

Math 351:03 — Fall 1999

MW4 SEC-217

Prof. Bumby

Workshop 8, Ideals and quotient rings.

19. Every nonzero ideal I in \mathbb{Z} contains a positive integer, and the Euclidean algorithm uses this to show that I consists of all multiples of the smallest positive integer in I . You may take this as given. Here, we let I be the ideal consisting of the multiples of 35. Another use of the Euclidean algorithm shows that each coset modulo I contains exactly one integer r with $0 \leq r < 35$. Addition and multiplication of cosets can be done by combining these representatives and finding the remainder when the result is divided by 35.

(a) Calculate 21^2 in \mathbb{Z}/I .

(b) The ideals of \mathbb{Z}/I are given by the correspondence theorem as ideals of \mathbb{Z} that contain I . Show that such ideals must be generated by divisors of 35.

(c) You may take as known that $35 = 5 \cdot 7$ and that the set of divisors of 35 is $\{1, 5, 7, 35\}$. Show that the set of multiples of 21 in \mathbb{Z}/I is the same as the set of multiples of 7 in \mathbb{Z}/I . Equivalently, show that the set of multiples of 21 in \mathbb{Z}/I consists of the cosets determined by $\{0, 7, 14, 21, 28\}$.

(d) Show that the multiples of 15 in \mathbb{Z}/I consists of the cosets determined by $\{0, 5, 10, 15, 20, 25, 30\}$.

(e) If $x \in \mathbb{Z}/I$, show that $x = 21x + 15x$ in \mathbb{Z}/I . That is, x can be written as a sum of a multiple of 5 and a multiple of 7.

(f) If a sum of a multiple of 5 and a multiple of 7 is zero in \mathbb{Z}/I , show that both terms must themselves be zero in \mathbb{Z}/I . This shows that the representation found in (e) is unique.

18*. We look at two particular ideal in $G = \mathbb{Z}[i]$, so this supplements the original problem without extending it. The ideals we consider are the multiples of 3, denoted (3), and the multiples of 5, denoted (5).

(a) Show that $G/(3)$ is a ring with 9 elements.

(b) Show that any ideal of $G/(3)$ that is neither the zero ideal nor the whole ring must contain 3 elements.

(c) Show that $G/(3)$ is a field with 9 elements by showing that there are no ideals in $G/(3)$ containing 3 elements.

(d) Show that $G/(5)$ is a ring with 25 elements.

(e) Show that any ideal of $G/(5)$ that is neither the zero ideal nor the whole ring must contain 5 elements.

(f) Find an ideal of $G/(5)$ with 5 elements, thereby showing that $G/(5)$ is not a field.

... continued on other side

20. Here, we rediscover a Theorem of Lagrange and obtain some applications. Let F be a field and consider a polynomial $p(x)$ with coefficients in F and coefficient of the highest degree term equal to 1. Examples are $x^2 - x$, $x^2 + 1$, or $x^3 - 5x + 17$. The division algorithm allows us to extend familiar results for such polynomials over the real numbers to an arbitrary field F .

(a) If $a \in F$, when $p(x)$ is divided by $x - a$ we get

$$p(x) = (x - a)q(x) + r(x) \tag{D}$$

by Theorem 4.5.5, and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $x - a$. Show that this means that $r(x)$ can be chosen to be a constant.

(b) Substitute a for x in (D). This leads to the *Factor theorem*, which says that $x - a$ divides $p(x)$ if and only if $p(a) = 0$.

(c) If $p(a) = 0$, the factor theorem tells us that

$$p(x) = (x - a)q(x), \tag{F}$$

and the degree of $q(x)$ is one less than the degree of $p(x)$. Use the assumption that F is a field to show that if $b \neq a$ and $p(b) = 0$, then $q(b) = 0$. Thus all but one root of $p(x) = 0$ is a root of the equation $q(x) = 0$ of lower degree.

(d) The theorem of Lagrange is that a polynomial of degree n over a field F has at most n roots in F . Part (c) gives the induction step of this, and the basis is the case $n = 0$, which says that a polynomial of degree 0 has no roots in F . Note that this requires that polynomials of degree zero be identified with **nonzero** constants.

(e) Apply this result to the polynomial $x^n - 1$. This says that there are at most n elements of F that can have order dividing n in the multiplicative group of F . In a finite field with q elements, there are $q - 1$ nonzero elements. Since this is the order of the multiplicative group, every nonzero element has order dividing $q - 1$. For each $d|q - 1$, there are at most d elements with order dividing d . If there were no element of order exactly $q - 1$, this would give fewer than $q - 1$ nonzero elements in F . Hence the multiplicative group of a field must be cyclic.