

Math 317 C1
HOUR EXAM III
31 July 2002

SOLUTIONS

1. Find all positive integers, $m \geq 2$, such that $x^2 + 2$ is a divisor of $x^5 - 10x + 12$ in $Z_m[x]$.

SOLUTION: The Division Algorithm gives (using long division)

$$x^5 - 10x + 12 = (x^2 + 2)(x^3 - 2x) + (-6x + 12)$$

Thus for $x^2 + 2$ to be a divisor of $x^5 - 10x + 12$, the remainder $(-6x + 12)$ must be the 0 polynomial in $Z_m[x]$. That will be true only if m is one of 2, 3, or 6.

2. Let G be a group and let \sim be a relation on G defined as follows.

$a \sim b$ means that there is an element $g \in G$ such that $gag^{-1} = b$.

- Show that \sim is an equivalence relation on G .
- Describe the equivalence classes of G if G is an abelian group.
- Find the equivalence classes of S_3 .

SOLUTION:

a. We must show that \sim is reflexive, symmetric and transitive.

Reflexive: Let e be the identity of the group G . Then $eae^{-1} = a$ and so $a \sim a$.

Symmetric: If $a \sim b$, then there is $g \in G$ such that $gag^{-1} = b$. Therefore $a = g^{-1}bg$. Now let $h = g^{-1}$ and $a = h b h^{-1}$ and so, $b \sim a$.

Transitive: If $a \sim b$ and $b \sim c$, then there are $g, h \in G$ such that $b = gag^{-1}$ and $c = h b h^{-1}$. Thus $c = h b h^{-1} = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1}$ and so $a \sim c$.

Hence \sim is an equivalence relation.

b. If $a \sim b$, then there is $g \in G$ such that $b = gag^{-1}$. But if G is abelian, then $gag^{-1} = a$ and therefore $a = b$. Hence \sim is just equality and therefore the equivalence classes are the single elements of the group.

c. Given the fact that conjugation preserves cycle structure, it follows that the equivalence classes of \sim for S_3 are:

$$\{(1)\}, \{(12), (13), (23)\}, \{(123), (132)\}$$

3. Let F be a finite field and let 1 be the multiplicative identity of F .

a. Show that there exists a prime p such that $\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0$.

b. Show that for every $a \in F$, $\underbrace{a + a + \dots + a}_{p \text{ times}} = 0$.

SOLUTION:

a. Since F is finite, the prime field of F is finite and so cannot be \mathbb{Q} , the rationals. Therefore, the prime field of F is \mathbb{Z}_p for some prime p . Hence $\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0$.

b. If $a \in F$, then $\underbrace{a + a + \dots + a}_{p \text{ times}} = a \underbrace{(1 + 1 + \dots + 1)}_{p \text{ times}} = a0 = 0$.

4. Let R be a commutative ring. Let $a \in R$ and let the set

$$D_a = \{ar \mid r \in R\}.$$

a. Show that D_a is an ideal of R for each $a \in R$.

b. Show that if the only ideals in R are (0) and R , then R is a field.

SOLUTION:

a.) D_a is an ideal of R if: $0 \in D_a$, $u + v \in D_a$ whenever $u, v \in D_a$ and $uw \in D_a$ whenever $u \in D_a$ and $w \in R$.

Since $a0 = 0, 0 \in D_a$.

Let $u, v \in D_a$. Then $u = ar_1$ and $v = ar_2$ for some $r_1, r_2 \in R$. Then $u + v = ar_1 + ar_2 = a(r_1 + r_2)$ which is in D_a since $r_1 + r_2 \in R$.

Let $u \in D_a$ and $w \in R$. Then there is $r \in R$ such that $uw = arw = a(rw) \in D_a$.

b. If the only ideals of R are (0) and R , then for each $a \in R, a \neq 0$, D_a is an ideal which is different from (0) since $a \in D_a$. Thus $D_a = R$. Hence $1 \in D_a$ and therefore there is an element $r \in R$ such that $1 = ar$ and so r is the inverse of a . Thus every nonzero element of R has an inverse and thus R is a field.