Solutions to assignment 5

1) F is a field since $x^2 + 2$ is irreducible over $\mathbb{R}$. The inverse of $x + 1$ is $-\frac{1}{3}(x - 1)$, indeed,

$$(x + 1)[-\frac{1}{3}(x - 1)] = -\frac{1}{3}(x^2 - 1) = -\frac{1}{3}(x^2 + 2) + 1 = 1(mod\ x^2 + 2).$$

2) The inverse of (x^2+x+1) in $\mathbb{Z}_2[x]/(x^3+x+1)$ is x^2. Indeed, by Euclidean algorithm

$$(x^2 + x + 1)x^2 - (x^3 + x + 1)(x + 1) = -1$$

hence the result.

3) Yes, it is a field since $x^3 + 2x^2 + x + 1$ is irreducible over $\mathbb{Z}_3$. Indeed, it does not have any roots in $\mathbb{Z}_3$ (that can be checked directly).

4) a) easy. To prove b) observe first that (as in the first example on page 122) every element of $\mathbb{Q}[x]/(x^2 - 3)$ can be uniquely written in the form $[rx + s]$, with $r, s \in \mathbb{Q}$. Now the map

$$[rx + s] \mapsto r\sqrt{3} + s$$

is clearly a bijection and it's easy to check that it is a ring homomorphism.

5) Let $f : \mathbb{Q}(\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2})$ be an isomorphism. Then $f(\sqrt{3}) = a + b\sqrt{2}$ for suitable $a, b \in \mathbb{Q}$. Since f(1)=1, we have

$$3 = f(3) = f(\sqrt{3})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

This implies $a = 0$ or $b = 0$. If $a = 0$ then $3 = 2b^2$, if $b = 0$ then $3 = a^2$. In both cases we have contradiction with $a, b \in \mathbb{Q}$.

6) a) Straightforward verification.

To prove b) notice that, for example, $(1, 1)$ is in J, but $(1, 2)(1, 1)$ is not.

c) It is not. For example,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \notin J$$

8) Obviously, I is closed under addition (if $a, b \in I$ and $t \in J$ then $(a + b)t = at + bt = 0$). Let $r \in R$ and $x \in I$. For every $t \in J$ one has $(rx)t = r(xt) = 0$ and $(xr)t = x(rt) = 0$ (since $rt \in J$!), so I is an ideal.

9) Define a map $f : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_5$ as follows:

$$f([x]_{10}) = [x]_5$$

Then f is well-defined, it is surjective by construction, and it is a ring homomorphism. It is easy to check that $ker(f) = J$. Now the result follows from the first isomorphism theorem.