Homework #1

1.
We would proceed by induction.
Base Case: If |A|=1, and write A={a} where aœA, the only possible 2^1 subsets of A are « and {a}. The base case is established.
Induction Hypothesis: Let |A|=n, then A has 2^n subsets. We want to show that this implies if |B|=n+1, B has 2^{n+1} subsets.

By naïve set theory, the elements of set X are either in a particular subset of X or not in that particular subset of X, and any subset of A contains only the elements that are in A. Write B = {b} » C, where b is an element of B but not in C and |C|=n. By the induction hypothesis, C has 2^n subsets. For each of the subset C', C' is a subset of B, and {b} » C' is also a subset of B. Hence, there are $2 \cdot 2^n = 2^{n+1}$ subsets of B, completing the proof.

2.
f: **R**-> **R**
x |->2x-3
f is injective iff x ∫ y => f(x) ∫ f(y).
Claim: f is injective
Proof: Suppose f(x)=f(y) <=> 2x-3 = 2y-3 <=> x=y.
Claim: f is surjective
Proof: f is surjective iff for all rœ**R**, $\exists x \in R$ such that f(x)=r. Clearly, for any r and x=(r+3)/2, f(x)=r.

g: **R**-> **R**
x |->x^2
Claim: g is not injective.
Proof: g(-1)=1 and g(1)=1, hence it is not the case that x ∫ y => g(x) ∫ g(y)
Claim: g is not surjective.
Proof: There does not exists a x such that g(x)=-1. g(x) is a even function **R**-> **R**, and we know that all even functions **R**-> **R** are not surjective.

3.
f and g are inverses of each other iff f(g(x)) = x and g(f(x))=x for all x in R^3.

Claim 1: $f \circ g = I_{R^3}$
Proof: By the definition of f and g, we see that
$f \circ g$: R^3->R^3

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \frac{1}{2}\begin{pmatrix} (x_1+x_2)-(x_2+x_3)+(x_1+x_3) \\ (x_1+x_2)+(x_2+x_3)-(x_1+x_3) \\ -(x_1+x_2)+(x_2+x_3)+(x_1+x_3) \end{pmatrix} <=> \frac{1}{2}\begin{pmatrix} x_1+x_1 \\ x_2+x_2 \\ x_3+x_3 \end{pmatrix} <=> \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Clearly, f(g(x)) = x for all x in R^3.

Claim 2: $g \circ f = I_{R^3}$

Proof: By the definition of f and g, we see that

$g \circ f$: R^3->R^3

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} \frac{1}{2}(x_1 - x_2 + x_3) + \frac{1}{2}(x_1 + x_2 - x_3) \\ \frac{1}{2}(x_1 + x_2 - x_3) + \frac{1}{2}(-x_1 + x_2 + x_3) \\ \frac{1}{2}(x_1 - x_2 + x_3) + \frac{1}{2}(-x_1 + x_2 + x_3) \end{pmatrix} <=> \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Clearly, g(f(x))=x for all x in R^3.

Claim 1 and 2 => f and g are inverses of each other.

4

a.

Claim: $f^1(x)$ is not idempotent

Proof: We see that f(x) is not idempotent. For example, f(1)=2 but f(f(1))=3 ∫ 2.

Claim: $f^2(x)$ is idempotent

Proof:

Clearly, we want to take advantage of f(3)=4, and f(4)=f(3).

Hence, the task becomes finding the smallest integer n such that $f^n(1)$ = 3 or 4 and $f^n(2)$ = 3 or 4.
We see that f(f(1))=$f^2(1)$=3 and $f^2(2)$=4.

X	1	2	3	4
$f^2(x)$	3	4	3	4

X	1	2	3	4
$f^{2x2}(x)=f^4(x)$	3	4	3	4

Since $f^2(x) = f^{2x2}(x) = f^4(x)$ for all x in A, $f^2(x)$ is idempotent. i.e. 2 is the smallest positive n.

4b.

Since we need fgf=f:

f(g(2))=2 => g(2)=1

f(g(3))=3 => g(3)=2 or 4

f(g(4))=4 => g(4)=3

f(g(1))=1 does not need to be considered because 1 is not in the range of f.

So far, we know g is one of the following possible 8 mappings:

X	1	2	3	4
g'(x)	1 or 2 or 3 or 4	1	2 or 4	3

Since we need gfg=g:
g(f(1))=1 => g(2)=1
g(f(2))=2 => g(3)=2
g(f(3))=3 => g(4)=3
g(f(4))=4 => g(3)=4
And we want g(1)=1 so that gfg(1)=g(1)=1.

So g(x) can be either of the following 2 mappings:

X	1	2	3	4
g(x)	1	1	2	3

X	1	2	3	4
g(x)	1	1	4	3

4c.
Claim: fg is idempotent:
Proof: We want to show that fg=fgfg by definition of idempotency. From b) and by the associativity of functions, we know that fg=(fgf)g=fgfg.

Claim: gf is idempotent:
Proof: Similarly, we want to show that gf=gfgf by definition of idempotency. From b) and by the associativity of functions, we know that gf=(gfg)f=gfgf.

4d.
Suppose h:

X	1	2	3	4
h(x)	2	3	4	1

and k:

X	1	2	3	4
k(x)	4	1	2	3

we see that

X	1	2	3	4
hk(x)	1	1	1	1

X	1	2	3	4
kh(x)	1	1	1	1

h and k are mappings in T_A s.t. h $\int I_A$ and hk=kh=I_A

5.
Proof $1+5+9+\ldots+4n+1=(2n+1)(n+1)$

We would proof by using the first form of principle of induction
If n=0, $4(0)+1=(2(0)+1)(0+1)$, so the equivalence holds for n=0. Our base is established.

Assume as induction hypothesis that $1+5+9+\ldots+4n+1=(2n+1)(n+1)$ for some integer $n\geq 1$, we want to show that $1+5+9+\ldots+4n+1+4(n+1)+1 = (2(n+1)+1)((n+1)+1)$.

By induction hypothesis,
$1+5+9+\ldots+4n+1+4(n+1)+1 = (2n+1)(n+1)+ 4(n+1)+1$
$= 2n^2+7n+9$
$= (2n+3)(n+2)$
$= (2(n+1)+1)((n+1)+1)$.

Our induction step is complete. Hence, by induction we show that $1+5+9+\ldots+4n+1=(2n+1)(n+1)$ for $n\geq 0$

6a.
Using the second form of the principle of induction

For n=1, $a_1=1 < 2^1$
For n=2, $a_1=1 < 2^2$
For n=3, $a_1=2 < 2^3$. Our bases are established.

We adopt the hypothesis that for some integer $n\geq 3$ and $0\leq k\leq n$, $a_k < 2^k$. We want to show that $a_{n+1}<2^{k+1}$.

By definition, $a_{n+1} = a_n + a_{n-1}$. By induction hypothesis, $a_n < 2^n$ and $a_{n-1} < 2^{n-1}$. Hence,
$a_{n+1} = a_n + a_{n-1} < 2^n + 2^{n-1} < 2^n + 2^n = 2^{n+1}$ for $n\geq 2$, completing our induction step.

b)
i)
We want to show that $a_n a_{n+1} - a_{n-1}a_n = a_n^2$:

$a_n a_{n+1} - a_{n-1}a_n$ $= a_n(a_{n+1}-a_{n-1})$ $= a_n(a_n+a_{n-1}-a_{n-1})$ $= a_n(a_n)$ $=a_n^2$	By definition of Fibonacci sequence for $n\geq 2$

ii)
We will proceed by induction:
For n=2, $a_{n-1}a_{n+1}-a_n^2 = 1\cdot 2-1= (-1)^n=1$

For n=3, $a_{n-1}a_{n+1}-a_n^2 = 1\cdot3-2^2= (-1)^n=-1$. Our bases are established.

For the induction hypothesis, we adopt that $a_{n-1}a_{n+1}-a_n^2 = (-1)^n$ for some integer $n\geq3$. We want to show that $a_na_{n+2}-a_{n+1}^2 = (-1)^{n+1} = -(-1)^n$.

Claim: $a_na_{n+2}-a_{n+1}^2 = (-1)^{n+1} = -(-1)^n = - a_{n-1}a_{n+1}-a_n^2$
Proof: Applying our induction hypothesis, we want to show that $a_na_{n+2}-a_{n+1}^2 = -(a_{n-1}a_{n+1}-a_n^2)$.

We show that by first observing $a_{n+1}^2=a_{n+1}(a_n+a_{n-1})$
$a_{n+1}(a_n+a_{n-1}) = a_{n+1}a_n+a_{n-1}a_{n+1}$
$\Rightarrow a_n^2+a_{n+1}^2= a_n^2+a_{n+1}a_n+a_{n-1}a_{n+1}$
$\Rightarrow a_n^2+a_{n+1}^2= a_n(a_{n+1}+a_n)+a_{n-1}a_{n+1}$
$\Rightarrow a_n^2+a_{n+1}^2=a_na_{n+2}+a_{n-1}a_{n+1}$
$\Rightarrow a_na_{n+2}-a_{n+1}^2= -a_{n-1}a_{n+1}+a_n^2$
Hence, $a_na_{n+2}-a_{n+1}^2 = -(a_{n-1}a_{n+1}-a_n^2)$ for $n\geq2$. By induction hypothesis, $a_na_{n+2}-a_{n+1}^2 = -(a_{n-1}a_{n+1}-a_n^2)$ $= -(-1)^n = (-1)^{n+1}$

c) We will proceed by induction. For n=1, $a_n^2 = 1 = a_na_{n+1} = 1\cdot1=1$. For n=2, $a_1^2+a_2^2 = 1+1 = a_na_{n+1} = 1\cdot2=2$. Our bases are established.

For the induction hypothesis, suppose for some integer $n\geq2$, $a_1^2+a_2^2\ldots+a_n^2=a_na_{n+1}$, we want to show that $a_1^2+a_2^2\ldots+a_n^2+a_{n+1}^2=a_na_{n+1}$.

Applying the induction hypothesis, it is equivalent to show $a_na_{n+1}+a_{n+1}^2=a_{n+1}a_{n+2}$.

$a_na_{n+1}+a_{n+1}^2$ $=(a_n+a_{n+1})a_{n+1}$ $=(a_{n+2})a_{n+1}$	By definition of Fibonacci sequence for $n\geq2$

7. Let P(n) denote the proposition that with |V|=n, the color of the horses in V are the same. From the argument, we see that P(1) does not imply P(2). i.e. Using the definition of $W_1\ldots W_2$ in the problem, when n=2, $W_1\ldots W_2=\emptyset$, and hence it does not follow that the horses in W_1 and W_2 are of the same color.

8. To show that $2|n^2+3n$, we need to consider two cases:
Claim 1 : If n is an odd integer, $2|n^2+3n$:
Proof: Suppose n = 2k+1 for some k, then $n^2+3n = 4k^2+4k+1+3(2k+1)=4k^2+10k+4$. Clearly, $2|4k^2+10k+4$ because $2|4k^2$ and 2|10k and 2|4.

Claim 2 : If n is an even integer, $2|n^2+3n$:
Proof: Suppose n = 2k for some k, then $n^2+3n = 4k^2+3(2k)$. Clearly, $2|4k^2+3(2k)$ because $2|4k^2$ and 2|6k.

Claim 1 and 2 $\Rightarrow 2|n^2+3n$ for all $n\in\mathbb{Z}$

9i)
a=175; b=72
We apply the extended Euclidean algorithm to gcd(a,b):

I	q_i	r_i	x_i	y_i
0	-	175	1	0
1	-	72	0	1
2	2	31	1	-2
3	2	10	-2	5
4	3	1	7	-17
5	10	0	-72	175

gcd(a,b)=1
1=7(175)-72(17)

9ii)
a=377; b=341

gcd(a,b)=gcd(a',b') where a'=b and b'=a
We apply the extended Euclidean algorithm to gcd(a',b'):

I	q_i	r_i	x_i	y_i
0	-	377	1	0
1	-	341	0	1
2	1	36	1	-1
3	9	17	-9	10
4	2	2	19	-21
5	8	1	-161	178
6	2	0	341	-377

gcd(a,b)=1
1=-161(377)+178(341)

9iii)
a=1848; b=525

We apply the extended Euclidean algorithm to gcd(a,b):

I	q_i	r_i	x_i	y_i
0	-	1848	1	0
1	-	525	0	1
2	3	273	1	-3
3	1	252	-1	4
4	1	21	2	-7
5	12	0	-25	88

gcd(a,b)=21
21=2(1848)-7(525)

10.
a) Since gcd(a,b)=r_n by Euclidean Algorithm, gcd(a,b)=$x_n a+y_n b$ if $r_k = x_k a+y_k b$ for $0\leq k\leq n+1$.
Claim 1: $r_k = x_k a+y_k b$ for $0\leq k\leq n+1$
Proof:
We will show $r_k = x_k a+y_k b$ by the second principle of induction.

