HW3 Solutions:

Sec. 23

#14 $f(x)=x^2+8x-2$ satisfies Eisenstein Criterion for $P=2$, so it is irr. over $\mathbb{Q}$. The quad. formula shows that $(-8\pm\sqrt{72})/2$ are roots of $f(x)$ in $\mathbb{R}$ & hence it is not irr. over $\mathbb{R}$. Of course it is not irr. over $\mathbb{C}$.

#16 $f(x)=x^3+3x^2-8$. If $f(x)$ is reducible over $\mathbb{Q}$, then by Thm. 23.11 it should factor over $\mathbb{Z}$, and therefore must have a linear factor of the form $x-a$, $a\in\mathbb{Z}$. Thus $\underline{a}$ is a root of $f(x)$ and hence should divide -8, so possibilities are $\pm1,\pm2,\pm4,\pm8$.

Plugging-in these values in $f(x)$ one verifies that none of them is a root of $f(x)$. We thus conclude that $f(x)$ is irr. over $\mathbb{Q}$.

#34 Let $p=2$. Then two possiblities are $a=0$ or 1. $x^2+0=x\cdot x$ is clearly reducible. $x^2+1=(x+1)^2$ is also reducible.

Let p be an odd prime, then $(-a)^p+a=-a^p+a \overset{\text{Fermat's thm.}}{=} -a+a=0 \pmod p$

Thus $f(x)=x^p+a$ has a root in $\mathbb{Z}_p$ and hence not irreducible

Alt. solution (without Considering 2 case):

$x^p+a \overset{\text{Fermat's thm.}}{=} x+a$ which has $x=-a$ as a root and hence not irreducible.

Sec. 24

#6 $(i+j)^{-1} = \frac{1}{(i+j)} \frac{(-i-j)}{(-i-j)} = \frac{-i-j}{1^2+1^2} = (\frac{-1}{2})i + (\frac{-1}{2})j$.

Sec. 26

#2 Suppose $\mathbb{Z}_n$ has a subring iso. to $\mathbb{Z}_2$ i.e. $\exists\, \phi : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_n$ such that ϕ is homo$\underline{\text{ism}}$ and ϕ is 1-1. Of course $\phi(0)=0$. Let $a=\phi(1)$. Then $a+a=0$ and $a^2=a$. $2a=0 \pmod n$ implies that n should be even equal to $2a$ (i.e. $a=\frac{n}{2}$). Then $a^2=a \pmod n$ implies $n=2a \mid a^2-a \Rightarrow 2a \mid a(a-1) \Rightarrow 2 \mid a-1 \Rightarrow a$ is odd.

Conversely, if $n=2a$ where a is odd then $\phi(0)=0$ and $\phi(1)=a$ is an iso. of $\mathbb{Z}_2$ and a subring of $\mathbb{Z}_n$ because $\phi(1+1)=\phi(1)+\phi(1)=0$ and $\phi(1)=\phi(1\cdot 1)=\phi(1)\phi(1)$ in $\mathbb{Z}_n$ ($a+a=0 \pmod n$ and $a\cdot a = a \pmod n$).

#20 By binomial thm. we know: $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$.

(binomial thm. is true in any commutative ring, proof word by word the same as the proof for real numbers).

We know $\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$. If we consider factorization of num. and denom. into prime numbers (just as integers) we see there is exactly one factor of p in $p! = 1\times 2\times \cdots \times p$ & no factor of p in

Let $1 \le i \le p-1$.

the denom. (because p is prime). We thus conclude that $\binom{p}{i}$, for $1 \leq i \leq p-1$, is div. by p and hence $\binom{p}{i} a^i b^{p-i} = 0$ in the ring R since R is assumed to have char. p (just def. of char. of a ring). We thus obtain:

$$(a+b)^p = a^p + b^p$$

terms corr. to $i=0$ and $i=p$.