HW 5 Solutions MATH1250

#4 Let $\alpha = \sqrt{1+\sqrt[3]{2}}$. Then $\alpha^2 = 1+\sqrt[3]{2}$, so $\alpha^2 - 1 = \sqrt[3]{2}$, $(\alpha^2-1)^3 = 2$. Thus α is a root of $(\alpha^2-1)^3 - 2 = \alpha^6 - 3\alpha^4 + 3\alpha^2 - 3 = 0$.

#18 (a) Let $f(x) = x^2 + 1$. Then $f(0) = 1$, $f(1) = 2$ and $f(-1) = 2$. So $f(x)$ is cubic with no zeros in $\mathbb{Z}_3$ and thus is irr. in $\mathbb{Z}_3[x]$.

#25 (a)

Let $f(x) = x^3 + x^2 + 1$. Then $f(0) = 1$, $f(1) = 1$, so $f(x)$ has no zeros in $\mathbb{Z}_2$ and is thus irreducible over $\mathbb{Z}_2$.

(b) The long div. uses the relations $\alpha^3 = \alpha^2 + 1$ and $-\alpha^3 - \alpha^2 = -\alpha^2 - 1 - \alpha^2 = -1$.

$$
\begin{array}{r|l}
X-\alpha & x^2 + (1+\alpha)x + (\alpha^2+\alpha) \\
\hline
 & x^3 + x^2 + 1 \\
 & x^3 - \alpha x^2 \\
\hline
 & (1+\alpha)x^2 \\
 & (1+\alpha)x^2 - (\alpha^2+\alpha)x \\
\hline
 & (\alpha^2+\alpha)x + 1 \\
 & (\alpha^2+\alpha)x - 1 \\
\hline
 & 0
\end{array}
$$

Continuing we try α^2 as a zero of $q(x) = x^2 + (1+\alpha)x + (\alpha^2+\alpha)$. Subsitituting

We obtain:

$$\alpha^4+(1+\alpha)\alpha^2+(\alpha^2+\alpha) = \cdots = 2(\alpha^2+1)+2\cdot\alpha^2+2\cdot\alpha = 0.$$

So α^2 is a zero of $q(x)$. We do another long div. noting:

$$\alpha^2(\alpha^2+\alpha+1) = \alpha^2+\alpha.$$

$$\begin{array}{r|l} & x+(\alpha^2+\alpha+1) \\ \hline x-\alpha^2 & x^2+(1+\alpha)x+\alpha^2+\alpha \\ & x^2-\alpha^2 x \\ \hline & (\alpha^2+\alpha+1)x+(\alpha^2+\alpha)x \\ & (\alpha^2+\alpha+1)x+(\alpha^2+\alpha)x \\ \hline & 0 \end{array}$$

Thus in $\mathbb{Z}_2(\alpha)[x]$: $x^3+x^2+1 = (x-\alpha)(x-\alpha^2)(x-(\alpha^2+\alpha+1))$.

#36 Suppose F has m elements. Then $F^* = F\setminus\{0\}$ has $m-1$ elements. Because the order of an element of a finite group divides the order of the group we see that $\forall a \in F^*$ (multi. gp. of F) we have $a^{m-1}-1=0$. Thus every $a\in F^*$ is a root of $x^{m-1}-1=0$. Clearly 0 is a root of x. Thus every $a\in F$ is alg. over the prime field $\mathbb{Z}_p$ of F ($p=$ char. of F). Note that every finite field has char $=p>0$.

#37 Let E be a finite field with prime subfield $\mathbb{Z}_p$. Take a ver. space basis $\{\alpha_1,\cdots,\alpha_n\}$ for E over $\mathbb{Z}_p$, where $n=[E:\mathbb{Z}_p]$.

Then every $\alpha \in E$ can be uniquely represented as

$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for $a_i \in \mathbb{Z}_p$. Since there are p choices for each a_i, in total there are p^n choices for α & hence $|E| = p^n$.