By definition, $x_0=1$, $y_0=0$, $x_1=0$, $y_1=1$, $r_0=a$, $r_1=b$. Clearly, $r_i = x_i a+y_i b$ for i=0 and i=1. Our basis is established. Let the induction hypothesis be $r_j=x_j a+y_j b$ for $0\leq j\leq k$ for some integer $k\geq 1$. We will now show that $r_{k+1}=x_{k+1}a+y_{k+1}b$:

As followed from Euclidean Algorithm, $r_{k+1} = r_{k-1}-r_k q_{k-1}$.
By induction hypothesis, $r_k=x_k a+y_k b$ and $r_{k-1}=x_{k-1}a+y_{k-1}b$.
Hence, $r_{k+1} = x_{k-1}a+y_{k-1}b-(x_k a+y_k b)q_{k-1} = x_{k-1}a+y_{k-1}b-x_k aq_{k-1}-y_k bq_{k-1}$
$= x_{k-1}a-x_k aq_{k-1}+y_{k-1}b-y_k bq_{k-1} = (x_{k-1}-x_k q_{k-1})a+(y_{k-1}-y_k q_{k-1})b = x_{k+1}a+y_{k+1}b$ for $0\leq k\leq n+1$.

Claim 1 => $r_k = x_k a+y_k b$ for $0\leq k\leq n+1$ => $r_n = x_n a+y_n b$ => gcd(a,b)=$x_n a+y_n b$

b)
By definition of A_k, $\det(A_k) = x_k\cdot y_{k+1}-y_k x_{k+1}$.
Claim: $x_k\cdot y_{k+1}-y_k x_{k+1} = (-1)^k$ for $0\leq k\leq n+1$
Proof: We will now proceed by induction:
For k=0, $x_0=1$, $y_0=0$, $x_1=0$, $y_1=1$. Clearly, $\det(A_0) = (-1)^0$.

For the induction hypothesis, we assume that $x_k\cdot y_{k+1}-y_k x_{k+1} = (-1)^k$. To show $x_{k+1}\cdot y_{k+2}-y_{k+1}x_{k+2} = (-1)^{k+1}$, we apply our induction hypothesis and show instead:
$x_k\cdot y_{k+1}-y_k x_{k+1}= (-1)^{k+1}= -(-1)^k = -(x_{k+1}\cdot y_{k+2}-y_{k+1}x_{k+2})$.

From the definition of x_k and y_k, we can write $q_k = \frac{x_{k+2}-x_k}{x_{k+1}} = \frac{y_{k+2}-y_k}{y_{k+1}}$.

$\frac{x_{k+1}}{x_{k+2}-x_k} = \frac{y_{k+1}}{y_{k+2}-y_k} \Rightarrow x_{k+1}(y_{k+2}-y_k) = y_{k+1}(x_{k+2}-x_k)$. Rearranging, we get $x_k y_{k+1}-x_{k+1}y_k = -x_{k+1}y_{k+2}+x_{k+2}y_{k+1}$, completing our induction step.

$x_k y_{k+1}-x_{k+1}y_k = -x_{k+1}y_{k+2}+x_{k+2}y_{k+1}$ => $x_k y_{k+1}-x_{k+1}y_k = -x_{k+1}y_{k+2}+x_{k+2}y_{k+1}=(-1)^{k+1}= -(-1)^k$.

c) From part b), we know that for $1\leq k\leq n+1$, $x_k\cdot y_{k+1}-y_k x_{k+1} = (-1)^k = \pm 1$.
Claim 1: $x_k\cdot y_{k+1}-y_k x_{k+1} = -1$ => $\gcd(x_k,y_k)=1$
Proof: $x_k\cdot y_{k+1}-y_k x_{k+1} = -1$ => $-x_k\cdot y_{k+1}+y_k x_{k+1} = 1$. By Corollary 1.3.8, this implies $\gcd(x_k,y_k)=1$

Claim 2: $x_k\cdot y_{k+1}-y_k x_{k+1} = 1$ => $\gcd(x_k,y_k)=1$
Proof: Since $x_k\cdot y_{k+1}-y_k x_{k+1} = 1$, by Corollary 1.3.8, this implies $\gcd(x_k,y_k)=1$

Claim 1 and 2 imply $\gcd(x_k,y_k)=1$ for $1\leq k\leq n+1$.

d) By Matrix multiplication $A_k \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x_k a + y_k b \\ x_{k+1} a + y_{k+1} b \end{pmatrix}$. From the general proof from a), $r_k = x_k a + y_k b$ for $0 \leq k \leq n+1$. Hence, $A_k \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x_k a + y_k b \\ x_{k+1} a + y_{k+1} b \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}$

e) From the general proof we gave in a), we see that $r_k = x_k a + y_k b$ for $0 \leq k \leq n+1$. $r_{n+1}=0$ => $0 = x_{n+1} a + y_{n+1} b$ => $-x_{n+1} a = y_{n+1} b$ => $\frac{a}{b} = -\frac{y_{n+1}}{x_{n+1}}$.

Homework #2

1. We insist on not using prime factorization because we're in that section:
To show that for any a,b $\mathbf{Z}_{>0}$, we have gcd(a,b)·lcm(a,b)=ab, we show instead gcd(a,b)·lcm(a,b)| ab and ab|gcd(a,b)·lcm(a,b).

Claim 1: gcd(a,b)·lcm(a,b)| ab
Proof:
Let d=gcd(a,b) and write a=da' and b=db', where a' and b' are integers.

We recognize that a|da'b'=ab'=a'b and b|da'b'=a'b=ab'. Hence, da'b' is a common multiple of a and b. By definition of lcm, lcm(a,b)| da'b'=a'b=ab'. Hence, gcd(a,b)·lcm(a,b)=d·lcm(a,b)| d·da'b'=ab.

Claim 2: ab|gcd(a,b)·lcm(a,b)
Proof:
By definition of lcm(a,b), b| lcm(a,b). This implies ab|a·lcm(a,b). Similarly, ab|b·lcm(a,b). Again, by definition of lcm, lcm(a,b)|ab because ab is a common multiple of a and b. Hence, ab|a·lcm(a,b) => ab/lcm(a,b)|a and ab|b·lcm(a,b) => ab/lcm(a,b)|b. Hence, by definition of gcd, ab/lcm(a,b)|gcd(a,b) since ab/lcm(a,b) is a common factor of a and b. ab/lcm(a,b)|gcd(a,b) => ab|gcd(a,b)·lcm(a,b).

Claim 1+2 => gcd(a,b)·lcm(a,b)=ab for any a,b $\mathbf{Z}_{>0}$.

2.
Let a,b,c be $\mathbf{Z}_{>0}$.

Claim 1: gcd(a,bc)=1 => gcd(a,b)=1 and gcd(a,c)=1.
Proof:
By Corollary 1.3.8, gcd(a,bc)=1 <=> there exists integers x and y s.t. ax + bcy=1. Clearly, there exists integers x' and y' s.t. ax' + by'=1, namely, let x'=x and y'=cy. Hence, gcd(a,b)=1 by corollary 1.3.8. Similarly, there exists integers x" and y" s.t. ax" + cy"=1, namely, let x"=x and y"=by. Hence, gcd(a,c)=1 by corollary 1.3.8.

Claim 2: gcd(a,bc)=1 <= gcd(a,b)=1 and gcd(a,c)=1.
By Corollary 1.3.8, gcd(a,b)=1 <=> there exists integers x and y s.t. ax + by=1. By Corollary 1.3.8, gcd(a,c)=1 <=> there exists integers x' and y' s.t. ax' + cy'=1. Clearly, (ax+by)(ax' + cy')=1·1=1 <=> aaxx'+acxy'+byax'+bcyy'=1 <=> a(xx'+cxy'+byx')+bcyy'=1 <=> gcd(a,bc)=1 since clearly, there exists integers x" and y" s.t. a(x")+bcy"=1, namely, let x"= xx'+cxy'+byx' and y"= yy'.

3.
a)
It is straightforward to show by simple algebraic manipulation that
$(x^a-1)(x^{(b-1)a} + x^{(b-2)a} + \dots + x^a + 1)$
$= (x^{(b-1)a} + x^{(b-2)a} + \dots + x^a + 1)\, x^a - (x^{(b-1)a} + x^{(b-2)a} + \dots + x^a + 1)$

$= (x^{(ab)} + x^{a(b-1)} + \ldots + x^{a+a} + x^{a}) - x^{(b-1)a} - x^{(b-2)a} - \ldots - x^{a} - 1$
$= x^{ab} + x^{(b-1)a} - x^{(b-1)a} + x^{(b-2)a} - x^{(b-2)a} \ldots + x^{a+a} - x^{2a} + x^{a} - x^{a} - 1$
$= x^{ab} - 1$

b) To show that 2^n-1 can only be prime if n is, it is equivalent to show that if n is not prime, then 2^n-1 is not prime.

If n is not a prime, then by definition we can write n=ab where a and b are integers >1. Hence, by part a of this question, and letting x=2, we see that $2^a-1 \mid 2^n-1 = 2^{ab}-1$. By assumption, $2^a-1 \int 1 \int 2^n-1$, and so by definition 2^n-1 is not prime.

c)
23 is a prime. However, $47|2^{23}-1$, so $2^{23}-1$ is not a prime.

4
a) R is not reflexive because 1 does not relate to 1 since 1+1<10 but $1 \in Z$
R is symmetric because if a R b <=> a+b=10 <=> b+a=10 <=> b R a
R is not transitive because 2 R 8 and 8 R 2 but 2 does not related to 2 because 2 +2 <10 and 8 and 2 are $\in Z$

b)
a) R is reflexive. Let $a \in Z$ and $b \in (Z\backslash\{0\})$, then $(a,b) \in X$. We see that (a,b) R (a,b) <=> $a \cdot b = a \cdot b$ for all (a,b) in X =>R is reflexive

b) R is symmetric. For (a,b) and (c,d) in X, (a,b) R (c,d) <=> $a \cdot b = c \cdot d$ <=> $c \cdot d = a \cdot b$ <=> (c,d) R (a,b).

c) R is transitive. For (a,b), (e,f) and (c,d) in X, (a,b) R (c,d) and (c,d) R (e,f) <=> $a \cdot b = c \cdot d$ and $c \cdot d = e \cdot f$ => $a \cdot b = e \cdot f$ <=> (a,b) R (e,f) => R is transitive.

6. $33^{33} \equiv 2^{33} \equiv (2^{5 \cdot 6+3}) \equiv (2^5)^6 \cdot 2^3) \equiv 1^6 \cdot 2^3 \equiv 8 \pmod{33}$

7.
a) We first establish that $10 \equiv -1 \pmod{11}$. Clearly, we see that $11 \mid (10 - (-1)) = 11$.

$10^n \equiv 10 \cdot 10 \cdot 10 \ldots 10$ (n times) $\equiv (-1) \cdot (-1) \cdot (-1) \ldots .. (-1)$ (n times) $\equiv (-1)^n \pmod{11}$.

We show by induction just to be rigorous. As stated previously, it is clear that $10^n \equiv (-1)^n \pmod{11}$ for n=1. As induction hypothesis, now assume that for n=k, $10^k \equiv (-1)^k \pmod{11}$. We want to show that $10^{k+1} \equiv (-1)^{k+1} \pmod{11}$:

Using what we have shown in lecture, that $a \equiv_n b$ and $c \equiv_n d$ => $ac \equiv_n bc$, we can conclude that $10^k \equiv (-1)^k \pmod{11}$ => $10^k(-1) \equiv (-1)^k(-1)$ <=> $10^{k+1} \equiv (-1)^{k+1} \pmod{11}$, completing our proof by induction.

b) Write a as $x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + x_{n-2} \cdot 10^{n-3} + \ldots + x_2 \cdot 10^1 + x_1 \cdot 10^0$.

Hence, $a \equiv x_n \cdot 10^{n-1} + x_{n-1} \cdot 10^{n-2} + x_{n-2} \cdot 10^{n-3} + \ldots + x_2 \cdot 10^1 + x_1 \cdot 10^0 \pmod{11}$
$\Rightarrow a \equiv x_n \cdot (-1)^{n-1} + x_{n-1} \cdot (-1)^{n-2} + x_{n-2} \cdot (-1)^{n-3} + \ldots + x_2 \cdot (-1)^1 + x_1 \cdot (-1)^0 \pmod{11}$
Rearranging,
$\Rightarrow a \equiv x_1 \cdot (-1)^0 + x_2 \cdot (-1)^1 + x_3 \cdot (-1)^2 \ldots + x_{n-2} \cdot (-1)^{n-3} + x_{n-1} \cdot (-1)^{n-2} + x_n \cdot (-1)^{n-1} \pmod{11}$
Since $(-1)^k = 1$ iff k is an even integer and $(-1)^k = -1$ iff k is an odd integer
$\Rightarrow a \equiv x_1 \cdot (1) + x_2 \cdot (-1)^1 + x_3 \cdot (1) + \ldots + x_{n-2} \cdot (-1)^{n-3} + x_{n-1} \cdot (-1)^{n-2} + x_n \cdot (-1)^{n-1} \pmod{11}$

c) To show $43,171,234 \equiv 7 \pmod{11}$, we employ the method suggested in b) and first calculate $x_1 \cdot (1) + x_2 \cdot (-1)^1 + x_3 \cdot (1) + \ldots + x_{n-2} \cdot (-1)^{n-3} + x_{n-1} \cdot (-1)^{n-2} + x_n \cdot (-1)^{n-1}$ where n=8.

