Set 1 - Ma 5b - Solutions

Luciena Xiao

January 16, 2017

7.1.7. Let $R$ be a ring and let $Z(R)$ denote its center. First note that $1 \in Z(R)$ because $1 \cdot r = r = r \cdot 1$ for any $r \in R$. Now, to show $Z(R)$ is a subring, it suffices to show closure under subtraction and multiplication: for any $a, b \in Z(R)$ and $r \in R$, we have $(a - b)r = ar - br = ra - rb = r(a - b)$, and $abr = arb = rab$. Thus $Z(R)$ is indeed a subring that contains the identity.

Suppose $R$ is a division ring. For any $a \in Z(R), a \in R$ and $a^{-1}$ exists because $R$ is a division ring. For any $r \in R, a^{-1}r = (r^{-1}a)^{-1} = (ar^{-1})^{-1} = a^{-1}r$, which implies $a^{-1} \in Z(R)$. This proves that $Z(R)$ is a division ring. Clearly, $Z(R)$ is commutative, so $Z(R)$ is a field.

7.1.13. (a) Clearly, $a^k b^k = (ab)^k$ and $n = a^k b^k | a^m b^m$, so $(ab)^k \equiv 0 \mod n$, i.e. $ab$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

(b) Suppose $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent, then $n|a^m$ for some positive integer $m$. Thus if $p$ is any prime divisor of $n$, then $p|a^m$, which implies $p|a$.

Conversely, suppose any prime divisor $p$ of $n$ also divides $a$. Write $n = \prod_{i=1}^{k} p_i^{m_i}$ where $p_i$ are primes. Let $m = \max\{m_1, \cdots, m_k\}$, then $n|a^m$, so $\overline{a}$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

By the above statement, all nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ must be multiples of 6 since $72 = 2^33^2$.

Therefore they are: $0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66$.

(c) Suppose $f \in R$ is nilpotent. Then there exists some positive integer $m$ such that for any $x \in X, (f(x))^m = 0$. Since $F$ is a field and $f(x) \in F$, $f(x)$ cannot be a zero divisor, so $f(x) = 0$. But this holds for any $x \in X$, so $f$ is the zero function. Therefore $R$ has no non-zero nilpotent element.

7.1.14. (a) Since $x$ is nilpotent, there exists some minimal positive integer $m$ with $x^m = 0$. If $m = 1, x = 0$; otherwise $x^{m-1} = 0$ where $x^{m-1} \neq 0$, which implies $x$ is a zero divisor.

(b) gain, since $x$ is nilpotent, there exists $m$ such that $x^m = 0$. Since $R$ is commutative, for any $r \in R$ we have $(rx)^m = r^m x^m = r^m 0 = 0$, so $rx$ is nilpotent.

(c) Let $m$ be as above. $1 = 1 + x^m = (1 + x)(1 - x + \cdots + (-x)^{m-1})$, so $1 + x$ is a unit.

(d) For any unit $a \in R, a + x = a(1 + a^{-1}x)$. By parts (b) and (c), $1 + a^{-1}x$ is a unit. A product of units is a unit, so $a + X$ is a unit.
7.1.23. We first prove \( \mathcal{O}_f \) is a subring containing the identity. \( 1 = 1 + 0f\omega \), so \( 1 \in \mathcal{O}_f \). For any \( x = a + b\omega, y = c + d\omega \in \mathcal{O}_f \), we have \( x - y = (a-c) + (b-d)f\omega \in \mathcal{O}_f \). Also, \( xy = (ac + bdf^2\omega^2) + (ac + bd)f\omega \). If \( D \not\equiv 1 \) mod 4, then \( \omega^2 = D \) and \( xy \) is clearly in \( \mathcal{O}_f \); if \( D \equiv 1 \) mod 4, then \( \omega^2 = (1 + \sqrt{D})^2/4 = (D-1)/4 + \omega \) and \( 4|D-1 \), so we can write \( xy = (ac + bdf^2(D-1)/4) + (ac + bd + bdf)f\omega \), which is in \( \mathcal{O}_f \). Thus \( \mathcal{O}_f \) is a subring.

One can define a map \( \phi : \mathcal{O} \to \mathcal{O}_f \) by \( a + b\omega \mapsto a + b'f\omega \) where \( b' \) is the remainder of \( b \) modulo \( f \). It is easy to check that this map is a \( f \)-to-1 group homomorphism, so \( |\mathcal{O} : \mathcal{O}_f| = |\ker(\phi)| = f \).

Now conversely suppose \( R \subset \mathcal{O} \) is a subring with the stated properties. Then there exists a smallest integer \( f' \) such that \( f'\omega \in R \) since otherwise \( R \) wouldn’t have finite index. Now if there exists \( n\omega \in R \) with \( f' \nmid n \), then \( n'\omega \in R \) where \( n' \) is the remainder of \( n \) modulo \( f' \), contradicting the minimality of \( f' \). Therefore \( R \) must be of the form \( \mathbb{Z}[f'\omega] \). By the previous result we conclude \( f' = f \), i.e. \( R = \mathcal{O}_f \).

7.3.17. (a) Suppose \( \phi(1) \neq 1 \). Then \( \phi(1)^2 = \phi(1^2) = \phi(1) \), so \( \phi(1)(\phi(1) - 1) = 0 \), but \( \phi(1) - 1 \neq 0 \), so we conclude \( \phi(1) \) is a zero divisor. If \( S \) is an integral domain, then \( S \) contains no zero divisor, so \( \phi(1) \) must be the identity.

(b) If \( u \) is a unit, then \( 1 = \phi(1) = \phi(u\bar{u}^{-1}) = \phi(u)\phi(u^{-1}) \), so \( \phi(u) \) is a unit and \( \phi(u^{-1}) = \phi(u)^{-1} \).

7.3.22. (a) Write \( I = \{ x \in R | ax = 0 \} \). Clearly 0 \( \in I \), so \( I \) is nonempty. For any \( x, y \in I \), we have \( a(x - y) = ax - ay = 0 - 0 = 0 \) and \( a(xy) = (ax)y = 0y = 0 \), so \( I \) is closed under subtraction and multiplication. Thus \( I \) is a subring of \( R \). For any \( x \in I \) and \( r \in R \), \( a.xr) = (ax)r = 0 \), so \( I s \subset R \) for all \( s \in R \). Thus \( I \) is a right ideal. Similarly, the left annihilator is a left ideal.

(b) Write \( I = \{ x \in R | xa = 0 \) for all \( a \in L \} \). By an argument analogous to part (a) we see \( I \) is a subring. For any \( r \in R, x \in I, a \in L \) we have \( (rx)a = r(xa) = r0 = 0 \) and \( (xr)a = x(ra) = 0 \) since \( ra \in L \). Thus \( I \) is a two-sided ideal.