Let $p \in \mathbb{Z}_+$ be prime. For all $i, j \in \mathbb{Z}_+$ with $i < j$ let $\phi_{ji} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ denote the natural quotient ring homomorphisms

$$\phi_{ji}(a \ (mod \ p^j)) = a \ (mod \ p^i).$$

Set

$$R = \{(a_1, a_2, a_3, \ldots) | a_i \in \mathbb{Z}/p^i\mathbb{Z} \text{ and } \phi_{ji}(a_j) = a_i \text{ for all } i < j \} \subset \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}.$$

(i) From exercise 19, page 231 (which you may assume) we know that

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$

and

$$(a_1, a_2, \ldots) \cdot (b_1, b_2, \ldots) = (a_1 b_2, a_2 b_2, \ldots)$$

defines a commutative ring structure on $\prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$. Prove that $R$ is a subring with 1.

**Solution** Observe that $1 = (1, 1, \ldots) \in R$, so $1 \in R \neq \emptyset$. So, it suffices to show that for all $a = (a_1, a_2, \ldots), b = (b_1, b_2, \ldots) \in R$, we have $a - b, ab \in R$. For all $j > i$, $\phi_{ji}$ is a homomorphism and hence

$$\phi_{ji}(a_j - b_j) = \phi_{ji}(a_j) - \phi_{ji}(b_j) = a_i - b_i$$

and

$$\phi_{ji}(a_j b_j) = \phi_{ji}(a_j) \phi_{ji}(b_j) = a_i b_i.$$

By definition of $R$, it follows that $a - b, ab \in R$, as required.

(ii) Consider the set of infinite series

$$S = \left\{ \sum_{k=0}^{\infty} c_k p^k | c_k \in \{0, \ldots, p-1\} \right\}$$

Given $c = \sum_{k=0}^{\infty} c_k p^k \in S$, we note that although this series may not converge, for all $i \in \mathbb{Z}_+$, we can formally make sense of the reduction $mod \ p^i$, written $\psi_i : S \to \mathbb{Z}/p^i\mathbb{Z}$, by declaring

$$\psi_i(c) = \psi_i \left( \sum_{k=0}^{\infty} c_k p^k \right) = \sum_{k=0}^{i-1} c_k p^k \ (mod \ p^i).$$

Now set

$$\psi(c) = (\psi_1(c), \psi_2(c), \ldots)$$

and prove that this defines a bijection from $S$ to $R$.

**Hint:** observe that any $x \in \{0, 1, \ldots, p^i - 1\}$ can be uniquely written in the form $x = \sum_{k=0}^{j-1} c_k p^k$. 

Solution In all of what follows, we do not distinguish between elements of $\mathbb{Z}$ and $\mathbb{Z}/p^i\mathbb{Z}$ when the context determines the meaning.

First, we must show that $\psi(S) \subset R$. For this, observe that for all $j > i$, we have

$$\phi_{ji}(\psi_j(\sum_{k=0}^{\infty} c_k p^k)) = \phi_{ji}(\sum_{k=0}^{j-1} c_k p^k) = \sum_{k=0}^{i-1} c_k p^k = \psi_i(\sum_{k=0}^{\infty} c_k p^k)$$

where the second-to-last equality comes from the fact for all $k \geq i - 1$, $c_k p^k = 0$ in $\mathbb{Z}/p^i\mathbb{Z}$. So, $\psi$ maps $S$ into $R$.

Next, we show that $\psi$ is injective. For this, observe that if $\psi(c) = \psi(d)$, then

$$\psi_i(c) = \psi_i(d)$$

for all $i$, and so

$$\sum_{k=0}^{i-1} c_k p^k = \sum_{k=0}^{i-1} d_k p^k$$

as elements in $\mathbb{Z}/p^i\mathbb{Z}$. Since both sums are between 0 and $p^i - 1$, it follows from the uniqueness of the hint that $c_k = d_k$ for all $0 \leq k \leq i - 1$. Since $i$ was arbitrary, it follows that $c_k = d_k$ for all $k$, and hence $\psi$ is injective.