We see that $43,171,234 \equiv 4-3+2-1+7-1+3-4 = 7 \equiv 7 \pmod{11}$

8.
f = g if:
$[a]_5 = [b]_5 \Rightarrow f([a]_5) = g([b]_5)$ for any [a], [b] in Z/5Z $\Leftrightarrow 5 \mid f(a') - g(a')$ where a' is in Z

Let [a] be an element of Z/5Z. Clearly $5 \mid [a]_5^3 + 2[a]_5^2 + 3 - ([a]_5^3 - 3[a]_5^2 + 5[a]_5 - 2) = 5[a]_5^2 + 5[a]_5 + 5$. Hence, $f(a) \equiv g(a) \pmod{5}$, or equivalently, $f([x]) = g([y])$ for [x] and [y] in Z/5Z.

9a)
We will show by cases. There are only 3 equivalent classes to consider in Z/3Z. We consider the 6 cases. WLOG, let $x \geq y$, where x and y are as defined in the question. x and y can only take on the following values: $[0]_3, [1]_3$ and $[2]_3$.

Case x=[2] and y=[2]:
$[2]^2 + [2]^2 = [2][2] + [2][2] = [8] \int [0]$

Case x=[2] and y=[1]
$[2]^2 + [1]^2 = [2][2] + [1][1] = [5] \int [0]$

Case x=[2] and y=[0]
$[2]^2 + [0]^2 = [2][2] + [0][0] = [4] \int [0]$

Case x=[1] and y=[1]
$[1]^2 + [1]^2 = [1][1] + [1][1] = [2] \int [0]$

Case x=[1] and y=[0]
$[1]^2 + [0]^2 = [1][1] + [0][0] = [1] \int [0]$

Case x=[0] and y=[0]
$[0]^2 + [0]^2 = [0][0] + [0][0] = [0]$

We have exhausted all the possibilities. Hence, the only solution is $x=y=[0]_3$

9b)

Suppose there is a solution. We will prove by contradiction.

Let integers x' and y' in **Z** be the solution. a) implies that $x'^2+y'^2 = 3k$ for some k in Z implies x'=3s and y'=3t for some s and t in Z. However, by the following Claim 1, this implies k = 3k' where k' is an integer. This implies gcd(k,3k)=3 ∫ 1, so there is no solution.

Claim 1: For integers x' and y' in **Z**, $x'^2+y'^2 = 3k$ for some k in Z implies x'=3s and y'=3t for some s and t in Z, and this in turn implies k = 3k' where k' is an integer.
Proof: It is easy to see that if x'=3s and y'=3t, then $3k= 9s^2+9t^2$ <=> $k=3s^2+3t^2$ <=> 3| k <=> k=3k' for an integer k'.

10)
We will use the Extended Euclidean Algoithm to find the inverse of 17 ∈ Z/95Z

I	q_i	r_i	x_i	y_i
0	-	95	1	0
1	-	17	0	1
2	5	10	1	-5
3	1	7	-1	6
4	1	3	2	-11
5	2	1	-5	28
6	3	0	17	-95

We see that 95(-5)+17(28) = 1. Hence, 95 | 17(28)+1 => 28 is the inverse of 17∈ Z/95Z

11.
a) Claim1: $a=a^{-1}$ => $a^2=1$
Proof: By definition of inverse, $a.a^{-1} = 1$ if a is a unit. If $a=a^{-1}$, then $a^2 = a\cdot a = a\cdot a^{-1} = 1$.

Claim 2: $a^2=1$ => $a=a^{-1}$
Proof: By Theorem 1.7.1, inverses are unique. $a^2=1$ <=> a·a=1 => a is a's own inverse. In other words, uniqueness of inverse and claim 1 => claim 2.

Claim 1+Claim 2 completes the proof.

b)
Claim 1: if a =1 or a=-1 then $a=a^{-1}$.
Proof:
If a =1, then $a^2=1$. By a), $a=a^{-1}$
If a =-1, then $a^2=1$. By a), $a=a^{-1}$

Claim 2: If $a=a^{-1}$ => a=1 or a=-1

By a), $a=a^{-1}$ => $a^2=1$ => $\exists \tilde{a}, x, y \in Z$ s.t. $\tilde{a}^2x+py=1$ where [ã]=a and $0\leq\tilde{a}<p$ <=> p | $\tilde{a}^2-1$ <=> ã =1 or ã = -1 <=> a=1 or a=-1.

Claim 1+Claim 2 completes the proof.

c)
(p-1)! = 1·2·3·. … (p-2)·(p-1). By theorem 1.7.4, the invertible elements in Z/pZ are [1],[2], [3], … ,[p-1]. By uniqueness of inverses, every element [a] in Z/pZ has exactly one [b] in Z/pZ s.t. [a][b]=[1]. By part a and part b of this question, if [a]∫[-1] and [a]∫[1], then [a][b]=1 => [a] ∫[b]. Hence, for elements [2], [3], …, [(p-3)], [(p-2)], we can match each of them up with its inverses. Hence, (p-1)! ≡ 1·2·3·. … (p-2)·(p-1) ≡ 1·(1·1 …. 1·1)·(p-1) ≡ -1 (mod p)

12.
To simplify notation, we drop the square brackets but recognize that we are working in Z/5Z (e.g. $[a]_5$ is simply written as a
1) 3x+y+2z = 3
2) x+y+2z = 2
3) 2x+y+4z = 3

We add the 1) and 3) together and get 4) 5x+2y+6z=6 <=> 0x+2y+z=1.
We add 2) and 3) together and get 5) 3x+2y+6z=5 <=> 3x+2y+z=0.
We add 1) and 2) together and get 6) 4x+2y+4z=0
We subtract 5) from 4) and get 7) 2x=1 <=> 2x=6 <=> x=3.
We subtract 6 from 5) and get 8) x-2z=0
Substituting in results from 7) to 8), we get -2z=-3 <=> 2z=8 <=> z=4
Substituting in results from 8) to 6), we get 4(3)+2(y)+4(4) = 0 <=> y=1
So in sum, x≡3 (mod 5), y≡4 (mod 5), z≡1 (mod 5).

Homework #3

1.
We will prove by contradiction.
We know that $10a_1+9a_2+\ldots+ma_j+\ldots na_i+\ldots+2a_9+1a_{10} \equiv 0 \pmod{11}$, where m and n are integers s.t. $10 \geq m > n \geq 0$ and $m+j=11$ and $n+i=11$.
Suppose now we have swapped a_i and a_j, where $i>j$ and B is still a valid code. If B is still a valid code, then $10a_1+\ldots+ma_j+\ldots na_i+\ldots+a_{10} \equiv 10a_1+\ldots+ma_i+\ldots na_j+\ldots+a_{10} \equiv 0 \pmod{11}$.
This implies $ma_j-ma_i+na_i-na_j \equiv 0 \pmod{11} \Rightarrow m(a_j-a_i)-n(a_j-a_i) \equiv 0 \pmod{11}$
$\Rightarrow (m-n)(a_j-a_i) \equiv 0 \pmod{11}$. However, $10 \geq m > n \geq 1$, so $9 \geq (m-n) \geq 1 \Rightarrow \gcd(m-n,11)=1 \Rightarrow (m-n)$ is invertible $\Rightarrow (a_j-a_i) \equiv 0 \pmod{11}$. But $0 \leq a_j, a_i \leq 9$, so $(a_j-a_i) \equiv 0 \pmod{11} \Rightarrow a_i = a_j$.
Contradicting the assumption that $i>j$, so B is not a valid code.

2. We first checked and verified that 6, 5, and 11 are pairwise co-prime. Then we apply the Chinese remainder theorem.
We first try to solve:
$x' \equiv 3 \bmod 6$
$x' \equiv 0 \bmod (11 \cdot 5)$
Note: We could have solved the system $x' \equiv 1 \bmod 6$ and $x' \equiv 0 \bmod (11 \cdot 5)$
first, and then multiply the solution x' by 3. However, because we are solving by trial and error anyway, we can shortcut the process. (i.e. If w_1 is an integer s.t. $w_1 \equiv 1 \bmod 6$ and $w_1 \equiv 0 \bmod (11 \cdot 5)$, then $x'=3w_1$ where x' is the solution to the system.)
By trial and error, $(11 \cdot 5) \cdot 3 = 165$ and $165 \equiv 3 \bmod 6$. Hence $x'=165$.

Then we try to solve:
$x'' \equiv 2 \bmod 5$
$x'' \equiv 0 \bmod (11 \cdot 6)$

By trial and error, $(11 \cdot 6) \cdot 2 = 132$ and $132 \equiv 2 \bmod 5$. For the same reason as before, we solve the presented system of equations instead of the one involving $x'' \equiv 1 \bmod 5$. Hence $x''=132$

Then we try to solve:
$x''' \equiv 1 \bmod 11$
$x''' \equiv 0 \bmod (5 \cdot 6)$

We perform extended euclidean algorithm since the solution is not immediately obvious:

i	q_i	r_i	x_i	y_i
0	-	30	1	0
1	-	11	0	1
2	2	8	1	-2
3	1	3	-1	3
4	2	2	3	-8
5	1	1	-4	11

$(5 \cdot 6) \cdot (-4) = -120$ and $-120 \equiv 1 \pmod{11}$. Hence $x''' = -120$

By Chinese remainder theorem, $x \equiv x' + x'' + x''' = 165 + 132 - 120 = 177 \pmod{330}$ is the set of solutions to $x \equiv 3 \bmod 6$, $x \equiv 2 \bmod 5$ and $x \equiv 1 \bmod 11$.

3.
a) We perform the Extended Euclidean algorithm:

i	q_i	r_i	x_i	y_i
0	-	198	1	0
1	-	5	0	1
2	39	3	1	-39
3	1	2	-1	40
4	1	1	2	-79
5	2	0	-5	198

Hence, $2 \cdot 198 - 79 \cdot 5 = 1 \Rightarrow 5 \cdot 79 \equiv 1 \pmod{198} \Rightarrow [5]_{198}^{-1} = [-79]_{198} = [119]_{198}$

b. Solving $[5]_{198}^{-1}$ is equivalent to finding $x \in Z/198Z$ such that $5x \equiv 1 \pmod{198}$. We know that 198 can prime factorized to be $2 \cdot 3^2 \cdot 11$.

By Chinese Remainder Theorem, $5x \equiv 1 \pmod{198} \Leftrightarrow 5x \equiv 1 \pmod 2$, $5x \equiv 1 \pmod 9$ and $5x \equiv 1 \pmod{11}$.

So first we consider the system:
$5x' \equiv 1 \pmod 2 \Leftrightarrow x' \equiv 1 \pmod 2$ and
$x' \equiv 0 \pmod{9 \cdot 11}$

Obviously, $x' = (9 \cdot 11) \cdot 1$ would satisfy the above system.

Next we consider the following system:
$5x'' \equiv 1 \pmod 9 \Leftrightarrow x'' \equiv 2 \pmod 9$ and
$x' \equiv 0 \pmod{2 \cdot 11}$

I	q_i	r_i	x_i	y_i
0	-	22	1	0
1	-	9	0	1
2	2	4	1	-2
3	2	1	-2	5

$-2 \cdot 22 + 5 \cdot 9 = 1 \Rightarrow -44 \equiv 1 \pmod 9$ and $-44 \equiv 0 \pmod{2 \cdot 11} \Leftrightarrow -88 \equiv 2 \pmod 9$ and $-88 \equiv 0 \pmod{2 \cdot 11}$
One can regard the previous step as finding the w_1 as defined in CRT, and then multiply by "a" (2 in this case).
Hence, $x'' = -88$ is a solution.

Next, we consider the following system:
$5x''' \equiv 1 \pmod{11} \Leftrightarrow x''' \equiv 9 \pmod{11}$ and

$5x''' \equiv 0 \pmod{2 \cdot 3^2}$

I	q_i	r_i	x_i	y_i
0	-	18	1	0
1	-	11	0	1
2	1	7	1	-1
3	1	4	-1	2
4	1	3	2	-3
5	1	1	-3	5

EGCD => $-3(18)+5 \cdot 11 = 1$ => $-54 \equiv 1 \pmod{11}$ => $-486 \equiv 9 \pmod{11}$

By Chinese Remainder Theorem then, $x \equiv x' + x'' + x'''$ (we are not dealing with the weights as defined in CRT in this sum, but x', x'', x''' are the product of the corresponding weights and the corresponding constant "a_i" as defined in CRT in p.46 of text) = 99-88-486 = -475 ≡ 119(mod 198). We check that $5 \cdot 119 \equiv 1 \pmod{198}$, hence $[119]_{198}$ is indeed $[5]_{198}^{-1}$

4.
Since (2,31)=1, by Fermat's Theorem, $2^{30} \equiv 1 \pmod{31}$. Hence, $2^{127} = 2^{30 \cdot 4 + 7} = (2^{30})^4 \cdot 2^7 \equiv 2^7 = 2^5 \cdot 2^2 \equiv 2^2 = 4 \pmod{31}$.

