

Math 541  
Problem Set 9

7.4.4. This is immediate from Proposition 7.4.12, since  $R \cong R/(0)$ .

7.4.13. (a) First observe that a subring of an integral domain is either an integral domain or 0, since any zero divisors in the subring would be zero divisors in the big ring.

Let  $\psi : S \rightarrow S/P$  be the natural map and consider the composition  $\psi \circ \varphi : R \rightarrow S/P$ . We have

$$\ker(\psi \circ \varphi) = (\psi \circ \varphi)^{-1}(0) = \varphi^{-1}(\psi^{-1}(0)) = \varphi^{-1}(\ker \psi) = \varphi^{-1}(P),$$

so by the first isomorphism theorem,  $\text{im}(\varphi \circ \psi) = R/\varphi^{-1}(P)$ . Now  $\text{im}(\varphi \circ \psi)$  is a subring of the integral domain  $S/P$ , hence is either 0 or is itself an integral domain, so  $\varphi^{-1}(P)$  is either  $R$  or a prime ideal by Proposition 7.4.13.

For second statement, observe that if  $R$  is a subring of  $S$  and  $\varphi : R \rightarrow S$  is the inclusion, then  $\varphi^{-1}(P) = R \cap P$ .

(b) Again let  $\psi : S \rightarrow S/M$  be the natural map and consider the composition  $\psi \circ \varphi : R \rightarrow S/M$ . Since both  $\varphi$  and  $\psi$  are surjective, so too is  $\psi \circ \varphi$ . By the first isomorphism theorem,  $R/\ker(\psi \circ \varphi) \cong \text{im}(\psi \circ \varphi) = S/M$ . Since  $S/M$  is a field,  $\ker(\psi \circ \varphi) = \varphi^{-1}(M)$  is maximal by Proposition 7.4.12.

For a counterexample when  $\varphi$  is not surjective, let  $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$  be the inclusion. Since  $\mathbb{Q}$  is a field,  $(0)$  is maximal, but  $\varphi^{-1}((0)) = (0)$  is not maximal in  $\mathbb{Z}$ ; for example, it is contained in the ideal  $(4)$ .

7.4.27. Since  $a$  is nilpotent, there is an  $n \geq 1$  such that  $a^n = 0$ . Observe that

$$(1 - ab)(1 + ab + a^2b^2 + \cdots + a^{n-1}b^{n-1}) = 1 - a^n b^n = 1,$$

so  $1 - ab$  is a unit.

7.5.3. Let  $\varphi : \mathbb{Z} \rightarrow F$  be the ring homomorphism determined by  $\varphi(1) = 1$ . Then  $\text{im } \varphi$  is a subring of  $F$  and is not 0 since  $1 \neq 0$  in  $F$ , so  $\text{im } \varphi$  is an integral domain. Thus  $\ker \varphi$  is a prime ideal of  $\mathbb{Z}$ , so either  $\ker \varphi = p\mathbb{Z}$  for some prime number  $p$  or  $\ker \varphi = (0)$ . In the former case,  $\text{im } \varphi \cong \mathbb{Z}/p\mathbb{Z}$ , which is a field, so we are done. In the latter case,  $\text{im } \varphi \cong \mathbb{Z}$ , so take

$$F_0 = \{m/n \in F : m, n \in \text{im } \varphi \text{ and } n \neq 0\}$$

which is isomorphic to  $\mathbb{Q}$ .

We got  $F_0$  by letting 1 generate a field, but any subfield of  $F$  contains 1, hence contains  $F_0$ .

(7.5.1. on reverse.)

7.5.1. In the proof of Theorem 7.5.15, they observe that  $r/d = re/rd$  for all  $e \in D$ . We will use this fact freely.

Multiplication is well-defined: if  $a/b = a'/b'$  and  $c/d = c'/d'$  then  $ab' = a'b$  and  $cd' = c'd$ , so  $acb'd' = a'c'bd$ , so  $ac/bd = a'c'/b'd'$ .

The additive identity is  $0/d$ :  $a/b + 0/d = (ad + 0b)/bd = ad/bd = a/b$ .

The additive inverse of  $a/d$  is  $-a/d$ :  $a/d + -a/d = (ad - ad)/d^2 = 0/d^2$ .

Addition is associative:  $(a/b + c/d) + e/f = (ad + bc)/bd + e/f = (adf + bcf + bde)/bdf$ , whereas  $a/b + (c/d + e/f) = a/b + (cf + de)/df = (adf + bcf + bde)/df$ , which is the same.

Addition is commutative:  $a/b + c/d = (ad + bc)/bd$ , whereas  $c/d + a/b = (cb + da)/db$ , which is the same since  $R$  is commutative.

Multiplication is associative:  $(a/b \cdot c/d) \cdot e/f = (ac/bd) \cdot e/f = (ac)e/(bf)d$ , whereas  $a/b \cdot (c/d \cdot e/f) = a/b(ce/df) = a(ce)/b(df)$ , which is the same since multiplication in  $R$  is associative.

Multiplication is distributive:  $(a/b + c/d) \cdot e/f = [(ad + bc)/bd] \cdot e/f = [(ad + bc)e]/bdf = (ade + bce)/bdf$  since multiplication in  $R$  is distributive, whereas  $a/b \cdot e/f + c/d \cdot e/f = ae/bf + ce/df = (aedf + cebf)/bdf^2 = (aed + ceb)f/bdf^2$ , which is the same. Distributivity on the other side is similar.

Multiplication is commutative:  $a/b \cdot c/d = ac/bd$ , whereas  $c/d \cdot a/b = ca/db$ , which is the same since multiplication in  $R$  is commutative.

The multiplicative identity is  $d/d$ :  $a/b \cdot d/d = ad/bd$ , which equals  $a/b$  since  $adb = bda$ .