Solutions to Homework 2

13.29 Let F be a field with $|F|=2^n$ for some n e N. To show that char F=2.
In particular, F is an integral domain (proved on page 250).
Therefore, by 13.4, charF is zero or prime.
Then treating F as a group under addition, consider the cyclic subgroup generated by the unity:
S = <1>={1,1+1,1+1+1,…}
Since F is a finite field, S is by definition a finite subgroup.
Therefore there exists some s e S such that $s=1^{-1}$ (additive inverse)
Therefore, $s = 1+1+\ldots+1=1^{-1}$
Therefore s+1=0=(1+1+…+1)+1 and therefore there exists some k e N such that k.1=0.
By 13.3 if 1 has order k under addition in ring R, then char R=k. Therefore charF=k≠0.
By Lagrange's Theorem, the order of a subgroup must divide the order of the group. Therefore $k|2^n$. But char F=k and charF is prime. Therefore charF=2.

13.41 Let x,y e R, char R=p for some p prime and let R be commutative.
Because R is commutative we can expand $(x+y)^p$ by the binomial expansion:
charR=p implies that p.r=0 for all r e R. Since p is prime, it is simple to show that p divides the binomial coefficients (p choose k for 0<k<p) (the largest possible element in the denominator is p-1 and so the p is never cancelled from the numerator). Therefore all the binomial coefficients except p choose 0 and p choose p and therefore $(x+y)^p=x^p+y^p$.

b) By induction:
From above $(x+y)^p=x^p+y^p$
Assume for k: $(x+y)^{(p^k)}=x^{(p^k)}+y^{(p^k)}$
For k+1: $(x+y)^{(p^{(k+1)})}=(x+y)^{(pp^k)}=[(x+y)^p]^{p^k}=[x^p+y^p]^{(p^k)}$
Let $x^p=X$, $y^p=Y$ and since we are in a ring, X,YeR
$(x+y)^{(p^{(k+1)})}=(X+Y)^{(p^k)}=X^{p^k}+Y^{p^k}$ (by induction hypothesis, and the result immediately follows for all n e N.

c) Let char R=4 and let R be commutative:
$(x+y)^4=x^4+4x^3y+6x^2y^2+4xy^3+y^4=x^4+2x^2y^2+y^4$

Let $R=Z_4$ (clearly commutative with characteristic 4)
Let x=y=1: then $(1+1)^4=1+2+1=0\neq1^4+1^4$

13.54 Let F be a field with |F|=n
In particular F\{0} is a group under multiplication and |F\{0}|=n-1
Consider x e F\{0} and the cyclic subgroup generated by x (for any x).
S=<x>={x,x^2,…}
Since S is a subgroup there exists k e N such that $x^k=1$ and for this k, |S|=k
By Lagrange's Theorem |S| divides |F\{0}|
Therefore k|n-1
Therefore km=n-1 for some m
Therefore $(x^k)^m=x^{km}=x^{n-1}=1^m=1$ for all x e F\{0}.

Note, it isn't shown above that that was a group, but it can be shown by checking the axioms.

14.11 <2>+<3>=<1>, <3>+<6>=<3>, <a>=<m>+<n> if a=gcd(|m|,|n|)
Confirmation of these is computational.

Let R={f:**R**→**R** | f is continuous}, A={f in R | f(0)=0}

To show that R is commutative with unity:
Let f,g eR;
Then for all x in **R**: (fg)(x)=f(x)g(x)=g(x)f(x)=(gf)(x) (Since f(x), g(x) are in **R**)
Let 1(x)=1. Then for all f in R, (f.1)(x)=f(x)=(1.f)(x) and therefore 1(x) is the unity.
Note: 1(x) is the constant function f(x)=1.

To show A is ideal:
f(x)=0(x)=0 is continuous and 0(0)=0 and so A is nonempty.
If f,g e A: then (f-g)(0)=f(0)-g(0)=0-0=0 and f-g e A
If g e R, f e A: (fg)(0)=f(0)g(0)=0g(0)=0=…=(gf)(0).
By the Ideal Test, A is an ideal.

To show that R/A = {r+A | r e R} is a field:
R/A is a ring because A is an ideal (14.2).
Commutativity: Let r+A, s+A be elements of R/A:
Then (r+A)(s+A)=rs+A and for all x e **R**, (rs)(x)=r(x)s(x)=s(x)r(x)=sr(x)
Therefore, rs+A=sr+A=(s+A)(r+A) and R/A is commutative.

To show that R/A has a unity:
If (r+A)(u+A)=ru+A=r+A then (ru)(x)=r(x) for all x in **R**.
Therefore u(x)=1.
Therefore the unity of R/A = u+A=1+A

To show that for all r+A in R/A, r+A has an inverse (is a unit) (r+A non zero (where zero is 0+A)).
If $r(0)\neq 0$, then $(r+A)^{-1}=\{f \text{ in } R \mid f(0)=1/r(0)\}=r^{-1}+A$
To show that this is in fact an inverse, multiply out $(r+A)(r^{-1}+A)$ to yield:
$\{f:\mathbf{R}\rightarrow\mathbf{R} \mid f \text{ continuous}, f(0)=r(0)/r(0)=1\}=1+A$ which is the unity of R/A.
If r(0)=0, then r+A=A
Therefore every nonzero element is a unit. Therefore R/A is a field.
Therefore A is a maximal ideal (14.4)

N.B. The quotient field is defined above.