Finally, we must prove that $\psi$ is surjective. For this, let $(a_1, a_2, \ldots) \in R$, and we note that because $\phi_{j+1,i}(a_{j+1}) = a_j$, then $p^j|(a_{j+1} - a_j)$ (if we represent these by integers). If we further require $a_{j+1} \in \{0, \ldots, p^{j+1} - 1\}$ and $a_j \in \{0, \ldots, p^j - 1\}$, as we may, then $(a_{j+1} - a_j)/p^j \in \{0, \ldots, p - 1\}$. If we set $a_0 = 0$ and let

$$c = \sum_{k=0}^{\infty} c_k p^k$$

where

$$c_k = \left(\frac{a_{k+1} - a_k}{p^k}\right)$$

then $\psi(c) = (a_1, a_2, \ldots)$. Therefore, $\psi$ is surjective.

(iii) (nothing to prove here) Using the bijection $\psi$, we may identify the two sets $S$ and $R$, and so freely refer to $c = \sum_{k=0}^{\infty} c_k p^k$ as an element of $R$. Note that ring operations take on a particularly natural form in this in this way. That is, the sum and products of elements

$$c = \sum_{k=0}^{\infty} c_k p^k \text{ and } d = \sum_{k=0}^{\infty} d_k p^k.$$

are computed by simply adding and multiplying formally, then appropriately rewriting the series to have all coefficients in $\{0, \ldots, p - 1\}$.

(iv) Prove that $R$ is an integral domain and that it contains an isomorphic copy of $\mathbb{Z}$ (in particular, observe that the field of fractions of $R$ has characteristic zero!).
Solution Since we already know that $R$ is a subring with 1 of the commutative ring $\prod_{j=1}^{\infty} \mathbb{Z}/p^j\mathbb{Z}$, we need only show that $R$ contains no zero divisors. Suppose $a = (a_1, a_2, \ldots), b = (b_1, b_2, \ldots) \in R$ are nonzero elements. We must show that $ab \neq 0$. For this, let $i, j \in \mathbb{Z}$ be the smallest positive integers such that $a_i \neq 0$ and $b_j \neq 0$ (such exist since $a \neq 0$ and $b \neq 0$). This means that $p^i |a_i$ and $p^j |b_j$. Because $\phi_k(a_k) = a_i$ and $\phi_k(b_k) = b_j$ for all $k$, we see that $p^i |a_k$ for all $k \geq i$ and $p^j |b_k$ for all $k \geq j$. In particular, $p^{i+j} |a_{i+j}b_{i+j}$, and so $a_{i+j}b_{i+j} \neq 0$, so $ab \neq 0$.

(v) Prove that $c = \sum_{k=0}^{\infty} c_k p^k \in R$ is a unit if and only if $c_0 \neq 0$.

Solution Representing $c = \sum_{k=0}^{\infty} c_k p^k$ as $a = (a_1, a_2, \ldots)$ (i.e. so $\psi(c) = a$) then we see that $c_0 = 0$ if and only if $a_1 = 0$. First, observe that if $a_1 = 0$, then for any $b = (b_1, b_2, \ldots) \in R$, we have $ab = (a_1 b_1, a_2 b_2, \ldots) = (0, a_2 b_2, \ldots) \neq (1, 1, \ldots)$, so $a$ is not a unit. If, on the other hand, $a_1 \neq 0$, then $p |a_1$. As above, it follows that $p |a_j$ for all $j$. In particular, $a_j$ is invertible in $\mathbb{Z}/p^j\mathbb{Z}$. It follows that there exists $a_j^{-1} \in \mathbb{Z}/p^j\mathbb{Z}$ with $a_j a_j^{-1} = 1$. Since $\phi_{ji}$ is a homomorphism, we see that $\phi_{ji}(a_j^{-1}) = a_i^{-1}$ for all $j > i$, and hence $(a_1^{-1}, a_2^{-1}, \ldots) \in R$, and $a$ is invertible.

2. Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of prime degree $p$, and let $K \subset \mathbb{C}$ denote a splitting field.

(i) Prove that if $f(x)$ has exactly $p - 2$ roots in $\mathbb{R}$, then $[K : \mathbb{Q}] = p!$ and $\text{Aut}(K/\mathbb{Q}) \cong S_p$.