5.
We use Theorem 1.11.3 (ii) which states that $a^p \equiv a \pmod{p}$ where p is prime and a is an integer. Theorem 1.11.3 (ii) follows directly from Fermat's Theorem, as shown in the text.

Claim 1: $(a+b)^p \equiv a^p + b^p \pmod{p}$, where a, b, and p are as defined in the problem.
$(a+b)^p \equiv a+b \pmod{p}$ by Theorem 1.11.3 (ii).

We notice that $a^p \equiv a \pmod{p}$ and $b^p \equiv b \pmod{p}$ by Theorem 1.11.3 (ii), hence,
$(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}$.

Claim 2: $(a-b)^p \equiv a^p - b^p \pmod{p}$, where a, b, and p are as defined in the problem.
$(a-b)^p \equiv a-b \pmod{p}$ by Theorem 1.11.3 (ii).

We notice that $a^p \equiv a \pmod{p}$ and $b^p \equiv b \pmod{p}$ by Theorem 1.11.3 (ii), hence,
$(a-b)^p \equiv a-b \equiv a^p - b^p \pmod{p}$.

Claim 1 and Claim 2 shows $(a+b)^p \equiv a^p + b^p \pmod{p}$ and $(a-b)^p \equiv a^p - b^p \pmod{p}$.

6.
For element $7 \in (Z/12)^*$:
Since $\varphi(12) = \varphi(3)\varphi(2^2) = 2 \cdot 2 = 4$, and by lemma 1.11.6, order m of this element must divide 4. Hence, the possible orders are 1,2, and 4 (we do not need to consider any larger integers because we are guaranteed that $7^4 \equiv 1$, but it might not be the least positive integer m such that $7^m \equiv 1$) . We try them in order:

We see that 7^1-1=6(mod 12) and 7^2-1≡1(mod 12). Hence, m =2.

For element $2 \in (Z/29)^*$:
Since $\varphi(29) = 28$ because 29 is a prime, and by lemma 1.11.6, order m of this element must divide 28. Hence, the possible orders are 1,2, 4, 7, 14 and 28 (we do not need to consider any larger integers because we are guaranteed that 2^{28}≡1, but it might not be the least positive integer m such that 2^m≡1). We try them in order:

We see that 2^i<29 for i=1,2 and 4, and not congruent to 1 (mod 29). We see that 2^7≡12 ≠ 1(mod 29) and 2^{14}≡$(2^7)^2$≡ 144 ≠ 1(mod 29). Hence, in fact, 28 is the order of the element $2 \in (Z/29)^*$.

7.
In the RSA scheme, we know that ed≡1 (mod $\varphi(n)$) , where e, d and n are as defined in the RSA scheme. Give the prime factorization of n=1022117=1009·1013, we first find $\varphi(n) = \varphi(1009)\varphi(1013)$. Hence, $\varphi(n) = 1008 \cdot 1012 = 1020096$ by theorem in text.

Now our task becomes finding d s.t. 816077d≡1 (mod 1020096). We apply the EGCD algorithm:

i	q_i	r_i	x_i	y_i
0	-	1020096	1	0
1	-	816077	0	1
2	1	204019	1	-1
3	4	1	-4	5

We see that 1020096(-4)+ 816077(5)=1 <=> 1020096| 816077(5)-1 <=> 816077(5) ≡1 (mod 1020096).

We have found the unique inverse for e, which we called d, to be 5.

Now we calculate c_i^5 mod 1022117**:**
For c_1=477727
477727^5≡$477727^{2\cdot2}$·477727≡ $(714301)^2$·477727≡443956·477727≡490512 (mod 1022117)

According to the table in pg 60, this represents the codes 49,05,12, which represents the alphabets: Wel

For c_2=304514
304514^5≡$304514^{2\cdot2}$·304514≡ $(277722)^2$·304514≡560464·304514≡126304 (mod 1022117)
According to the table in pg 60, this represents the codes 12,63,04, which represents the alphabets: l d

For c_3=355080
355080^5≡$355080^{2\cdot2}$·355080≡ $(608099)^2$·355080≡861307·355080≡151405 (mod 1022117)
According to the table in pg 60, this represents the codes 15,14,05, which represents the alphabets: one

For c_4=295177
$295177^5 \equiv 295177^{2\cdot 2}\cdot 295177 \equiv (119781)^2\cdot 295177 \equiv 31632\cdot 295177 \equiv 69 \pmod{1022117}$
According to the table in pg 60, this represents the code 69, which represents the alphabets:!

So in summary, the message is "Well done!" (sans quote).

8.
a. Using the definition of g_0, f_0, g_i, and f_i, we see that g_i is a bounded monotically decreasing sequence: by definition of gcd, $f_i \geq 1$; together with $g_0 \geq 1 \Rightarrow g_i \geq 1$ for all $i \geq 0$. Hence, g_i is bounded. Hence, it is clear that g_i is bounded, and monotically decreasing (since we are dividing by integers(since clearly $f_i | g_{i+1}$.)), and assumes finite number of values (i.e. the values are a subset from the set $\{1,2, \ldots g_0\}$). Hence, there exists integers i and j s.t. $g_i = g_j$ where i=j-1. By definition, $g_j = \frac{g_i}{f_i}$. $g_i = g_j \Rightarrow f_i = 1$.

b.

Claim B0: gcd(a,bc)=gcd(a,b) if gcd(a,c)=1 where a, b and c are integers
gcd(a,c) <=> ax+cy = 1 for some integers x and y
Write gcd(a,b) = d. This implies, there exists integers x' and y' such that ax'+by'=d.
Notice that (ax'+by')·(ax+cy) = a(ax'x+x'cy+bxy')+bc(yy') = d, gcd(a,bc)=d.

Claim B1: gcd(gcd(a,b),c)=gcd(a,gcd(b,c))
Proof:
Let d be the gcd(gcd(a,b),c). This implies d|gcd(a,b) and d|c. d|gcd(a,b) => d|a and d|b. Because d|b and d|c, d|gcd(b,c). d|gcd(b,c) and d|a => d|gcd(a,gcd(b,c)).

Similarly, let e be gcd(a,gcd(b,c)). This implies e| gcd(b,c) and e|a. e|gcd(b,c)=>e|b and e|c. Because e|a and e|b, e|gcd(a,b). e|gcd(a,b) and e|c => e| gcd(gcd(a,b),c)=d.

Since e|d and d|e, e=d, completing our proof.

We will proceed by induction. We will show that $\varphi(n) \mid g_i$ for i=0.
By definition of e_2 and d_2, $e_2\cdot d_2 \equiv 1 \pmod{\varphi(n)}$. Hence, $e_2\cdot d_2 - 1 = (k_0\cdot\varphi(n))$, for some integer k_0.
Hence, $\varphi(n) \mid g_0$

Suppose $\varphi(n) \mid g_i$ for some i=n (as our induction hypothesis). We will show that this implies $\varphi(n) \mid g_{n+1}$
(**) By definition of e_1, e_1 is an invertible element in $Z/\varphi(n)$ <=> $\gcd(e_1, \varphi(n)) = 1$. By induction hypothesis, $\varphi(n) \mid g_n$ <=> $g_n = k_n\cdot\varphi(n)$ for some integer k_n. Hence, by claim B0, $f_n = \gcd(e_1, g_n) = \gcd(e_1, k_n\varphi(n)) = \gcd(e_1, k_n)$. Furthermore, by Claim B1, $\gcd(f_n, \varphi(n)) = \gcd(\gcd(e_1, g_n), \varphi(n)) = \gcd(\gcd(e_1, \varphi(n)), g_n) = 1$. Therefore, $f_n \mid g_n = k_n\cdot\varphi(n) \Rightarrow f_n \mid k_n$.

By definition, $g_{n+1} = \frac{k_n\varphi(n)}{f_n}$. By (**), We can write $g_{n+1} = \frac{k_n}{f_n}\varphi(n)$ <=> $\varphi(n) \mid g_{n+1}$.

This completes our induction.

Hence $g=g_I$ where I is as defined in problem and $I \geq 0$, $\varphi(n) \mid g$.

c) By selection of $g=g_I$, we have $f_I = \gcd(e_1, g_I) = 1$. Hence, by a theorem, there exists integers s and t such that $sg_I + te_1 = 1 \Rightarrow g_I \mid te_1 - 1 \Rightarrow e_1 t \equiv 1 \pmod{g_I} \Leftrightarrow e_1 t \equiv 1 \pmod{g}$

d) By b), we can write $g = \varphi(n) k_I$ for some integer k_I. By c), $\varphi(n) k_I = g = g_I \mid te_1 - 1 \Rightarrow \varphi(n) \mid te_1 - 1 \Rightarrow e_1 t \equiv 1 \pmod{\varphi(n)}$

e) From part d), we have that $e_1 t = \varphi(n) k_I + 1$ for some integer k_I. Hence, $(m^{e_1})^t = m^{e_1 t} = m^{\varphi(n)(k_I)+1} = m^{\varphi(n)(k_I)} \cdot m = 1^{(k_I)} \cdot m = m \pmod{n}$. The second last result follows from Euler's Theorem because gcd(n,m)=1.

Homework #4

1.
Suppose, by way of contradiction, that the identity is not unique. Then there exists I_R and $w \in R$ s.t. $a \cdot w = w \cdot a = a$ and $a \cdot I_R = I_R \cdot a = a$ for all a in R, and $w \neq I_R$.

a) $a \cdot w = w \cdot a = a \Rightarrow I_R \cdot w = w \cdot I_R = I_R$

b) $a \cdot I_R = I_R \cdot a = a \Rightarrow w \cdot I_R = I_R \cdot w = w$.

Claim a+Claim b $\Rightarrow I_R = w = w \cdot I_R = I_R \cdot w$. We reached a contradiction, and hence identity is unique.

2a.
In each case, we need to check the 6 properties for $(R,+,\cdot)$
Let f, g, and h be real valued functions (and hence an element in R)

(0) Since + and · are given to be well defined maps, R is closed with respect to the two operations.
i) We need to check f+(g+h)=(f+g)+h:

f+(g+h): $\begin{matrix} R \to R \\ a \mapsto f(a) + (g(a) + h(a)) \end{matrix}$
(f+g)+h: $\begin{matrix} R \to R \\ a \mapsto (f(a) + g(a)) + h(a) \end{matrix}$
Clearly, f+(g+h)= (f+g)+h because $f(a) + (g(a) + h(a)) = (f(a) + g(a)) + h(a)$ since real value addition is associative.

ii) We need to check f+g=g+f
f+(g+h): $\begin{matrix} \mathbb{R} \to \mathbb{R} \\ a \mapsto f(a) + g(a) \end{matrix}$
(f+g)+h: $\begin{matrix} \mathbb{R} \to \mathbb{R} \\ a \mapsto g(a) + f(a) \end{matrix}$
Clearly, f+g= g+f because $f(a) + g(a) = g(a) + f(a)$ since real value addition is commutative.

iii) We need to check there exists element 0_R s.t. $f+0_R=f$
$0_R : \begin{matrix} \mathbb{R} \to \mathbb{R} \\ a \mapsto 0 \end{matrix}$ is a function that always returns the real value 0. We see that $f+0_R$ is f because then by definition of addition, $f+0_R = \begin{matrix} \mathbb{R} \to \mathbb{R} \\ a \mapsto f(a) + 0 \end{matrix} \Rightarrow f+0_R = \begin{matrix} \mathbb{R} \to \mathbb{R} \\ a \mapsto f(a) \end{matrix}$

iv) We need to check there exists element denoted –f s.t. $f+(-f)=0_R$

Let f' be a real value function s.t. if f(a)=b, then f'(a)=-b. Then by definition of addition, f+f'= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)+f'(a)\end{matrix}$ = $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto b-b\end{matrix}$ = $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto 0\end{matrix}$ =0_R. We rewrite f' as –f.

v) We need to check (f·g)·h = f·(g·h)

By definition of multiplication and addition, (f·g)·h= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto (f(a)\cdot g(a))\cdot h(a)\end{matrix}$. But since real values are associative, this is just (f·g)·h= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)\cdot (g(a)\cdot h(a))\end{matrix}$. Since f·(g·h) = $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)\cdot (g(a)\cdot h(a))\end{matrix}$, we see (f·g)·h = f·(g·h).

vi) We need to check f·(g+h)=f·g+f·h and (g+h)·f= g·f+h·f

By definition of multiplication and addition, f·(g+h)= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)\cdot (g(a)+h(a))\end{matrix}$. Since real values are distributive, we can rewrite f·(g+h)= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)g(a)+f(a)h(a)\end{matrix}$. But then f·g+f·h= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto f(a)g(a)+f(a)h(a)\end{matrix}$, so f·(g+h)= f·g+f·h.

Similarly, by definition of multiplication and addition, (g+h)·f= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto (g(a)+h(a))\cdot f(a)\end{matrix}$. Since real values are distributive, we can rewrite (g+h)·f= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto g(a)f(a)+h(a)f(a)\end{matrix}$. But then g·f+h·f= $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto g(a)f(a)+h(a)f(a)\end{matrix}$, so (g+h)·f= g·f+h·f.