14.39 To show that Z is a principal ideal domain. Z is clearly an integral domain (Table 13.2). The solution to this problem is lifted verbatim from the Homework One Solutions showing that any ideal is of the form kZ (and therefore of the form <k>).

Bonus:
Let a sequence of rational numbers $(x_1,x_2,\ldots)$ be denoted $\{x_i\}$.
Then a sequence $\{x_i\}$ is a Cauchy sequence of rationals if and only if $\forall\ r>0, \exists\ N>0$ such that $\forall m,n>N, |x_m-x_n|<r$. i.e. A Cauchy sequence is a sequence of rationals that can be truncated so that the remaining elements are arbitrarily close.
Let C be the set of all such sequences and let $\{x_i\}+\{y_i\}=\{x_i+y_i\}=\{(x+y)_i\}$, $\{x_i\}\{y_i\}=\{(xy)_i\}=\{x_iy_i\}$
Cauchy sequence will always refer to a Cauchy sequence of rationals.

1. To show that C is a ring:
   C is nonempty because the sequence $\{x_i \mid x_i=0 \text{ for all } i\}$ is clearly a Cauchy sequence.
   The axioms 1,2,5 and 6 follow immediately from the definition of addition and multiplication.
   Axiom 3: $0=\{x_i \mid x_i=0 \text{ for all } i\}$ is the additive identity (trivial to show)
   Axiom 4: Given $\{a_i\}$ e C, let $\{b_i\}=\{-a_i\}$ and then it is trivial to show that $\{a_i\}+\{b_i\}=\{0\}$.

To show that $\{b_i\}$ is in fact in C:
By definition: for all r>0, there exists N>0 such that for all m,n e N, m,n>N
$|a_m-a_n|<r$
And: $|a_m-a_n|=|-1||a_m-a_n|=|-a_m-(-a_n)|=|b_m-b_n|$
Therefore, for all r>0, there exists N>0 such that for all m,n e N, m,n >N $|b_m-b_n|<r$.
Therefore $\{b_i\}$ e C.

To show that C is closed under addition:
Assume that $\{a_i\},\{b_i\}$ are elements of C;
Then by definition, for all r>0 there exists some N>0 such that for all m,n>N $|a_m-a_n|<r$, and $|b_m-b_n|<r$.
Therefore, choose some arbitrary r>0.
Then, by definition, since the condition holds for all r>0, it holds in particular for r/2.
Therefore there exists an N>0 such that $|a_m-a_n|<r/2$ and some M>0 such that $|b_m-b_n|<r/2$.
Then for max(M,N)=P, whenever $|a_m-a_n|<r/2$ and $|b_m-b_n|<r/2$ for all m,n>P.
Therefore for all m,n>P: $|(a_m+b_m)-(a_n+b_n)|=|(a_m-a_n)+(b_m-b_n)|<|a_m-a_n|+|b_m-b_n|<r$.
Therefore if $\{a_i\}$ and $\{ b_i \}$ are in C, then $\{a_i+ b_i \}$ is in C.

2. The zero element is $0=\{0\}=\{x_i | x_i=0 \text{ for all } i\}$
   The unity element is $1=\{1\}=\{x_i | x_i=1 \text{ for all } i\}$
   Verification:
   $\{a_i\}.1=\{a_ix_i | x_i=1 \text{ for all } i\}=\{a_i\}=1.\{a_i\}$

   C is not a field. (Not all elements are units)
   Let $\{a_i\}\neq 0$, $\{a_i\}$ e C, then $\{a_i\}^{-1}=\{ b_i \}$ would need to satisfy:
   $\{a_i\}\{b_i\}=\{a_i\ b_i \}=1$
   Therefore, $a_ib_i=1$ for all i.
   Therefore $b_i=1/a_i$ for all i e N (a_i, b_i e **R**)
   But if $a_m=0$ for some m e N, and $a_n\neq 0$ for some n e N, then $\{a_i\}\neq 0$ and the sequence $\{b_i\}$ has undefined elements.
   An example is: $\{a_i | a_1=1, a_j=0, j>1\}$ then $\{a_i\}$ is clearly a Cauchy sequence with no inverse.