Hint: Prove that $\text{Aut}(K/\mathbb{Q})$ contains a $p$-cycle and a transposition.

Solution Since $f(x)$ has degree $p$, the action on the roots makes $\text{Aut}(K/\mathbb{Q})$ isomorphic to a subgroup of $S_p$. Since $f(x)$ is irreducible, if $\theta \in K$ is a root of $f(x)$, then $[\mathbb{Q}(\theta) : \mathbb{Q}] = p$. It follows that $p = [\mathbb{Q}(\theta) : \mathbb{Q}][K : \mathbb{Q}] = [\text{Aut}(K/\mathbb{Q})]$. By Cauchy’s theorem, there is an element of $\text{Aut}(K/\mathbb{Q})$ of order $p$. Since $p$ is prime and $\text{Aut}(K/\mathbb{Q}) \leq S_p$, and since the only elements of order $p$ in $S_p$ are $p$-cycles, we see that $\text{Aut}(K/\mathbb{Q})$ contains a $p$-cycle.

Since there are exactly $p - 2$ real roots of $f(x)$, the other roots must be complex conjugates. Complex conjugation leaves $K$ invariant (since the coefficients of $f(x)$ are rational, hence real), and so gives an involution in $\text{Aut}(K/\mathbb{Q})$. Since it fixes all the real roots, this is a transposition. In $S_n$, any transposition and $n$-cycle generate the entire group (appealing to Proposition 4.3.10, it is straightforward to see that every transposition is in the group generated by a single transposition and an $n$-cycle). It follows that $\text{Aut}(K/\mathbb{Q})$ is all of $S_p$ as required.

(ii) Construct a degree 4 polynomial $f(x) \in \mathbb{Q}[x]$ with exactly 2 real roots in
the splitting field $K \subset \mathbb{C}$ (so the assumption that $p$ is prime should be used in your proof).

This question was supposed to ask for such an $f(x)$ which was irreducible and so that $\text{Aut}(K/\mathbb{Q}) \neq S_4$. However, I graded this question as it is stated here.
**Solution** The polynomial \( f(x) = x^4 - 3 \) is irreducible, and as we showed in class, the splitting field is \( \mathbb{Q}(\sqrt[4]{3}, i) \). The four roots of \( f(x) \) are \( \sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3} \), which has exactly two real roots. Furthermore, observe that \( [\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}] = 8 \neq 4! \).

3. Let \( ch(F) = p < \infty, a \in F \) and consider the polynomial \( f(x) = x^p - x + a \in F[x] \). Let \( K/F \) be the splitting field of \( f \).

   (i) Show that \( K/F \) is Galois.

**Solution** \( f'(x) = px^{p-1} - 1 = -1 \) since \( ch(F) = p \), so \( f(x) \) and \( f'(x) \) have no roots in common. It follows that \( f(x) \) is separable, and so \( K/F \) is Galois.

   (ii) Show that if \( \alpha \in K \) is a root of \( f \), so is \( \alpha + c \) for \( c \in \mathbb{F}_p \), and that this gives all the roots of \( f \).

**Solution** Observe that \( \alpha \) is a root and \( c \in \mathbb{F}_p \), then

\[
f(\alpha + c) = (\alpha + c)^p - (\alpha + c) + a = \alpha + c^p - \alpha + a = c^p - c = 0
\]

where the last equality comes from the fact that \( c \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \) and Fermat’s Little Theorem (or from the fact that \( c^p = \sigma(c) \), where \( \sigma \) is the Frobenius endomorphism, and this fixes \( \mathbb{F}_p \)). It follows that \( \alpha + c \) is a root for all \( c \in \mathbb{F}_p \), and since there are exactly \( p \) such elements, these are all the roots.

   (iii) Let \( G = Aut(K/F) \). Fix a root \( \alpha \in K \) of \( f \), and show that the function \( \phi : G \to K \) defined by \( \phi(\sigma) = \sigma(\alpha) - \alpha \) has image in \( \mathbb{F}_p \), and is an injective homomorphism of groups (where \( \mathbb{F}_p \) is viewed as the additive group \( \mathbb{Z}/p\mathbb{Z} \)).

