Problem 1. Prove that there is an injective homomorphism between the group of homomorphisms of $\frac{\mathbb{Q}[\zeta]}{\mathbb{Q}}$ where ζ is the nth root of unity $\zeta^n = 1$ and the multiplicative group R_n where $\{x \in R_n : \gcd(x, n) = 1\}$

Proof. First, we need to establish some results about the homomorphisms of $\frac{\mathbb{Q}[\zeta]}{\mathbb{Q}}$. Let σ be one such homomorphism. Thus σ permutes the roots of $z^n - 1$. Now, we know from definition that for ζ^k where k is from 1 to $n-1$ that $\sigma(\zeta) \neq \zeta$; else we would have that σ doesn't just fix the rationals, and that would be a contradiction.

What else can we say about σ? We already know that the elements $1, \zeta, \zeta^2 ..., \zeta^{n-1}$ form a cyclic group with generator ζ. From our knowledge of cyclic groups, the image of a cyclic group of order n under a group homomorphism is the cyclic group generated by the image of the generator. Thus if we wish to apply the homomorphism σ to ζ we need to force $\sigma(\zeta)$ to also be a generator of a cyclic group of order n; or in other words, the image of ζ under σ should also be one of the nth roots of unity. Thus $\sigma(\zeta) = \zeta \cdot \zeta^s$ where s is relatively prime to n (note that we include 1 as a value that is relatively prime to n). The relatively prime is crucial- if we did not have that condition, then we are not guaranteeing that $\sigma(\zeta)$ is a generator of a cyclic group of order n: we could have that $\sigma(\zeta)$ generates a cyclic group of order a where a is one of the prime factors of n less than n; since the cyclic group generated by $\sigma(\zeta)$ is not isomorphic to the one generated by ζ, we conclude that at least one ζ^i must exist where $\sigma(\zeta^i)$ is not a root of unity, which contradicts the definition of homomorphism: if $\zeta^n = 1$ then $\sigma(\zeta^n) = \sigma(\zeta)^n = 1$. The easiest case to see this occuring is when $n = 4$: examine $\sigma(\zeta) = \zeta \cdot \zeta^2$. The roots of unity in this case are $\{1, \zeta, \zeta^2, \zeta^3\}$; applying σ we get the new values $\{\zeta^2, \zeta^3, 1, \zeta\}$. However, note that ζ^2 only generates a cyclic subgroup of order 2: since $\zeta^4 = 1$, $(\zeta^2)^2 = 1$.

So σ is of the form $\sigma(\zeta) = \zeta \cdot \zeta^s$ where s is relatively prime to n. From here, we need to establish a homomorphism from the group of homomorphisms that σ is a member of to the group R_n. Let f map $\sigma : \sigma(\zeta) = \zeta \cdot \zeta^s$ to $s \in R_n$ where s may fall into a conjugacy class mod n.

f is a homomorphism: let $\sigma = \zeta \cdot \zeta^s$ and $\tau = \zeta \cdot \zeta^t$ be two elements of the group of homomorphisms as described above on the field extension. $f(\sigma\tau) = f(\zeta \cdot \zeta^s \cdot \zeta^t) \equiv st \mod n \equiv f(\sigma)f(\tau)$. The first equals sign comes from the interpretation that "σ or τ is multiplication by s or t times ζ; it's rotation by ζ s or t times." The next equals sign comes from our definition of f; the next equals sign is because $f(\sigma) \equiv s \mod n$ and $f(\tau) \equiv t \mod n$.

f is injective: consider the kernel of f. The identity element in the multiplicative group R_n is 1. For $\sigma(\zeta) = \zeta \cdot \zeta^s$ with s between 1 and $n-1$, s relatively prime to n, the preimage of 1 is $\square$