Answers to HW7

1. In $\mathbb{C}[x,y]$, $x^2+y^2=(x-iy)(x+iy)$, where $x\pm iy$ have degree 1 and are therefore irreducible. Consequently x^2+y^2 is irreducible in $\mathbb{R}[x,y]$. This shows that $\mathbb{C}[x,y]$ is not an integral domain, while $\mathbb{R}[x,y]/(x^2+y^2)$ is. (Indeed, if $ab=(x^2+y^2)c$ for some $a,b,c\in\mathbb{R}[x,y]$, then from the unique factorization property in $\mathbb{R}[x,y]$, it follows that either $x^2+y^2\mid a$ or $x^2+y^2\mid b$.)

Likewise, in $\mathbb{Z}_5$, -1 is a square ($(\pm 2)^2\equiv -1 \mod 5$), and in $\mathbb{Z}_{11}$, -1 is not a square (since the squares $\mod 11$ are $(\pm 1)^2\equiv 1$, $(\pm 2)^2\equiv 4$, $(\pm 3)^2\equiv -2$, $(\pm 4)^2\equiv 5$, $(\pm 5)^2=3$), and therefore $\mathbb{Z}_5[x,y]/(x^2+y^2)$ has zero divisors $x\pm 2y$, while $\mathbb{Z}_{11}/(x^2+y^2)$ is an integral domain.

$\mathbb{C}[x,y]/(x^2+y^2-1)$ is an integral domain too, since x^2+y^2-1 cannot be factored even over complex numbers. Indeed, if it did factor, i.e. x^2+y^2-1 were the product of linear functions, then the solution set to $x^2+y^2=1$ would be the union of two (complex) lines (or a double line). But the actual solution set is not, as it is clear by looking at the set of real solutions, which is a circle.

2. *Answer:* (a) $\cong$ (c), (b) $\cong$ (e).

In $\mathbb{Z}[x]$, $2x^2-6=(2x+4)(x-2)+2$, i.e. $I:=(x^2-3,2x+4)=(x^2-3,2)=((x+1)^2,2)$. Therefore $\mathbb{Z}[x]/I\cong\mathbb{Z}_2[x]/((x+1)^2)\cong\mathbb{Z}_2[y]/(y^2)$. This ring has 4 elements: $0,1,1+x,x \mod (x^2)$, of which only x is not invertible. In $\mathbb{Z}_2\times\mathbb{Z}_2$, also consisting of 4 elements, $(0,0),(1,1),(1,0),(0,1)$, the last two are not invertible, and hence (d) is not isomorphic to (a) and (c).

In $\mathbb{Z}[i]$, the ideal $(i-2)$ contains $(i-2)(i+2)=-5$, i.e. $(5)\subset(i-2)\subset\mathbb{Z}[i]$. The quotient $\mathbb{Z}[i]/(5)\cong\mathbb{Z}_5[i]$ is *additively* isomorphic to $\mathbb{Z}_5\oplus\mathbb{Z}_5=\{a+bi|a,b\in\mathbb{Z}_5\}$. In this quotient, $i-2$ is neither zero, nor invertible (since it is a zero divisor). Thus, the quotient $\mathbb{Z}[i]/(i-2)$ is *additively* isomorphic to $\mathbb{Z}_5$. The *ring* homomorphism $\mathbb{Z}\mapsto\mathbb{Z}[i]/(i-2)$, defined by mapping 1 to $1+(i-2)$ has kernel $5\mathbb{Z}$. Indeed, if an ordinary integer n is divisible in $\mathbb{Z}[i]$ by $i-2$, i.e. $n=(i-2)(a+bi)$, then $n^2=5(a^2+b^2)$, hence $5|n^2$ in $\mathbb{Z}$, hence $5|n$. Thus the *ring* homomorphism $\mathbb{Z}/5\mathbb{Z}\to\mathbb{Z}[i]/(i-2)$ is well-defined, injective and therefore bijective.

On the other hand, identify $\mathbb{Z}_5[x]/(2x+4)$ with $\mathbb{Z}_5[y]/(y)$ by the change of variable $y=2x+4$, invertible since 2 is invertible in $\mathbb{Z}_5$: $x=(y-4)/2=3y-2$. Clearly, $\mathbb{Z}_5[y]/(y)\cong\mathbb{Z}_5$ (and not isomorphic to (d) since it has 5 elements, not 4).

3. Clearly, $m/n+m'/n' = (mn'+m'n)/nn'$ has denominator coprime to p if both n, n' are coprime to p, and numerator divisible by p when both m, m' are divisible by p. Also, $(m/n) \times (m'/n') = mm'/nn'$ has the denominator coprime to p if both n, n' are coprime to p and the numerator divisible by p whenever at least one of m, m' is divisible by p. Thus, the fractions of the form m, n with n coprime to p form a subring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$, and among them the fractions m/n with $p|m$ form an ideal $(p) \subset \mathbb{Z}_{(p)}$. The quotient $\mathbb{Z}_{(p)}/(p)$ is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$ of integers $\mod p$.

4. Let $b_0x^n + b_1x^{n-1} + \cdots + b_n$, $b_i \in R$, be an element in $R[x]$. In the quotient $R[1/a] := R[x]/(1-ax)$, it represents $b_0\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = \alpha^n(b_0 + b_1a + \cdots + b_na^n)$. Indeed, in $R[x]$, for $k \le n$ we have

$$x^n a^k = x^{n-k}(ax)^k = x^{n-k}(1-(1-ax))^k \equiv x^{n-k} \mod (1-ax).$$