**Solution** Since \( \sigma(\alpha) = \alpha + c_\sigma \) for some \( c_\sigma \in \mathbb{F}_p \) by part (ii), we see that \( \sigma(\alpha) - \alpha = c_\sigma \in \mathbb{F}_p \). So, \( \phi(\sigma) = c_\sigma \in \mathbb{F}_p \). To see that \( \phi \) is a homomorphism, let \( \sigma, \tau \in Aut(K/F) \). Then

\[
\phi(\tau \circ \sigma) = \tau \circ \sigma(\alpha) - \alpha = \tau(\sigma(\alpha)) - \alpha
\]

\[
= \tau(\alpha + c_\sigma) - \alpha = \alpha + \tau(c_\sigma) - \alpha
\]

\[
= \tau(c_\sigma + c_\sigma) = \phi(\tau) + \phi(\sigma)
\]

where \( \tau(c_\sigma) = c_\sigma \) because \( c_\sigma \in \mathbb{F}_p \subset F \). Therefore, \( \phi \) is a homomorphism.

Finally, to see that \( \phi \) is injective, we note that \( \phi(\sigma) = 0 \) if and only if \( \sigma(\alpha) = \alpha \). Since \( \sigma(\alpha + c) = \alpha + \sigma(c) = \alpha + c \), it follows that \( \sigma \) fixes all the roots of \( f(x) \), and so is the trivial automorphism. Therefore, \( \phi \) is injective.

   (iv) Use (iii) to describe the group \( G \) up to isomorphism. (There is more than one possibility depending on \( [K : F] \).) Use this to prove that \( f \) is either irreducible over \( F \), or splits completely over \( F \).

**Note:** Since \( ch(F) = p \), we have \( \mathbb{F}_p \subseteq F \), but we are not assuming they are equal.

**Solution** Since \( G \) is isomorphic to a subgroup of \( \mathbb{F}_p \), it must have order 1 or \( p \). In the former case, \( K = F \), and so all the roots of \( f(x) \) lie in \( F \), and so \( f(x) \) splits completely in \( F \). Otherwise, \( G \cong \mathbb{F}_p \) and \( [K : F] = p \). In this case, adjoining some root gives a nontrivial extension \( F(\alpha)/F \). Since the only
subfield of $K$ containing $F$ other than $F$ is $K$. It follows that that the minimal polynomial of $\alpha$ over $F$ is degree $p$, which must therefore be $f(x)$, and hence $f(x)$ is irreducible.

4. Let $p_1, p_2, \ldots, p_n$ be distinct primes in $\mathbb{Z}_+$. For concreteness, let $\sqrt{p_i} \in \mathbb{R}_+$ be the positive square root. In this problem you will analyze the extension $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$, which is the splitting field of the polynomial

$$f(x) = (x^2 - p_1)(x^2 - p_2) \cdots (x^2 - p_n).$$

(i) Prove that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] \leq 2^k$ for any $1 \leq k \leq n$.

**Solution** We have $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_2}) : \mathbb{Q}(\sqrt{p_1})] = 2$ since $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_2})$ is obtained from $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_j})$ by adjoining $\sqrt{p_j}$, a root of $x^2 - p_j$, which has degree 2. Therefore

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})] \cdots [\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] \leq 2 \cdots 2 = 2^k$$

(ii) Assuming $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$ for some $1 \leq k \leq n$, prove that the following is a basis for $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q}$

$$\{1\} \cup \bigcup_{r=1}^{k} \{\sqrt{p_{i_1}} \cdots \sqrt{p_{i_r}} \}_{i_1 < i_2 < \ldots < i_r}.$$

Hint: write the extension as an iterated extension

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1}) \subseteq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \subseteq \ldots \subseteq \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}).$$

**Solution** This is proven by induction. Observe that the suggested basis is just the set of all possible products of distinct elements of $\{\sqrt{p_1}, \ldots, \sqrt{p_k}\}$ and 1. This is clear for $k = 1$. Assuming the set is a basis for $j < k$, it is proven for $k$ by first observing that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})] = 2$ from the equality situation of part (i). A basis for this extension is $\{1, \sqrt{p_k}\}$. Now the argument from Lemma 13.2.16 proves the case $k$.