3. Let $A=\{\{a_i\} | \lim a_n = 0, a_i \text{ e } Q \text{ for all } i\}$ (all limits are n→infinite)
   A is nonempty because 0 e A.
   To show that A is contained in C:
   Clearly A is contained {sequences of rationals} by definition of A.
   By definition, if $\lim x_n=L$ then
   $\forall$ E>0 $\exists$ N>0 such that if m>N, $|x_m-L|<E$.
   Therefore for A:
   $\forall$ E>0 $\exists$ N>0 such that if m>N $|a_m|<E$.
   Therefore if m,n>N $|a_m|<E$, $|a_n|<E$
   Therefore $|a_m-a_n|<2E$
   Therefore $\forall$ r=2E, $\exists$ N>0 s.t. if m,n>0 then $|a_m-a_n|<r$
   Therefore $\{a_i\}$ is a Cauchy sequence.
   Therefore A is contained in C.
   If $\{a_i\},\{b_i\}$ e A: $\{a_i\}-\{ b_i \}=\{a_i- b_i \}=\{(a-b)_i\}$
   Note: $\lim a_n=0=\lim b_n$
   Therefore $\lim a_n-b_n=0$ (limit of differences is difference of limits)
   Therefore $\{a_i\}-\{ b_i \}$ e A.
   If $\{a_i\}$ e A, $\{c_i\}$ e C: $\{c_i\}\{a_i\}=\{c_ia_i\}$
   Since $\{c_i\}$ e C, all r>0 there exists N>0 such that m,n>N means $|c_n-c_m|<r$

Therefore let r=1>0
There exists N>0 such that m,n>N → $|c_m-c_n|<1$
Take some arbitrary m>N, then for all n>N, $|c_m-c_n|<1$
Therefore for all n>N $c_m-1<c_n<c_m+1$
The sequence $\{c_i\}$ is bounded from above and below.
Therefore lim $c_n \neq \pm$infinite

Lim $c_n a_n$=(lim c_n)(lim a_n)=0 lim c_n = 0
Therefore $\{c_i\}$ e C, $\{a_i\}$ e A, $\{c_i\}\{a_i\}$eA (show first that this is commutative)

Therefore A is an ideal of C.

4. To show that A is maximal:

By 14.4 A is maximal if and only if C/A is a field.
C/A={$\{c_i\}$+A | $\{c_i\}$ e C}
By 14.2 and above, C/A is a ring because A is an ideal (operations are standard).
C/A is commutative:
Let p=$\{c_i\}$+A, q=$\{d_i\}$+A be in C/A
Then: pq = $\{c_i d_i\}$ +A = $\{d_i c_i\}$+A = qp
Therefore C/A is commutative.

To show C/A has a unity:
Let $\{x_i\}$=1 (from above, the unity of C)
For all p=$\{c_i\}$+A in C/A:
p(1+A) = $\{c_i\}$.1 +A
= $\{c_i\}$ +A = p = (1+A)p
Therefore 1+A is the unity of C/A

To show that every nonzero element of C/A is a unit:
Let p=$\{c_i\}$+A be an arbitrary nonzero element of C/A
Lim $c_n \neq 0$ because if it were so then p= {set of all sequences that converge to zero}=A=0+A

Notice that p = set of all sequences that converge to lim c_n.

Let lim c_n = L ≠0. By the completeness of reals, there exists E>0 such that 0 is not in [L-E,L+E].

By definition of limits:
For all d>0, ∃ N>0 such that $|c_m-L|<d$ for all m>N
Therefore, for all m>N cm e (L-E,L+E).
Verification: $|c_m-L|<E$ → $-E<c_m-L<E$ → $L-E<c_m<L+E$
Therefore for all m>N $c_m \neq 0$, c_m e Q.
Define c_I = {i e N | c_i=0}
c_I is finite by the above and therefore there exists some maximal element of c_I; denote it max(c_I).

To define p^{-1}:
Let p^{-1}=$\{d_i\}$+A where $\{d_i\}$=$\{d_j$=0 for all i<=max(c_I), d_j=1/c_j for all j>max(c_I)$\}$
$\{d_i\}$ is clearly a sequence of rational numbers.
To show it is a Cauchy sequence:
Notice from above that ∃ N>0 such that if m>N then $c_m<0$ or $c_m>0$ and also that the functions f:**R**→**R** by f(x)=1/x is continuous on **R**\{0}
By the epsilon-delta definition of continuity:

For all E>0 there exists d>0 such that f((x-d,x+d)) is contained in (f(x)-E, f(x)+E) and therefore if lim x_n=L, lim $1/x_n$=1/L provided x_i>0 or x_i<0.

Since there exists N>0 such that for all m>N, c_m>0 or c_m<0

Lim $1/c_n$ = 1/L

Therefore the sequence $\{d_i\}$ converges to 1/L

Therefore $\{d_i\}$ is a Cauchy sequence.

pp^{-1} = set of all Cauchy sequences that converges to lim c_nd_n

= set of all Cauchy sequences that converge to (lim c_n)(lim d_n)

= set of all Cauchy sequences that converge to L(1/L)

= set of all Cauchy sequences that converge to 1

= 1+A

Therefore every element of C/A is a unit.

Note: We could not define $\{d_i\}=\{1/c_i\}$ because c_i could be zero for some i and we could not define $\{x_i\}=\{(1/L)c_i\}$ since lim c_n = L is not necessarily rational.

5. C/A is isomorphic to the Reals. This is essentially the method of defining the reals from the rationals by way of Dedekind cuts.

∃∀