HW4 Solutions

#1 $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1 = \dfrac{x^6 - 1}{x - 1}$.

As discussed in class the Complex roots are $\omega_k = e^{2\pi i\, k/6}$

$k = 1, \ldots, 5$. ($k=0$ corr. to $e^{2\pi i\, 0/6} = e^0 = 1$). Thus: $f(x) = \prod_{k=1}^{5} (x - e^{\frac{2\pi i k}{6}})$

This gives factorization into irr. factors over $\mathbb{C}$.

As for factorization over $\mathbb{Q}$, remember from lecture that cyclotomic poly. for $n=6$ is $\Phi_6(x) = \prod_{(k,6)=1} (x - e^{\frac{2\pi i k}{6}})$ which is irr. over $\mathbb{Q}$.

$$= (x - e^{2\pi i \cdot 1/6})(x - e^{2\pi i\, 5/6}) = (x - \omega_1)(x - \tfrac{1}{\omega_1}) = x^2 - (\omega_1 + \tfrac{1}{\omega_1})x + 1.$$

Note $\omega_1 = \cos(2\pi/6) + i \sin(\frac{2\pi}{6}) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\omega_5 = \frac{1}{\omega_1} = \cos(\frac{-2\pi}{6}) + i \sin(\frac{-2\pi}{6})$.

$$\Rightarrow \frac{1}{\omega_1} = \frac{1}{2} - i\frac{\sqrt{3}}{2} \Rightarrow \omega_1 + \frac{1}{\omega_1} = \frac{1}{2} + \frac{1}{2} = 1 \Rightarrow \Phi_6(x) = x^2 - x + 1.$$

Dividing $f(x)$ by $\Phi_6(x)$ we obtain:

$$x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 - x + 1)(x^3 + 2x^2 + 2x + 1).$$

Note $\omega_3 = \omega_1^3 = -1$ is root of $x^3 + 2x^2 + 2x + 1$ & hence $x^3 + 2x^2 + 2x + 1$ div. by $(x+1)$. By long div. We have:

$x^3 + 2x^2 + 2x + 1 = (x+1)(x^2 + x + 1)$. It is easy to verify that $x^2 - x + 1$ and $x^2 + x + 1$ are irr. over $\mathbb{Q}$ as they don't have any rat. roots. So $x^5 + x^4 + x^3 + x^2 + x + 1 = (x^2 - x + 1)(x^2 + x + 1)(x + 1)$

#2 Suppose $f(x) = g(x)h(x)$ where $f, g \in F[x]$ and $h \in E[x]$. We would like to show $h \in F[x]$.

Lets apply the division alg. Thm. for the ring of Poly. $F[x]$ & $f, g \in F[x]$.

We obtain $\exists h' \in F[x]$ and $r \in F[x]$ with $\deg r < \deg g$ or $r = 0$ s.t. $f = gh' + r$. But $gh' + r = gh$ in $E[x]$. It follows that $r = g(h - h')$ & hence r is div. by g as poly. in $E[x]$.

If $r \neq 0$, $\deg r < \deg g$ & hence r cannot be div. by g. So $r = 0 \Rightarrow h - h' = 0 \Rightarrow h = h' \in F[x]$ as required ☺

(There are other sol. too e.g. you can just use def. of product of poly. and show by induction that all the coeff. of h should lie in F.)

Sec. 26

#34 Let $a, b \in N \Rightarrow \exists m, n$, $a^m \in N$ & $b^n \in N$. Now $(a+b)^{m+n} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{m+n-i}$ (Since R is Commutative). From $a^m \in N$ and $b^n \in N$ and the fact that N is an ideal it follows that $\forall\, 0 \leq i \leq n+m$, $a^i b^{m+n-i} \in N$

(because if $0 \leqslant i \leqslant n+m$ then either $n \leqslant i$ or $0 \leqslant i < n$ which implies $m < m+n-i$, hence $a^i \in N$ or $b^{n+m-i} \in N$) $\Rightarrow (a+b)^{n+m} \in N$.

Also $\forall x \in R$, $(xa)^m = x^m a^m \in N$ since $a^m \in N \Rightarrow xa \in \sqrt{N}$.

Finally $0 \in N \Rightarrow 0 \in \sqrt{N}$.

It follows that $\sqrt{N}$ is an ideal.

\# 37 We have:

$$\phi\big((a+bi)+(c+di)\big) = \phi\big((a+c)+(d+b)i\big) = \begin{bmatrix} a+c & b+d \\ -b-d & a+c \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi(a+bi) + \phi(c+di).$$

$$\phi\big((a+bi)(c+di)\big) = \phi\big((ac-bd)+(ad+bc)i\big) = \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi\big((a+bi)(c+di)\big).$$

Thus ϕ is a homo$^{\underline{\text{ism}}}$. It is obvious that ϕ is one-to-one. Hence ϕ gives an iso$^{\underline{\text{ism}}}$ of $\mathbb{C}$ with the subring $\phi(\mathbb{C})$ which therefore must be a field.

Sec. 27

#8 Let us evaluate $f(x) = x^2 + x$ at all $a \in \mathbb{Z}_5$:

$f(0)=0$, $f(1)=2$, $f(2)=1$, $f(3)=2$, $f(4)=0$.

Thus x^2+x+c has root for $c=-2=3$, $c=0$ and $c=-1=4$.

Hence x^2+x+c is red. for $c=0,3,4$ and irr. for $c=1,2$ (because

$\deg(x^2+x+c)=2$ & hence it is reducible $\Leftrightarrow$ it has a root).

Now by Thm. 27.25 and Thm. 27.9, $\mathbb{Z}_5[x]/\langle x^2+x+c\rangle$ is a field

$\Leftrightarrow$ x^2+x+c is irr. $\Leftrightarrow$ $c=1,2$.

#32 $(r_1 f + s_1 g) + (r_2 f + s_2 g) = (r_1+r_2)f + (s_1+s_2)g$

shows that N is closed under addition.

$(rf+sg)h = h(rf+sg) = (hr)f + (hs)g$

shows that N is closed under multiplication by any $h \in F[x]$.
Now $0 = 0f + 0g$ and $-(rf+sg) = (-r)f + (-s)g \in N$, thus N is an ideal.

By Thm. 27.24 N is a principal ideal $N = \langle g(x) \rangle$.

By Contradiction assume both of f and g are irr. But $f, g \in N = \langle q \rangle \Rightarrow f = q \cdot f_1$ and $g = q g_1 \Rightarrow f_1$ & g_1 should be

Const. poly. (i.e. degree $\underline{0}$, because f & g are assumed to be irr.). But then $\deg f = \deg g = \deg q$ which contradiction as we assumed f & g have different degrees.

#35 It is clear that AB is closed under addition: (a sum of m products of the form $a_i b_i$) + (a sum of n products of the form

$a_j b_j$) is a sum of $n+m$ products of this form, and hence in AB.

Because A & B are ideals we see that $r(a_i b_i) = (r a_i) b_i$ & $(a_i b_i) r = a_i (b_i r)$ are again of the form $a_j b_j$. The distributive law then shows that each sum of products $a_i b_i$ when multi. on the left or right by $r \in R$ produces a sum of such products & hence in AB. Finally $0 = 00$ & $-(a_i b_i) = (-a_i) b_i$ are in AB, thus AB is an ideal.

Note that if $a_i \in A$ & $b_i \in B \Longrightarrow a_i b_i \in A$ & $a_i b_i \in B$ (because A, B are ideals). Thus $a_i b_i \in A \cap B$. It follows that $AB \subset A \cap B$.