Question: 4

Prove or disprove: Any subring of a field F containing 1 is an integral domain.

Solution: Let $R \subseteq F$. Suppose $x, y \in R$ such that $xy = 0$. Since the 0 element is the same in R and F, either $x = 0$ or $y = 0$ and as such, R has no zero divisors and therefore, is an integral domain. 😄

Question: 6

Let F be a field of characteristic zero. Prove that F contains a subfield isomorphic to $\mathbb{Q}$.

Solution: Let $\phi : \mathbb{Z} \to F$ and define $\phi(1_{\mathbb{Z}}) = 1_F$. Characteristic 0 means that ϕ is injective. We can use this to define $\varphi : \mathbb{Q} \to F$ such that $\varphi(a/b) = \phi(a)/\phi(b)$ whenever $b \neq 0_{\mathbb{Z}}$. This is a homomorphism because:

$$\varphi(1_{\mathbb{Z}}/1_{\mathbb{Z}}) = \phi(1_{\mathbb{Z}})/\phi(1_{\mathbb{Z}}) = 1_F/1_F = 1_F,$$

$$\varphi(\frac{a}{b}\frac{c}{d}) = \varphi(\frac{ac}{bd}) = \frac{\phi(ac)}{\phi(bd)} = \frac{\phi(a)}{\phi(b)}\frac{\phi(c)}{\phi(d)} = \varphi(\frac{a}{b})\varphi(\frac{c}{d}),$$

$$\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{ad+bc}{bd}) = \frac{\phi(ad+bc)}{\phi(bd)} = \frac{\phi(a)\phi(d) + \phi(b)\phi(c)}{\phi(b)\phi(d)} = \frac{\phi(a)}{\phi(b)} + \frac{\phi(c)}{\phi(d)} = \phi(\frac{a}{b}) + \phi(\frac{c}{d}).$$

φ is also injective because cross-multiplication. This injectiveness means that $ad = bc \implies a/b = c/d$. As such, contains a subfield isomorphic to $\mathbb{Q}$ that is $\varphi(\mathbb{Q}) \subseteq F$. 😄

Question: 10

A field F is called a ***prime field*** if it has no proper subfields. If E is a subfield of F and E is a prime subfield of F:

a. Prove that every field contains a unique prime subfield.

b. If F is a field of characteristic 0, prove that the prime subfield of F is isomorphic to the field of rational numbers, $\mathbb{Q}$.

c. If F is a field of characteristic p, prove that the prime subfield of F is isomorphic to the field of integers modulo p, $\mathbb{Z}_p$.

Solution:

a. To convince ourselves that E is nonempty, we realize that $0, 1 \in E$. For any $a, b \in E$, $a, b \in L$, so ab, $a+b$, $a-b$, and a/b are all in L, and thus all in E. As such, E is a subfield.

   If $L \subset E$ is a proper subfield, it is a subfield of F too. By definition, E is contained in all subfields of F. As such, E is a prime field.

   If E' is another prime subfield, by construction, $E \subseteq E'$. Since E' is prime, $E' = E$. 😄

b. Define $\phi : \mathbb{Z} \to F$ as $\phi(x) = x * 1_F$. F having characteristic 0 means that this definition of ϕ is injective, so its image is a subring of F isomorphic to $\mathbb{Z}$. By a theorem related to a field of fractions that we covered in class, F contains a subfield isomorphic to $\mathbb{Q}$. $\mathbb{Q}$ has no subfields, it is prime, and by part a., it is the unique subfield of F. 😄

c. Define ϕ the same as we did in b. Since $\text{char}(F) = p$, the kernel of ϕ is $p\mathbb{Z}$. By the first isomorphism theorem, the image of ϕ is isomorphic to $\mathbb{Z}_p$, which is a prime field. By part a., it is the unique prime field of F. 😄