Since (R,+,·) satisfies properties (0) to (vi), R is a ring.

2b)
Property (vi) <Multiplicative distributivity is violated>

Consider f: $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto a+1\end{matrix}$, g: $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto 3a\end{matrix}$ and h: $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto 7a\end{matrix}$, then if (R,+,o) is a ring, then by (vi), f(g+h)=fg+fh. But f(g+h): $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto (3a+7a)+1\end{matrix}$, and fg+fh: $\begin{matrix}\mathbb{R}\to\mathbb{R}\\ a\mapsto (3a+1)+(7a+1)\end{matrix}$, and clearly, $(3a+7a+1)\neq(3a+1)+(7a+1)$. Hence, there exists f, g, and h in R s.t. (vi) is not satisfied with respect to the defined operations. Hence, (R, +, o) is not a ring.

3.

From lecture, we know that **C** (complex numbers with usual addition and multiplication) is a ring. It is therefore sufficient to show R is a subring of **C**.
Clearly, R is a subset of **C**. R is also non-empty – if we let a=b=0, we see that the zero element is in R.
Let R = {a+ib}: a,b $\in$ **Z**}
By Lemma 2.2.4, R is a subring if R is closed under +, - and multiplication
It is straightforward to check that if a, b, c, d $\in$ **Z**, then a+ib $\in$ R, and c+id$\in$ R. We see that (a+ib) + (c+id) = (a+c) + (ib+id) (by associatively of complex numbers) = (a+c) + i(b+d) (by distributivity of complex numbers). (a+c) + i(b+d) is in R because a+c and b+d are both integers.

Similarly, it is closed under -:
If a, b, c, d $\in$ **Z**, then a+ib $\in$ R, and c+id$\in$ R. We see that (a+ib) - (c+id) = (a+c) - (ib+id) (by associatively of complex numbers) = (a+c) - i(b+d) (by distributivity of complex numbers) = (a+c) + i(-b-d). (a+c) + i(-b-d) is in R because a+c and -b-d are both integers.

It is also closed under multiplication:
If a, b, c, d $\in$ **Z**, then a+ib $\in$ R, and c+id$\in$ R. We see that (a+ib)·(c+id) = ac+aid+ibc+ibid (by distributivity of complex numbers) = ac+ibid+aid+ibc (by associativity of complex numbers) = ac-bd+aid+ibc= ac-bd+iad+ibc (by multiplicative associatively) = ac-bd+i(ad+bc) (by distributivity of complex numbers). ac-bd+i(ad+bc) is in R because ac-bd and ad+bc are both integers.

It is easy to see that (1+i0) is the identity element in R since (1+i0)·(a+ib)= (a+ib), where (a+ib) $\in$ R.

Now for which elements are invertible:
For each element (a+ib) $\in$ R, we want to find integers c and d s.t. (c+id) $\in$ R and (a+ib)(c+id) $=1_R$=(1+i0). Hence, we have to solve ac-bd=1 and ad+bc=0.

If a=0, and b=0, then (a+ib) = 0_R and clearly no inverse exists.
If a=0 and b$\neq$ 0, then –bd=1 and bc=0 => b=1, d=-1, c=0 or b=-1, d=1, c=0. Hence, 0+1i and 0+(-1)i are invertible elements in R and their inverses are 0+(-1)i and 0+1i respectively.

If a$\neq$ 0, then ac-bd=1=> ac=1+bd => a|1+bd => c=$\frac{1+bd}{a}$ => ad+b$\frac{1+bd}{a}$=0 => a^2d+b(1+bd)=0
a^2d+b^2d+b=0 => d(a^2+b^2)=-b.

Also, if a$\neq$ 0, then ad+bc=0 => ad=-bc => a|-bc => d=$\frac{-bc}{a}$ => ac+$\frac{b^2c}{a}$=1 => a^2c+b^2c=a =>
c(a^2+b^2)=a

Hence, we see that c and d $\in$ **Z** iff (a^2+b^2)|a and (a^2+b^2)|-b. Since $a^2\geq$a, $\frac{a}{a^2+b^2}$ $\in$ **Z** iff b^2=0,
because a^2+b^2 |a only if $a^2+b^2 \leq$ a. If b=0 and a^2|a then $\frac{a}{a^2+b^2}$ $\in$ **Z**. a^2|a and a|a^2 <=> $a=a^2$
=> a=-1 or a=1 since a $\in$ **Z**. Hence, we have that if a$\neq$ 0, only 1+0i and -1+0i are invertibles.

In sum, 0+1i, 0+(-1)i, 1+0i and -1+0i are the only invertible elements in R.

4a.

The identity of $M_2(\mathbf{Z}/3)$ is $\begin{pmatrix}[1]_3 & [0]_3\\ [0]_3 & [1]_3\end{pmatrix}$. It is easy to see that for any $a\in M_2(\mathbf{Z}/3)$, i.e. $a=\begin{pmatrix}b & c\\ d & e\end{pmatrix}$, where b, c, d and e $\in (\mathbf{Z}/3)$, we have $\begin{pmatrix}[1]_3 & [0]_3\\ [0]_3 & [1]_3\end{pmatrix}\cdot\begin{pmatrix}b & c\\ d & e\end{pmatrix}=\begin{pmatrix}b & c\\ d & e\end{pmatrix}\cdot\begin{pmatrix}[1]_3 & [0]_3\\ [0]_3 & [1]_3\end{pmatrix}=\begin{pmatrix}b & c\\ d & e\end{pmatrix}$.

4b.

We know that $\#(\mathbf{Z}/3) = 3$. Each entry in $M_2(\mathbf{Z}/3)$ can take on 3 values, so there are 3^4 possible elements in $M_2(\mathbf{Z}/3)$.

4c.

Let $A\in M_2(\mathbf{Z}/3)$. Write $A=\begin{pmatrix}b & c\\ d & e\end{pmatrix}$, where b, c, d and e $\in (\mathbf{Z}/3)$. Write $a'=\begin{pmatrix}b' & c'\\ d' & e'\end{pmatrix}$ where b', c', d' and e' $\in (\mathbf{Z}/3)$ and $b+b'=[0]_3$, $c+c'=[0]_3$, $d+d'=[0]_3$, and $e+e'=[0]_3$. We rename a' to –A. It is easy to see then $A+(-A)=\begin{pmatrix}[0]_3 & [0]_3\\ [0]_3 & [0]_3\end{pmatrix}$=Zero in $M_2(\mathbf{Z}/3)$. In particular, since for all entries a_{ij}, $a_{ij} + 2a_{ij} = [0]_3$, -A=2A.

4d.

No, $M_2(\mathbf{Z}/3)$ is not commutative. Let $A=\begin{pmatrix}[2]_3 & [2]_3\\ [2]_3 & [2]_3\end{pmatrix}\in M_2(\mathbf{Z}/3)$, and $B=\begin{pmatrix}[1]_3 & [2]_3\\ [1]_3 & [0]_3\end{pmatrix}\in M_2(\mathbf{Z}/3)$. Observe that $A\cdot B=\begin{pmatrix}[1]_3 & [1]_3\\ [1]_3 & [1]_3\end{pmatrix}$ and $B\cdot A=\begin{pmatrix}[0]_3 & [0]_3\\ [2]_3 & [2]_3\end{pmatrix}$. Clearly $AB\neq BA$.

4e. $\begin{pmatrix}[0]_3 & [1]_3\\ [2]_3 & [0]_3\end{pmatrix}$ is an invertible element and its inverse is $\begin{pmatrix}[0]_3 & [2]_3\\ [1]_3 & [0]_3\end{pmatrix}$ since

$$\begin{pmatrix}[0]_3 & [1]_3\\ [2]_3 & [0]_3\end{pmatrix}\begin{pmatrix}[0]_3 & [2]_3\\ [1]_3 & [0]_3\end{pmatrix}=\begin{pmatrix}[1]_3 & [0]_3\\ [0]_3 & [1]_3\end{pmatrix}$$

$\begin{pmatrix}[0]_3 & [0]_3\\ [0]_3 & [0]_3\end{pmatrix}$ is a non-invertible element.

5. Let $R= M_n(\mathbf{Z}/m)$

$A=\begin{pmatrix} [1]_m & [0]_m & \dots & [0]_m \\ [0]_m & [1]_m & . & . \\ . & \dots & [1]_m & . \\ [0]_m & .... & [0]_m & [1]_m \end{pmatrix}$ is the identity of R, where if $a_{ij}=[1]_m$ if i=j and $a_{ij}=[0]_m$ otherwise, where a_{ij} is the entry at column i row j.

We know that $n[1]_m = [0]_m$ iff n=m. We want to find positive characteristics c s.t. $cA=0_R=\begin{pmatrix} [0]_m & [0]_m & \dots & [0]_m \\ [0]_m & [0]_m & . & \vdots \\ \vdots & \dots & [0]_m & \vdots \\ [0]_m & .... & [0]_m & [0]_m \end{pmatrix}$. Equivalently, c s.t. $ca_{ij}=[0]_m$. This implies c=m.

Hence, the characteristics of $M_n(\mathbf{Z}/m)=m$.

6a. $F = (\{[0]_6,[3]_6\},+,\cdot)$ is isomorphic to $\mathbf{Z}/2$.
It is easy to see that F is non-empty, and it's closed under multiplication, subtraction and addition. F is a subring of $\mathbf{Z}/6$.

$$\mathbb{Z}/6 \to \mathbb{Z}/2$$

Let $\varphi : \begin{Bmatrix} [0]_6 \mapsto [0]_2 \\ [3]_6 \mapsto [1]_2 \end{Bmatrix}$. Clearly, φ is bijective.

φ respects addition:
$\varphi(a+b)= \varphi(a)+ \varphi(b)$, where a and b are elements of $\mathbf{Z}/6$:
$\varphi(0+0)= \varphi([0]_6)+ \varphi([0]_6)=[0]_2$
$\varphi(0+3)= \varphi([0]_6)+ \varphi([3]_6)=[1]_2$
$\varphi(3+3)= \varphi([3]_6)+ \varphi([3]_6)=[0]_2$

φ respects multiplication:
$\varphi(a\cdot b)= \varphi(a)\cdot \varphi(b)$, where a and b are elements of $\mathbf{Z}/6$:
$\varphi(0\cdot 0)= \varphi([0]_6)\cdot \varphi([0]_6)=[0]_2$
$\varphi(0\cdot 3)= \varphi([0]_6)\cdot \varphi([3]_6)=[0]_2$
$\varphi(3\cdot 3)= \varphi([3]_6)\cdot \varphi([3]_6)=[1]_2$

φ is isomorphism. Hence, F and $\mathbf{Z}/2$ are isomorphic.

From the multiplication table, we see that $[3]_6$ is the identity in F.

6b. $G = (\{[0]_6,[2]_6,[4]_6\},+,\cdot)$ is isomorphic to $\mathbf{Z}/3$.
It is easy to see that G is non-empty, and it's closed under multiplication, subtraction and addition. G is a subring of $\mathbf{Z}/6$.

$$\mathbb{Z}/6 \to \mathbb{Z}/3$$

Let $\varphi: \begin{Bmatrix} [0]_6 \mapsto [0]_3 \\ [2]_6 \mapsto [1]_3 \\ [4]_6 \mapsto [2]_3 \end{Bmatrix}$. Clearly, φ is bijective.

φ respects addition:

$\varphi(a+b)= \varphi(a)+ \varphi(b)$, where a and b are elements of **Z**/6:

$\varphi(0+0)= \varphi([0]_6)+ \varphi([0]_6)=[0]_3$

$\varphi(0+2)= \varphi([0]_6)+ \varphi([2]_6)=[2]_3$

$\varphi(0+4)= \varphi([0]_6)+ \varphi([4]_6)=[1]_3$

$\varphi(2+2)= \varphi([2]_6)+ \varphi([2]_6)=[1]_3$

$\varphi(2+4)= \varphi([2]_6)+ \varphi([4]_6)=[0]_3$

$\varphi(4+4)= \varphi([4]_6)+ \varphi([4]_6)=[2]_3$

φ respects multiplication:

$\varphi(a \cdot b)= \varphi(a) \cdot \varphi(b)$, where a and b are elements of **Z**/6:

$\varphi(0 \cdot 0)= \varphi([0]_6) \cdot \varphi([0]_6)=[0]_3$

$\varphi(0 \cdot 2)= \varphi([0]_6) \cdot \varphi([2]_6)=[0]_3$

$\varphi(0 \cdot 4)= \varphi([0]_6) \cdot \varphi([4]_6)=[0]_3$

$\varphi(2 \cdot 2)= \varphi([2]_6) \cdot \varphi([2]_6)=[1]_3$

$\varphi(2 \cdot 4)= \varphi([2]_6) \cdot \varphi([4]_6)=[2]_3$

$\varphi(4 \cdot 4)= \varphi([4]_6) \cdot \varphi([4]_6)=[1]_3$

φ is isomorphism. Hence, G and **Z**/3 are isomorphic.