(iii) Continuing to assume $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$, prove

$$\text{Aut}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^k.$$

Further, if $\sigma_1, \ldots, \sigma_k \in \text{Aut}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q})$ are generators corresponding under the isomorphism to generators of the factors $\mathbb{Z}/2\mathbb{Z}$, describe the effect of each $\sigma_i$ on the basis from part (ii).

**Solution** Observe that since $\{p_i\}_{i=1}^{k}$ are distinct primes, the roots of $f(x)$ are distinct, and $f(x)$ is separable. Therefore, $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})/\mathbb{Q}$ is Galois with Galois group $G$ of order $2^k$. Each element $\sigma \in G$ must permute the roots of the irreducible factors of $(x^2 - p_1) \cdots (x^2 - p_n)$. There are $2^k$ such permutations, so each such is induced by an element $\sigma \in G$. Explicitly, let $\sigma_i$ be the permutation which interchanges $\{\pm \sqrt{p_i}\}$, the two roots of $x^2 - p_i$, and fixes all the other roots. Since the permutations $\sigma_i$ and $\sigma_j$ commute for all $1 \leq i, j \leq k$, and each has order 2, it follows that $G = \langle \sigma_1, \ldots, \sigma_k \rangle \cong (\mathbb{Z}/2\mathbb{Z})^k$ with $\sigma_i$ generating the $i^{th}$ factor.
Given $\sigma_i$ and any $\sqrt{p_{i_1}\cdots p_{i_r}}$ we see that

$$\sigma_i(\sqrt{p_{i_1}\cdots p_{i_r}}) = \begin{cases} \sqrt{p_{i_1}\cdots p_{i_r}} & \text{if } i \notin \{i_1, \ldots, i_r\} \\ -\sqrt{p_{i_1}\cdots p_{i_r}} & \text{if } i \in \{i_1, \ldots, i_r\} \end{cases}$$

(iv) Prove that $[Q(\sqrt{p_1}, \ldots, \sqrt{p_k}) : Q] = 2^k$ for all $1 \leq k \leq n$.

Hint: Use induction. If there is $1 \leq k \leq n$ with $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$, pick the smallest $j \leq k - 1$ so that $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_j})$. Write $\sqrt{p_k}$ in terms of the basis from part (ii), and consider the product $\sqrt{p_k} \cdot \sigma_j(\sqrt{p_k})$.

Solution We follow the hint up to a point (though I found a much more direct way to prove this which I’m presenting here). The base case is clear, and we assume the result for $j < k$, and prove it for $k$. We suppose that $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$ and will arrive at a contradiction.

Observe that $Q \subset Q(\sqrt{p_k}) \subset Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$ and $[Q(\sqrt{p_k}) : Q] = 2$. Since $Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})/Q$ is Galois, the Fundamental Theorem of Galois Theory describes all the intermediate fields as the fixed subfields of subgroups of the Galois group $G$. These are easily computed by the action described in (iii), and in particular we see that there exists $1 \leq i_1 < \ldots < i_r \leq k - 1$ so that

$$Q(\sqrt{p_k}) = Q(\sqrt{p_{i_1}\cdots p_{i_r}}).$$

(in my previous proof, the equivalent of this statement was derived by a lengthy calculation). From here, it follows that

$$\sqrt{p_k} = a + b\sqrt{p_{i_1}\cdots p_{i_r}}$$

and

$$p_k = a^2 + 2ab\sqrt{p_{i_1}\cdots p_{i_r}} + b^2p_{i_1}\cdots p_{i_r}$$

so, since the left side is rational, so is the right side. Therefore $ab = 0$, and so $a = 0$ or $b = 0$. Since $\sqrt{p_k} \notin Q$, it follows that $a = 0$ and $b \neq 0$. Then writing $b = r/s$ with $r, s \in \mathbb{Z}$ and $(r, s) = 1$ we have

$$p_k s^2 = r^2p_{i_1}\cdots p_{i_r}.$$