Math 541
Homework 6

§7.5 #4. Let F be a subfield of $\mathbb{R}$. Then $1 \in F$, so $1 + \cdots + 1 \in F$, and $-1 \in F$, so $(-1) + \cdots + (-1) \in F$, so $\mathbb{Z} \subseteq F$. Since F contains multiplicative inverses, $1/n \in F$ for all $n \in \mathbb{Z}^+$, so $m \cdot 1/n \in F$ for all $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, so $\mathbb{Q} \subseteq F$.

§7.6 #4. If R and S are nonzero, let $r \in R$ and $s \in S$ be different from zero; then $(r, 0) \cdot (0, s) = (0, 0)$, so $R \times S$ has zero divisors. But in §7.1 we saw that fields contain no zero divisors.

7. Our argument is actually quite simple, but maddeningly difficult to make look simple.

First we prove a lemma: if $\varphi : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ is any surjective ring homomorphism (not necessarily the natural projection) and $a \in \mathbb{Z}$ then $\varphi(a)$ is a unit in $\mathbb{Z}/k\mathbb{Z}$ if and only if a relatively prime to k. Something similar to this is stated without proof in §7.1.

Since $\ker \varphi$ is an ideal of $\mathbb{Z}$, $\ker \varphi = k'\mathbb{Z}$ for some $k' \in \mathbb{Z}$. By the first isomorphism theorem, $\operatorname{im} \varphi \cong \mathbb{Z}/\ker \varphi = \mathbb{Z}/k'\mathbb{Z}$, so the order of $\operatorname{im} \varphi$ is k'. Since φ is surjective, $k' = k$, so $\ker \varphi = k\mathbb{Z}$. Thus for all $z \in \mathbb{Z}$, $\varphi(z) = 0$ if and only if k divides z.

Let d be the greatest common factor of a and k. Then $0 = \varphi(k \cdot a/d) = \varphi(a \cdot k/d) = \varphi(a)\varphi(k/d)$. If $\varphi(a)$ is a unit then $\varphi(k/d) = 0$, so k divides k/d, so $d = 1$.

Consider the group homomorphism $\mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ defined by $x \mapsto \varphi(a)x$. If $\varphi(a)$ is not a unit then 1 is not in the image of this map, so the map is not surjective, so since the domain and codomain are finite sets of the same size, it is not injective, so it the kernel is not zero, so there is a nonzero $x \in \mathbb{Z}/k\mathbb{Z}$ such that $\varphi(a)x = 0$. Now $x = \varphi(b)$ for some $b \in \mathbb{Z}$, so $0 = \varphi(a)x = \varphi(a)\varphi(b) = \varphi(ab)$, so k divides ab, but k does not divide b since $\varphi(b) = x \neq 0$, so k and a have a common factor. This proves the lemma.

For the main result, let s be the greatest integer that divides m and is relatively prime to n, and let $r = m/s$. (If $m = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$ is the prime factorization of m then r is the product over all p_i that divide n of ${p_i}^{\alpha_i}$ and s is the product over all p_i that do not divide n.) Then r and s are relatively prime, so by the Chinese Remainder Theorem $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/rs\mathbb{Z} \cong (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$, so the natural projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ induces a surjection $\varphi : (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$. It is enough to show that φ is surjective on the units.

If $x \in \mathbb{Z}/r\mathbb{Z}$ and $y \in \mathbb{Z}/s\mathbb{Z}$ then $\varphi(x, y) = \varphi(x, 0)$, as follows. Since s is relatively prime to n, $1 + \cdots + 1$ (s times) is a unit in $\mathbb{Z}/n\mathbb{Z}$. Now

$$(1 + \cdots + 1)\varphi(0, y) = \varphi(0, y) + \cdots + \varphi(0, y) = \varphi(0, y + \cdots + y) = \varphi(0, 0) = (0, 0)$$

so $\varphi(0, y) = (0, 0)$. Thus $\varphi(x, y) = \varphi(x, 0) + \varphi(0, y) = \varphi(x, 0)$.

Let $\pi : \mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ be the natural projection. Then the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $a \mapsto \varphi(\pi(a), 0)$ is surjective: if $z \in \mathbb{Z}/n\mathbb{Z}$ then there are $x \in \mathbb{Z}/r\mathbb{Z}$ and $y \in \mathbb{Z}/s\mathbb{Z}$ such that $z = \varphi(x, y) = \varphi(x, 0)$, and there is an $a \in \mathbb{Z}$ such that $x = \pi(a)$, so $z = \varphi(\pi(a), 0)$.

If z is a unit then a is relatively prime to n, hence is relatively prime to r, so $\pi(a)$ is a unit, so $(\pi(a), 1)$ is a unit. But $\varphi(\pi(a), 1) = \varphi(\pi(a), 0) = z$, so φ is surjective on the units.