From the multiplication table, we see that $[4]_6$ is the identity in G.

7.

φ is isomorphism => φ is bijective => φ^{-1} is also bijective.

Hence, we only need to check if φ^{-1} respects multiplication and addition.

Claim 1: φ^{-1} respects addition:

Proof:

Since φ is injective, $\varphi(a)= \varphi(b)$ iff a=b. To show $\varphi^{-1}(a+b)= \varphi^{-1}(a)+ \varphi^{-1}(b)$, we show instead $\varphi(\varphi^{-1}(a+b))= \varphi(\varphi^{-1}(a)+ \varphi^{-1}(b))$.

LHS = a+b, since φ and φ^{-1} are inverses of each other.

RHS = $\varphi(\varphi^{-1}(a))+ \varphi(\varphi^{-1}(b))$ since φ is homomorphic = a+b, since φ and φ^{-1} are inverses of each other.

LHS=a+b=RHS => φ^{-1} respects addition

Claim 2: φ^{-1} respects multiplication:
Proof:
Since φ is injective, $\varphi(a)=\varphi(b)$ iff a=b. To show $\varphi^{-1}(a\cdot b)=\varphi^{-1}(a)\cdot\varphi^{-1}(b)$, we show instead $\varphi(\varphi^{-1}(a\cdot b))=\varphi(\varphi^{-1}(a)\cdot\varphi^{-1}(b))$.

LHS = a·b, since φ and φ^{-1} are inverses of each other.
RHS = $\varphi(\varphi^{-1}(a))\cdot\varphi(\varphi^{-1}(b))$ since φ is homomorphic = a+b, since φ and φ^{-1} are inverses of each other.

LHS=a·b=RHS => φ^{-1} respects multiplication

Claim 1+Claim 2 implies φ^{-1} is homomorphic. Since φ^{-1} is bijective, φ^{-1} is isomorphic.

8.
We will proof by way of contradiction. Suppose **Z**/3 x **Z**/3 and **Z**/9 are isomorphic. It is easy to see that **Z**/3 x **Z**/3 has identity ($[1]_3$, $[1]_3$) and zero ($[0]_3$,$[0]_3$).
It is easy to see that **Z**/9 has identity $[1]_9$ and zero $[0]_9$.

By a theorem, if two rings are isomorphic, then their characteristics are equal. However, **Z**/3 x **Z**/3 has characteristics 3 (since $3\cdot([1]_3, [1]_3)=([0]_3,[0]_3)$), but **Z**/9 has characteristics 9 (9 is the small integer m s.t. $m[1]_9=[0]_9$). Hence, **Z**/3 x **Z**/3 and **Z**/9 are not isomorphic.

9.
a. By a theorem, I is a subring of R if I is a non-empty subset of R and I is closed under multiplication, subtraction and addition.

Let a and b $\in$ R s.t. $\varphi(a)=\varphi(b)=0_S$. Hence, a and b $\in$ I.
We want to show that a+b$\in$ I:
We see that $\varphi(a+b)=\varphi(a)+\varphi(b)=0_S+0_S=0_S$. The last result follows from the fact that φ is a homomorphism. Hence, a+b$\in$ I.

Similarly, we see that $\varphi(a-b)=\varphi(a)-\varphi(b)=0_S-0_S=0_S$. The last result follows from the fact that φ is a homomorphism. Hence, a-b$\in$ I.

Similarly, we see that $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)=0_S\cdot 0_S=0_S$. The last result follows from the fact that φ is a homomorphism. Hence, a·b$\in$ I.

Hence, I is a subring of R.

b. If b$\in$ I, then by definition, φ(b)=0. Consider φ(ab). By the fact that φ is a homomorphism, φ(ab)= φ(a) φ(b) = φ(a)$\cdot 0_S = 0_S$. The last result follows from the axiom of 0_S in S. Hence, ab$\in$ I.

Similarly, consider φ(ba). By the fact that φ is a homomorphism, φ(ba)= φ(b) φ(a) = φ(b)$\cdot 0_S = 0_S$. The last result follows from the axiom of 0_S in S. Hence, ba$\in$ I.

c.
By definition, a~b iff φ(a)= φ(b)
<=> φ(a)- φ(b) = 0_S (the axiom of 0_S and additive inverse in S)
<=> φ(a-b) = 0_S (φ is homomorphic)
<=> a-b$\in$ I (definition of I)

Hence, a~b iff a-b$\in$ I.

10.
Claim 1: If $f \in$ F[x] is a nonzero constant polynomial then f is invertible
Proof:
Since f is a nonzero constant polynomial, $f \in$ F. F is a field, so all nonzero elements are invertible => f is invertible.

Claim2: If f is invertible, then $f \in$ F[x] is a nonzero constant polynomial
Proof:
We will prove the contrapositive: If $f \in$ F[x] is not a nonzero constant polynomial then f is not invertible
Case1: Suppose f is the zero polynomial. Clearly f is invertible would imply 0 in F is invertible, which is a contradiction. f is not invertible if f is the zero polynomial.

Case 2: Suppose deg(f)=d_f>0 (i.e. f is not a nonzero constant polynomial and f is not the zero polynomial). Suppose, by way of contradiction, that there exists polynomial g of degree d_g s.t. f$\cdot$g = 1_F. By lemma 2.4.1, F is a field => deg(f$\cdot$g) = d_f+d_g => d_f+d_g=0 = deg(1_F). But d_f>0 and d_g is non-negative, so we have reached a contradiction => no such g exists => f is not invertible if deg(f) >0.

Case 1 + Case 2 => If $f \in$ F[x] is not a nonzero constant polynomial then f is not invertible

Claim1+Claim 2 => $f \in$ F[x] is a nonzero constant polynomial iff f is invertible

11.
We will show by construction.
Let φ_1 be the isomorphism from R to S.
Define $\varphi_2 : \begin{matrix} R[x] \to S[x] \\ r_m x^m + r_{m-1}x^{m-1} + \ldots + r_1 x^1 + r_0 \mapsto \varphi_1(r_m)x^m + \varphi_1(r_{m-1})x^{m-1} + \ldots + \varphi_1(r_1)x^1 + \varphi_1(r_0) \end{matrix}$, where m is the degree of the polynomial and r_i are the coefficients.

We will show φ_2 is an isomorphism, which would imply R[x] and S[x] are isomorphic rings.

Clearly φ_2 is injective, because φ_1 is injective:
Let f and g $\in$ R[x], and f$\neq$ g (i.e. there exists an index $0\leq i\leq \max(\deg(f),\deg(g))$ s.t. $f_i \neq g_i$ where f_i and g_i are the indexed coefficients of the polynomials f and g)
Since $\varphi_1(f_i) \neq \varphi_1(g_i)$ (follows from the fact that φ_1 is homomorphism), $\varphi_2(f) \neq \varphi_2(g)$ because the i^{th} coefficient is different.

Clearly φ_2 is surjective, because φ_1 is surjective:
Let g $\in$ S[x].
Write $g=g_{\deg(g)}x^g+\ldots g_1x^1+g_0$. Because φ_1 is surjective, there exists $f_{\deg(g)}, f_{\deg(g)-1},\ldots,f_1, f_0$ in R s.t. $\varphi_1(f_{\deg(g)})= g_{\deg(g)}, \varphi_1(f_{\deg(g)-1})= g_{\deg(g)-1}, \ldots, \varphi_1(f_0)= g_0$. Write $f= \varphi_1^{-1}(g_{\deg(g)})x^g+\ldots+ \varphi_1^{-1}g_0$.
Clearly, $\varphi_2(f)=g$.
Hence, φ_2 is surjective.

Claim 1: φ_2 respects addition
Proof:
Let a', b' $\in$ R[x].
Write $a'=a_{\deg(a)}x^{\deg(a)}+a_{\deg(a)-1}x^{\deg(a)-1}+\ldots+a_1x^1+a_0$.
Write $b'=b_{\deg(b)}x^{\deg(b)}+b_{\deg(b)-1}x^{\deg(b)-1}+\ldots+b_1x^1+b_0$.
Without loss of generality, let deg(a)>deg(b):
(a'+b')
$=a_{\deg(a)}x^{\deg(a)}+a_{\deg(a)-1}x^{\deg(a)-1}+\ldots+a_1x^1+a_0+b_{\deg(b)}x^{\deg(b)}+b_{\deg(b)-1}x^{\deg(b)-1}+\ldots+b_1x^1+b_0$
$=a_{\deg(a)}x^{\deg(a)}+a_{\deg(a)-1}x^{\deg(a)-1}+\ldots+(a_{\deg(b)}+b_{\deg(b)})x^{\deg(b)}+(a_{\deg(b)-1}+b_{\deg(b)-1})x^{\deg(b)-1}+\ldots+(a_1+b_1)x^1+a_0+b_0$
$\Rightarrow \varphi_2$ (a'+b')
$=\varphi_1(a_{\deg(a)})x^{\deg(a)}+\varphi_1(a_{\deg(a)-1})x^{\deg(a)-1}+\ldots+\varphi_1(a_{\deg(b)}+b_{\deg(b)})x^{\deg(b)}+\varphi_1(a_{\deg(b)-1}+b_{\deg(b)-1})x^{\deg(b)-1}+\ldots+\varphi_1(a_1+b_1)x^1+\varphi_1(a_0+b_0)$
$=\varphi_1(a_{\deg(a)})x^{\deg(a)}+\varphi_1(a_{\deg(a)-1})x^{\deg(a)-1}+\ldots+(\varphi_1(a_{\deg(b)})+\varphi_1(b_{\deg(b)}))x^{\deg(b)}+(\varphi_1(a_{\deg(b)-1})+\varphi_1(b_{\deg(b)-1}))x^{\deg(b)-1}+\ldots+(\varphi_1(a_1)+\varphi_1(b_1))x^1+\varphi_1(a_0)+\varphi_1(b_0)$
$=\varphi_2(a')+\varphi_2(b')$
The second last result follows because φ_1 is a homomorphism
Hence, φ_2 respects addition.

Claim 2: φ_2 respects multiplication
Proof:
Let a', b' $\in$ R[x].
Write $a'=a_{\deg(a)}x^{\deg(a)}+a_{\deg(a)-1}x^{\deg(a)-1}+\ldots+a_1x^1+a_0$.
Write $b'=b_{\deg(b)}x^{\deg(b)}+b_{\deg(b)-1}x^{\deg(b)-1}+\ldots+b_1x^1+b_0$.

$(a' \cdot b')$
$= a_{deg(a)}\, b_{deg(b)} x^{deg(a)+ deg(b)} + a_{deg(a)}\, b_{deg(b)-1} x^{deg(a)+ deg(b)-1} + \ldots + (a_1+b_0)x^1 + a_0 b_0$
$\Rightarrow \varphi_2(a' \cdot b')$
$= \varphi_1(a_{deg(a)}\, b_{deg(b)})x^{deg(a)+ deg(b)} + \varphi_1(a_{deg(a)}\, b_{deg(b)-1})x^{deg(a)+ deg(b)-1} + \ldots + \varphi_1(a_1 b_0)x^1 + \varphi_1(a_0 b_0)$
$= (\varphi_1(a_{deg(a)})\ \varphi_1\ (b_{deg(b)}))x^{deg(a)+ deg(b)} + \varphi_1(a_{deg(a)})\,\varphi_1(b_{deg(b)-1})x^{deg(a)+ deg(b)-1} + \ldots +$
$\varphi_1(a_1)\,\varphi_1(b_0)x^1 + \varphi_1(a_0)\,\varphi_1(b_0)$
$== \varphi_2(a') \cdot\ \varphi_2(b')$

The second last result follows because φ_1 is a homomorphism
Hence, φ_2 respects multiplication.

Claim 1+ Claim 2+ bijectivity of φ_2 => φ_2 is isomorphism from R[x] to S[x] => R[x] and S[x] are isomorphic rings

12.
Assume all polynomials in F[a] has degree < infinity.
Suppose $f \in F[x]$ is a nonzero polynomial of degree n, and f(a)=0 for all $a \in F$. By corollary 2.4.5, if $f \in F[x]$ is a nonzero polynomial of degree n, then f can have at most n distinct zeros in F. f(a)=0 for all $a \in F$ => f has infinitely many distinct zeros in F since F is infinite. But n<infinity, so we have reached a contradiction => f is not a nonzero polynomial of degree n => f = 0.

