 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$. Thus the degree of $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$ is 3.

Problem 2:
Find the multiplicative inverse of $1 + 2\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$.
Solution:
The multiplicative inverse will be $(x + y\sqrt[3]{2} + z\sqrt[3]{4})$ such that

$$(1 + 2\sqrt[3]{2})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = 1$$

$$\implies (x + 4z) + (y + 2x)\sqrt[3]{2} + (z + 2y)\sqrt[3]{4} = 1$$

We could solve this via

$$\begin{pmatrix} 1 & 0 & 4 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & \frac{1}{17} \\ 0 & 1 & 0 & -\frac{2}{17} \\ 0 & 0 & 1 & \frac{4}{17} \end{pmatrix}$$

Thus the inverse element is $(\frac{1}{17} - \frac{2}{17}\sqrt[3]{2} + \frac{4}{17}\sqrt[3]{4})$

Problem 3:
Can you write down the multiplicative inverse of $1+\sqrt[3]{2}+\sqrt[3]{4}$ in $\mathbb{Q}(\sqrt[3]{2})$ without doing any calculations?
Solution:
No I cannot, how am I supposed to without calculations.
Using calculations, we see $(x+2y+2z)+(x+y+2z)\sqrt[3]{2}+(x+y+z)\sqrt[3]{4}=1$.

$$\begin{pmatrix}1 & 2 & 2 & 1\\ 1 & 1 & 1 & 0\\ 1 & 1 & 1 & 0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1 & 0 & 0 & -1\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

Thus, the inverse is $(-1+1\sqrt[3]{2})$

Problem 4:
Let $F := \mathbb{Q}(\sqrt{2})$. Define $K := F(\sqrt{3})$ to be the set $\{a+b\sqrt{3} \mid a,b \in F\}$. Show that $[K:F]=2$. Can you guess $[K:\mathbb{Q}]$? If so, give a proof validating your guess.
Solution:
I would guess that $[K:\mathbb{Q}]=4$. This is because $\dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}} F(\sqrt{3})$ And
$F := \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, so
$F(\sqrt{3}) := \{a+b\sqrt{3} \mid a,b \in F\} = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$ To find a basis for this in $\mathbb{Q}$, we need the elements $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

$$\therefore [K:\mathbb{Q}]=4$$

Problem 5:
Let $p(x)=x^2+x+1 \in \mathbb{Z}_2[x]$.

(i) Show that $p(x)$ is irreducible over $\mathbb{Z}_2$.

(ii) Show the the commutative ring $\mathbb{Z}_2[x]/\langle p(x)\rangle$ has just four elements.

(iii) Prove that the ring $\mathbb{Z}_2[x]/\langle p(x)\rangle$ is a field.

Solution:

(i) Let us assume it can be reduced $p(x)=f(x)g(x)$ and neither f,g are units. So $deg(f(x)), deg(g(x))=1$. Additionally, we know that both $f(x)$ and $g(x)$ must have a constant term 1, since $p(x)$ has a constant term 1. So $f(x)=\alpha x+1$ and $g(x)=\beta x+1$ $f(x)g(x)=\alpha\beta x^2+(\alpha+\beta)x+1$ We know that $\alpha\beta=1$, and since we are in $\mathbb{Z}_2$, that means $\alpha=\beta=1$. However, this would cause the x term to be $2x \equiv 0x$ which is not allow.

$$\therefore p(x) \text{ is irreducible}$$

(ii) Let us try to enumerate the possible elements of $F := \mathbb{Z}_2[x]/\langle p(x) \rangle$. We know that for every power of x, the coefficient is either 0 or 1, since we are in $\mathbb{Z}_2$. We can find the following elements in F: $\{1, x, x+1, x^2+1, x^2+x\}$. Any other element will be canceled out be the quotient $\langle p(x) \rangle$. To demonstrate this, take an element $z = a_n x^n + \cdots + a_0$ for $n \geq 3$. If $a_n = 1$ then take out $z' = z - p(x) * x^{n-2} = (a_{n-1} - 1)x^{n-1} + \cdots + a_0$. Repeat this process until $n = 2$. At which point either $z' = p(x)$, in which case it has been canceled out, or $z' \in$ out previously laid out elements.

Admitted

(iii) To show that it is a field, we need to show primarily the multiplicative inverse property. The other properties are inherited from (ii) stating that $\mathbb{Z}_2/\langle p(x) \rangle$ is a commutative ring. Given the elements in F, we can find a multiplicative inverse for each.

(a) 1 is its own inverse

(b) $x * (x^2 + 1) = x^3 + x \equiv$

Admitted