Page 254

4. The zero divisors in Z_{20} are $\{2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18\}$. Every nonzero element is either a zero divisor or a unit.

7. See back.

13. Suppose $a \in R$ and R is a ring with unity. Then the distributive law gives $(1-a)(1+a+a^2+\cdots+a^{n-1}) = 1-a^n$. Thus if $a^n = 0$ then $(1+a+a^2+\cdots+a^{n-1})$ is the multiplicative inverse of $1-a$.

16. If $a^2 = a$ then $a(a-1) = 0$. In an integral domain this implies $a = 0$ or $a - 1 = 0$. Thus 0 and 1 are the only idempotents in an integral domain.

22. The zero divisors of R are $\{f \mid f(a) = 0$ for some but not all $a\}$. This is because for any such f we can define $g(x)$ to be one whenever $f(x)$ is 0 and to be zero elsewhere. Then $f(x)g(x) = 0$ but neither is the zero function. The only nilpotent element is the zero function. Finally if $f(x)$ is not a zero divisor then, by part a, it is never equal to zero. Thus $1/f(x)$ is well defined and is the multiplicative inverse to $f(x)$ in R.

38. Suppose ab is a zero divisor so $ab \neq 0$ and there exists $c \neq 0$ such that $abc = 0$. Since $ab \neq 0$ then neither a nor b is zero. Now $a(bc) = 0$ so either a is a zero divisor or $bc = 0$. But if $bc = 0$ then b is a zero divisor. Thus either a or b is a zero divisor.

42. Suppose $a^n = 0$. From # 41 we know that $(1+a)^{p^m} = 1 + a^{p^m}$. Thus choose m so that $p^m > k$. Thus $a^{p^m} = 0$ and so $(1+a)^{p^m} = 1$.

26. First check that 6 is a multiplicative identity. Then check that $2 * 8 = 4 * 4 = 6 * 6 = 6$ so every nonzero element has a multiplicative inverse.

44. $Z_3[x]$ is an infinite integral domain of characteristic 3.

55. Suppose $x^p = x$ and $y^p = y$. Then $(x-y)^p = x^p + (-1)^p y^p$. If p is odd, this is $x - y$. If p is 2 this is $x + y$ which is the same as $x - y$ since $-1 = 1$ in characteristic 2. Either way we have $(x-y)^p = x - y$ so $x - y \in K$. Also $(xy^{-1})^p = x^p/y^p = x/y = xy^{-1}$ so $xy^{-1} \in K$. Thus K is a subfield.

Page 268

4. Let $S = \{(a, a) \in Z \oplus Z\}$. Then S is a subring but not an ideal, for example $(1, 0) * S \not\subseteq S$.

5. See back.

12. Let $x = a_1b_1 + a_2b_2 + \cdots + a_nb_m, y = A_1B_1 + A_2B_2 + \cdots + A_mB_m \in AB$. $x - y$ is obviously in AB, it is just a sum of $m + n$ terms of the proper form. Let $r \in R$. Then $rx = ra_1b_1 + ra_2b_2 + \cdots + ra_nb_m$. A is an ideal so $ra_i \in A$ so $rx \in AB$. Similarly $xr \in AB$

since $b_i r \in B$ since B is an ideal. Thus AB is an ideal.

14. Since any $a_i b_i$ must be in A (since A is an ideal) and in B (since B is an ideal), then it is in $A \cap B$ so $AB \subset A \cap B$.

15. If $1 \in A$ then $r * 1 = r \in A$ for any $r \in R$.

29. Suppose $A \subset I \subseteq R$ where $A \neq I$. Let $g(x) \in I - A$ so $g(0) \neq 0$. Let $f(x) \in R$. Then:

$$f(x) = \left(f(x) - \frac{f(0)}{g(0)} g(x) \right) + \frac{f(0)}{g(0)} g(x).$$

Let $f(x) - \frac{f(0)}{g(0)} g(x) = h(x)$. Notice that $h(0) = 0$ so $h \in A \subset I$. Also $\frac{f(0)}{g(0)} g(x) \in I$ since $g(x)$ is, thus $f(x) \in I$. But $f(x)$ was arbitrary so $I = R$ and A is maximal.