13.
Suppose, by way of contradiction, that there are finitely many polynomials $f \in (\mathbf{Z}/p)[x]$ s.t. f(a)=0 for all $a \in (\mathbf{Z}/p)$. Let S be the set of all polynomials $f \in (\mathbf{Z}/p)[x]$ s.t. f(a)=0 for all $a \in (\mathbf{Z}/p)$. S is a finite set, and the degree of a polynomial is always nonnegative integer less than infinity, there is a polynomial in S with the largest degree, say g. We construct g'=gh, where $h=(x-b_p)$, a polynomial of degree 1, and $b_p \in (\mathbf{Z}/p)$. g'(a)=0 for all $a \in (\mathbf{Z}/p)$ because (x-a) is a factor of g and hence a factor of g', so $g' \in S$. Since Z/p is an integral domain, g', by corollary 2.4.5 has degree deg(g)+1, which contradicts the maximality of the degree of g => there are infinitely many polynomials $f \in (\mathbf{Z}/p)[x]$ s.t. f(a)=0 for all $a \in (\mathbf{Z}/p)$

14.

$$
\begin{array}{rl}
 & x^2+x-2 \\
x^2+x+1 \quad / & \overline{x^4+2x^3+0x^2+0x+1} \\
 & \underline{x^4+\ x^3+\ x^2} \\
 & \quad x^3-x^2 \\
 & \quad \underline{x^3+x^2+x} \\
 & \quad\ -2x^2-x+1 \\
 & \quad\ \underline{-2x^2-2x-2} \\
 & \qquad\ x+3
\end{array}
$$

a) Quotient is x^2+x-2 and remainder is $x+3$

b)

$$
\begin{array}{r|l}
 & x-2 \\
\hline
x+3 & x^2+x+1 \\
 & \underline{x^2+3x} \\
 & \quad -2x+1 \\
 & \quad \underline{-2x-6} \\
 & \qquad 7
\end{array}
$$

We perform the Extended Euclidean algorithm:

i	q_i	r_i	x_i	y_i
0	-	$x^4+2x^3+0x^2+0x+1$	1	0
1	-	x^2+x+1	0	1
2	x^2+x-2	$x+3$	1	$-x^2-x+2$
3	$x-2$	7	$-x+2$	$1-(x-2)(-x^2-x+2)$
4	$\frac{x}{7}+\frac{3}{7}$	0	$1-(-x+2)(\frac{x}{7}+\frac{3}{7})$	$-x^2-x+2-(\frac{x}{7}+\frac{3}{7})(1-(x-2)(-x^2-x+2))$

b) A greatest common divisor is 7, and the monic greatest common divisor is 1.

c) From extended Euclidean Algorithm, we see that $\lambda = \frac{-x+2}{7}$ and

$\mu = \frac{1-(x-2)(-x^2-x+2)}{7} = \frac{x^3-x^2-4x+5}{7}$ $\Rightarrow \lambda f + \mu g = \frac{7}{7} = 1.$

Homework #5

1.

There are 9 possible quadratic polynomials in (Z/3)[x]: ax^2+bx+c, where a, b, c are elements in Z/3 . A polynomial that is not reducible is irreducible. A quadratic monic polynomial in Z/3 is reducible if it can be expressed as a product of two linear polynomials: (x+a)(x+b) where a and b are elements in Z/3. This means that all reducible quadratic monic polynomials in Z/3 must have the form $x^2+(a+b)x+ab$ for some a and b in Z/3.

There are only 3 possible choices for each of a and b. Hence, we have 9 cases. We enumerate them in order ([0],[0]; [0],[1], … [2],[2]), and find that the following are reducible quadratic monic polynomials in Z/3:

x^2
x^2+x
x^2+2x
x^2+x
x^2+2x+1
x^2+2
x^2+2x
x^2+2
x^2+x+1

So the others are irreducible because a polynomial is either reducible or irreducible:
x^2+1
x^2+x+2
x^2+2x+2

2.

For this question, we are working in Z/3, so we drop the square bracket notation.
By Lemma 2.5.2, $f(x)=x^3+x^2+2$ is irreducible if f(x) does not have a zero for all x in F. The possible elements in Z/3 are 0, 1, and 2. We see that $0^3+0^2+2 \neq 0$, $1^3+1^2+2 \neq 0$, $2^3+2^2+2 \neq 0$. We have exhausted the elements in Z/3. Hence, x^3+x^2+2 is irreducible.

For x^4+x+2, we first establish that it has no linear factors by checking that it has no zeros: 0^4+0+2, 1^4+1+2, 2^4+2+2. We have exhausted the elements in Z/3. Hence, x^4+x+2 has no linear factors. It also has no factor of degree 3 because if it does, it would have a linear factor.

If x^4+x+2 has quadratic factors g, then g must be irreducible. Otherwise, g is reducible => g has linear factor => x^4+x+2 has linear factor.
From question 1, the quadratic irreducible polynomials in Z/3 are
x^2+1
x^2+x+2
x^2+2x+2

But, we see that by performing long divisions: $x^4+x+2=(x^2+1)(x^2+2)+x$,
$x^4+x+2=(x^2+x+2)(x^2+2x+2)+x+1$ and $x^4+x+2=(x^2+2x+2)(x^2+x+2)+x+1$
Hence, x^4+x+2 has no quadratic factor.

Clearly, since x^4+x+2 has no factor with degree less than 4, x^4+x+2 is irreducible.

For x^5+x^3+x+1:
First we establish that it has no linear factors by checking that it has no zeros:
$0^5+0^3+0+1 \neq 0$, $1^5+1^3+1+1 \neq 0$, and $2^5+2^3+2+1 \neq 0$. We have exhausted the elements in Z/3.
Hence, x^4+x+2 has no linear factors. It also has no factor of degree 4 because if it does, it would have a linear factor.

If x^5+x^3+x+1 has quadratic factors g, then g must be irreducible. Otherwise, g is reducible => g has linear factor => x^5+x^3+x+1 has linear factor.
From question 1, the quadratic irreducible polynomials in Z/3 are
x^2+1
x^2+x+2
x^2+2x+2

But, we see that by performing long divisions: $x^5+x^3+x+1 =(x^2+1)(x^3)+x+1$, x^5+x^3+x+1
$=(x^2+x+2)(x^3+2x^2+2)+2x$ and $x^5+x^3+x+1 =(x^2+2x+2)(x^3+x^2+1)+2x+2$
Hence, x^5+x^3+x+1 has no quadratic factor. x^5+x^3+x+1 also does not have degree 3 factor, because if it does, it would have a quadratic factor.

Clearly, since x^5+x^3+x+1 has no factor with degree less than 5, x^5+x^3+x+1 is irreducible.

3.
For $x^3+3=0$, we apply the rational root theorem. The factors of 3 are 1 and 3, and since $1^3+3 \neq 0$, $(-1)^3+3 \neq 0$, $(-3)^3+3 \neq 0$and $3^3+3 \neq 0$, x^3+3 has no rational root => x^3+3 does not have a root in Q => x^3+3 is a irreducible polynomial in Q[x] by Lemma 2.5.7.

So x^3+3 is an irreducible factor of x^3+3 by itself.

For $x^4+x^3+8x^2+5x+15$:
Write $f= x^4+x^3+8x^2+5x+15$
Clearly, $x^4+x^3>0$ for all x in Q, so there does not exists a x in Q s.t. $x^4+x^3+8x^2+5x+15=0$. Hence, by Lemma 2.5.7, f does not have a linear factor.

Suppose f has quadratic factors g and h. Write $g=(x^2+ax+b)$ and $h=(x^2+cx+d)$, where by proposition 2.5.7, we can assume a, b, c, and d to be integers. We have the following system of equations:
$bd=15$
$bc+da=5$
$b+d+ac=8$
$a+c=1$

Since 15 has the following factors: 1, 3, 5, 15, and it cannot be the case that b=1 and d=15 (or vice versa, the two are symmetric), we can try b=3 and d=5.
We see that b=3, d=5, c=0, a=1 satisfy the system of equations. Hence, $(x^2+x+3)(x^2+5)$. Using the discriminant from quadratic formula, we see that x^2+x+3 and x^2+5 have no root in R, and hence they have no root in Q. By lemma 2.5.7, x^2+x+3 and x^2+5 do not have linear factors => x^2+x+3 and x^2+5 are irreducible factors of f.

For $x^3+8x^2+5x-50$:
We again apply the rational root theorem. The factors of 50 are 1, 2, 5, 10, 25, 50 and we see that $2^3+8\cdot2^2+5\cdot2-50=0$. Hence (x+2) is a factor.
By long division, we have $x^3+8x^2+5x-50=(x^2+10x+25)(x+2)$ =>
$x^3+8x^2+5x-50=(x+5)(x+5)(x+2)$.

All linear polynomials are irreducible. Hence, $x^3+8x^2+5x-50$ has been factored into product of irreducible polynomials.

4
a)
Φ is homomorphic if $\Phi(a+b)=\Phi(a)+\Phi(b)$ and $\Phi(a\cdot b)=\Phi(a)\cdot\Phi(b)$ where a and b are elements of Z[x]. Write a = $\sum_{i=0}^{d_a} a_i x^i$ and b = $\sum_{i=0}^{d_a} b_i x^i$

For $\Phi(a+b)=\Phi(a)+\Phi(b)$:

We know from section 1.6 that φ is homomorphic. Hence, $\Phi(a+b)=\Phi(\sum_{i=0}^{d_a} a_i x^i+\sum_{i=0}^{d_a} b_i x^i)=$

$$\Phi(\sum_{i=0}^{d_a}(a_i+b_i)x^i)=\sum_{i=0}^{d_a}\varphi(a_i+b_i)x^i=\sum_{i=0}^{d_a}\varphi(a_i)x^i+\sum_{i=0}^{d_a}\varphi(b_i)x^i=\Phi(a)+\Phi(b)$$

For $\Phi(a\cdot b)=\Phi(a)\cdot\Phi(b)$:

Again, we make use of the fact that φ is homomorphic. $\Phi(a\cdot b)=$

$$\Phi(\sum_{i=0}^{d_a} a_i x^i\cdot\sum_{i=0}^{d_a} b_i x^i)=\Phi(\sum_{k=0}^{d_a}(\sum_{i=0}^{d_a} a_i b_{k-i})x^k)=\sum_{k=0}^{d_a}\varphi(\sum_{i=0}^{d_a} a_i b_{k-i})x^k=\sum_{k=0}^{d_a}(\sum_{i=0}^{d_a}(\varphi(a_i)\varphi(b_{k-i})))x^k$$

$$=(\sum_{i=0}^{d_a}\varphi(a_i)x^i)(\sum_{i=0}^{d_a}\varphi(b_i)x^i)=\Phi(a)\Phi(b)$$

b)
By Proposition 2.5.7, a monic polynomial that is reducible in Q[x] is also reducible in Z[x]. Hence, we can write f(x)=g(x)h(x) where g(x) and h(x) are in Z[x] with degree$\geq$1. Since Φ is a well-defined map, we can write $\Phi(f(x))=\Phi(g(x)h(x))$. But by part a, $\Phi(f(x))=\Phi(g(x))\Phi(h(x))$. f(x) is monic, g(x) and h(x) must also be monic. Since p is a prime and p does not divide 1, clearly $\Phi(g(x))$ and $\Phi(h(x))$ also have degree $\geq$1 if g(x) and h(x) have degree $\geq$1. So now, $\Phi(f(x))$ can be expressed as products of two polynomials in (Z/p)[x] with degree $\geq$1, hence $\Phi(f(x))$ is reducible.

c)
By b, $\Phi(f(x))$ is irreducible => f(x) is irreducible in Q where $\Phi : Z[x] \rightarrow (Z/3)[x]$.
In Z/3, x^4+3x^2-2x-1 can be rewritten as x^4+x+2. Exercise 2 shows that x^4+x+2 is irreducible.
Hence, x^4+3x^2-2x-1 is a irreducible polynomial in Q[x].
Similarly, in Z/3, $x^5-2x^3+3x^2+x+1$ can be rewritten as x^5+x^3+x+1. Exercise 2 shows that x^5+x^3+x+1 is irreducible. Hence, x^4+3x^2-2x-1 is a irreducible polynomial in Q[x].

5a)

We first prove that if $f=x^2+ax+b$ is reducible in Q[x] then $g=x^2-\left(\frac{a^2}{4}-b\right)$ is reducible:

By proposition 2.5.7, f is reducible in Q[x] => f is reducible in Z[x]. Since f is a quadratic, f is reducible => f = (x+c)(x+d) for some c and d in Z. By definition of f, a and b are integers. Hence, cd=b and c+d=a. We see that
$\left(x+\frac{(c-d)}{2}\right)\left(x-\frac{(c-d)}{2}\right)=x^2-\left(\frac{(c+d)^2}{4}-cd\right)=x^2-\left(\frac{a^2}{4}-b\right)$. Hence, $x^2-\left(\frac{a^2}{4}-b\right)$ is reducible.

We will now proof that if g is reducible, then f is reducible.

If g is reducible in Q[x], then g is reducible in R[x]. Clearly, $\left(\frac{a^2}{4}-b\right)>0$. (Otherwise, there would be no root x s.t. $x^2-\left(\frac{a^2}{4}-b\right)=0$, and by Lemma 2.5.2, g would be irreducible in R[x].)

$\left(\frac{a^2}{4}-b\right)>0$ implies $\left(a^2-4b\right)>0$, where $\left(a^2-4b\right)$ is actually the discriminant of x^2+ax+b.
Hence, x^2+ax+b has a root in R[x]. Furthermore, g is reducible implies

$g=\left(x+\sqrt{\left(\frac{a^2}{4}-b\right)}\right)\left(x-\sqrt{\left(\frac{a^2}{4}-b\right)}\right)$, where $\left(x+\sqrt{\left(\frac{a^2}{4}-b\right)}\right)$ and $\left(x-\sqrt{\left(\frac{a^2}{4}-b\right)}\right)$ are both rationals => $\sqrt{\left(\frac{a^2}{4}-b\right)}$ is rational => $\left(a^2-4b\right)$ is rational. Hence, the roots p and q given by applying quadratic formula on x^2+ax+b are rational, hence, $x^2+ax+b = (x-p)(x-q)$ => x^2+ax+b is reducible in Q[x].

b) Suppose x^2-d is reducible in R[x] where $d<0$. We can write (x+a)(x+b) for some a and b in R. a+b=0 => a=-b; and ab=-d => ab=-(-|d|) because d<0 => a(-a)=-(-|d|) => $a^2=-|d|$, which is a contradiction. x^2-d is irreducible.

c) First we show that if x^2-d is reducible then x^2-c^2d is reducible, where c and d are as defined in the question.

If x^2-d is reducible, then we can write x^2-d =(x+a)(x+b) for some a and b in Q, where ab=-d and a+b=0. We see that $(x+ca)(x+cb)=x^2+cax+cbx+cacb=x^2+c(a+b)x+c^2ab=x^2+c^2ab = x^2-c^2d$. Hence, x^2-c^2d is reducible.

If x^2-c^2d is reducible, then $(x+a)(x+b)= x^2-c^2d$ for some a and b in Q, where $ab=-c^2d$ and a+b=0. c^{-1} exists because c is in Q*. We see that $(x+c^{-1}a)(x+c^{-1}b) = x^2+(c^{-1})(a+b)x+(c^{-1})^2ab= x^2-(c^{-1})^2c^2d = x^2-d$. Hence, x^2-d is also reducible.

d)

Write $d \in Q = \frac{m}{n}$ and gcd(m,n)=1. Write $m = \prod_i p_i^{r_i}$ and $n = \prod_j q_j^{s_j}$, where $p_i \neq p_j$ if $i \neq j$, and $q_i \neq q_j$ if $i \neq j$. Let $R = \{p_i : r_i \text{ is odd}\}$. Let $S = \{q_j : s_j \text{ is odd}\}$. Write R" to be the product of all the elements in R, and S" to be the product of all the elements in S. Now, we let d' = R"·S". Note that d' is a product of distinct primes because gcd(m,n)=1. Clearly, we can write $\pm$ d/d' as $\frac{o}{p}$ where o and p are products of distinct primes with even powers => $\pm$ d/d' is a square in Q.

e)

We will first show that if d is not a square, then x^2-d is irreducible by Eiseinstein's irreducibility criterion:

Write $d \in Q = \frac{m}{n}$ and gcd(m,n)=1. Write $m = \prod_i p_i^{r_i}$ and $n = \prod_j q_j^{s_j}$. If d is not a square, then the set $\{p_i \mid r_i \text{ is odd}\} \cup \{q_i \mid s_i \text{ is odd}\}$ is non-empty. Let E_m be $\{ p_i^{r_i} \mid r_i \text{ is even}\}$ and E_n be $\{ q_j^{s_j} \mid s_j \text{ is even}\}$. Let E_m' be the product of elements in E_m and E_n' be the product of elements in E_n. Clearly, $\frac{E_m'}{E_n'}$ is a square in Q, so we can write $c=\sqrt{\frac{E_m'}{E_n'}} \in$ Q. So now d=cd', where d' is quotient of two products of distinct primes. Hence, for all p, p^2 does not divide d'. Clearly, for all p, p does not divide the coefficient of x^2, which is 1. p divides the coefficients of x, which is 0. We can apply Eiseinstein's irreducibility criterion and conclude that x-d' is irreducible. But then by part c, x^2-d' is irreducible iff x^2-c^2d' is irreducible. Hence, x^2-c^2d'=x^2-d is irreducible.

If d is a square, then x^2-d = (x+d)(x-d) where (x+d), (x-d)$\in$ Q so x^2-d is reducible.

Hence, x^2-d is irreducible iff d is not a square.

6a)

Since a $\equiv$ c and b $\equiv$ d, we have that f | (c – a) and f | (d – b). Therefore, f | (c – a + d – b) implies f | (c+d) – (a+b) implies a+b $\equiv$ c+d.

Again we have c = a + qf and d = b + rf for some r and q in F[x].

Then, cd = ab + f(ar + qb + qrf) implies f | (cd – ab) implies ab = cd.

b)
Let I = {qf : q in F[x]}.
We show that I is an ideal. Clearly, for all a $\in$ I, x$\in$ F[x], we have ax$\in$ I and xa$\in$ I.
Hence, by the way I is defined, it is sufficient to check that I is a subring of F[x].
I is non-empty. 0 is in I.
I is closed under addition: let a, b $\in$ I, write a as pf and b as qf where p and q are in F[x], then a+b=pf+qf=(p+q)f $\in$ I

I is closed under subtration: let a, b $\in$ I, write a as pf and b as qf where p and q are in F[x], then a+(-b)=pf+-(qf)=(p+(-q))f $\in$ I, where the last equality follows because by a theorem, a(-f)=(-a)f.

I is closed under multiplication: let a, b $\in$ I, write a as pf and b as qf where p and q are in F[x], then ab=pfqf=(pfq)f $\in$ I.

Hence, I is a subring of F[x]. By question 9b, F[x]/(f) is thus a ring.

It remains to show that F[x]/(f) is multiplicative commutative. It is clear that F[x] is commutative, and hence [a][b]=[ab]=[ba]=[b][a], where a and b are in F[x] (and [a],[b] are in F[x]/(f)) => F[x]/(f) is also commutative.

=> F[x]/(f) is a commutative ring.

7.
a)
Trivially, let the basis of F be y and 1. Clearly, y and 1 are linear independent because there does not exists an element a in Z/3 s.t. a1=y. It also spans F as a vector space over Z/3: an element in F has the form iy+j, so it can clearly be represented by a linear combination (with coefficient in Z/3) of y and 1.

b)
F is GF(9). Write a as a non-zero element in GF(9). By lemma 2.8.1, a^{9-1}=1 =>a^9=a. In fact, b^9=b for all elements in GF(9) because clearly 0^9=0. Rewriting, we have b^9-b = 0 for all b in F
Every element b in GF(9) is a root of x^9-x.

8.
Suppose element b is the root of x^2+1 where b is an element of R=(Z/3)[y]/(y^2+y+2) = (Z/3)[*a*] with a^2+*a*+2=0. b must have the form c*a* +d, where c and d are elements of Z/3.
b is a root implies (c *a* +d)^2+1=0 => c^2a^2+2cd*a* +d^2+1=0 => c^2(2 *a* +1)+2cd *a* +d^2+1 = 0 =>
($2c^2$+2cd) *a* +d^2+1+c^2=0 => 2c(c+d)=0 and d^2+1+c^2=0
Case 1:
c=0 => d=0 => d^2+1 = 0 => this case does not happen because there does not exists a d in Z/3 s.t. d^2+1=0.

Case 2:

c=1 => d=2 => c+d=0 and $d^2+1+c^2=0$ => a+2 is a root of x^2+1. We can stop because we found a root => R contains a root.

9.
a)
Since a $\underline{=}$ c and b $\underline{=}$ d, we have that (c – a) in I and (d – b) in I. Because I is a ring, their sum, (c – a) + (d – b) = (c+d) – (a +b) is also in I, which implies that c+d=a+b.

Again we have c = a + q and d = b + r for some r and q in I.
Then, cd = ab + ar + qb + qr. Since ar, qb and qr are all in I, it follows that cd – ab is in I implies ab $\underline{=}$ cd.

b)
The induced operations are:
[a] + [b] = [a+b] and [a][b] = [ab].
We must show that the operations are well-defined, independent of the choices of representatives.
If we have [a] = [b] and [c] = [d], we need to check that [a+c] = [b+d] and [ac] = [bd].
Let a = b+r and c=d+s where r, s in I.
Then, [a + c] = [b + r + d + s] = [b + d] because r + s is in I, and [ac] = [(b+r)(d+s)] = [bd + bs + rd + rs] = [bd], because bs, rd and rs are all in I.

i) Existence of Zero
I is a ring. $0 \in$ I. Clearly, [0] is in R/I.

ii) Additive associativity
a, b, c in R => a+(b+c)= (a+b)+c
=> [a+(b+c)]= [(a+b)+c] => ([a]+[b])+[c]= [(a+b)+c] =[a+(b+c)]= [a]+([b]+[c])

iii) Additive commutativity
a, b in R => a+b=b+a
[a]+[b]=[a+b]=[b+a]=[b]+[a]

iv) Additive inverse
Write –a in R as a'.
We see that [a]+[a']=[a+a']=[0]. So for every element [a], we have the additive inverse [a']

v) Multiplicative Distributivity
[a],[b],[c] in R/I
[a]([b]+[c])=[a]([b]+[c])=[a]([b+c])=[a(b+c)]=[ab+ac]=[ab]+[ac]=[a][b]+[a][c]

vi) Multiplicative Associativity
[a],[b],[c] in R/I
[a]([b][c])=[a]([bc])=[a(bc)]=[(ab)c]=[ab][c]=([a][b])[c]

Hence, R/I with the induced operations form a ring.

10.
The factors of 12 are 1, 2, 3, 4, 6, 12. By definition of order, it only makes sense to consider order of non-zero elements. By Lemma 2.8.1, $a^{12}=1$ for all non-zero element a in Z/13. By Lemma 2.8.2, if $a^{12}=1$ then order(a)|12. Hence, order(a) = 1 or 2 or 3 or 4 or 6 or 12 for all nonzero element a in Z/13.

a	a^2	a^3	a^4	a^6
1	1	1	1	1
2	4	8	3	12
3	9	1	3	1
4	3	12	9	1
5	12	8	1	12
6	10	8	9	12
7	10	5	9	12
8	12	5	1	12
9	3	1	9	1
10	9	12	3	1
11	4	5	3	12
12	1	12	1	1

From the tabulation, we see that :

a	order(a)
1	1
2	12
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

11.
By Lemma 2.8.1, $a^{ord(a)}=1$ for all $a \in F^*$. Since φ is given to be an isomorphism (and hence a homomorphism), $\varphi(1)=\varphi(a^{ord(a)}) = \varphi(\prod_i^{ord(a)} a) = \prod_i^{ord(a)} \varphi(a) = \varphi(a)^{ord(a)}$. By exercise 2.2.14, $\varphi(1)=1_S$. Hence, $\varphi(a)^{ord(a)} = 1_S$. By lemma 2.8.2, $ord(\varphi(a)) \mid ord(a) \Rightarrow ord(\varphi(a)) \leq ord(a)$.

Similarly, since φ is given to be an isomorphism (and hence a homomorphism), as proved in previous homework, φ^{-1} exists and is also an isomorphism. Suppose $ord(\varphi(a)) < ord(a)$. $\varphi(a)^{ord(\varphi(a))} = 1_S \Rightarrow \varphi^{-1}(\varphi(a)^{ord(\varphi(a))}) = 1_R \Rightarrow \varphi^{-1}(\prod_i^{ord(\varphi(a))} \varphi(a)) = 1_R \Rightarrow \prod_i^{ord(\varphi(a))} \varphi^{-1}(\varphi(a)) = 1_R \Rightarrow$

$\prod_{i}^{ord(\varphi(a))} a = 1_R$ => $a^{ord(\varphi(a))}=1_R$. But we assumed ord(φ(a))< ord(a), contradicting ord(a). Hence, ord(φ(a))=ord(a).

12.
a)
There are 2^4 elements in F (by counting). By Lemma 2.9.1, element *a* in F is primitive iff ord(*a*)=2^4-1=15. Hence *a* is not primitive because its order is given to be 5.

b)
By Lemma 2.8.1, a^{15}=1 for all non-zero element *a* in F because F has 2^5-1=15 elements.
By Lemma 2.8.2, if b^{15}=1 then order(*b*)|15
Hence order of b can only be 1 or 3 or 5 or 15.
$b^1=a+1$
$b^2=a^2+2a+1=a^2+1$
$b^4=(a^2+1)^2$ because by $(a+b)^2=(a^2+b^2)$ in a field with characteristic p as shown in lecture
$=a^4+1=a^3+a^2+a+1+1=a^3+a^2+a$
Hence, $b^3=(a^2+1)(a+1)=a^3+a^2+a+1$
$b^5=(a^3+a^2+a)(a+1)=a^4+a^3+a^2+a^3+a^2+a=a^4+a$

Hence, $b \neq 1$, $b^3 \neq 1$ and $b^5 \neq 1$ => ord(b)=15.

c)
By theorem 2.10.2, subfields of F have sizes 2^1, 2^2 and 2^4. Subfield of F with size 2^4 is just F.

By theorem 2.10.2, the other unique subfields are:

Subfield G of size 2^1:
Write $c=b^{15}$. G={0, c}.

Subfield H of size 2^2:
Write $d=b^5$. H={0, c, c^2, c^3}.
$d=b^5$ because $5\cdot(2^2-1)=15=ord(F)-1$.