HW 7 Solutions M31F11

(14.1) b) There are 6 abelian groups of size 72.

Proof: Since $72 = 8 \cdot 9 = 2^3 \cdot 3^2$, we know by Corollary 14.4 that there are $p(3)p(2) = 3 \cdot 2 = 6$ abelian groups of size 72.

(The three partitions of 3 are $1+1+1$, $1+2$, 3; the partitions of 2 are $1+1$, 2.)

They are given by:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$$

$$\mathbb{Z}_8 \times \mathbb{Z}_9$$

(14.7 c) There are 2 abelian groups of size 84, up to isomorphism.

Proof Observe that $84 = 7 \cdot 12 = 7 \cdot 3 \cdot 2^2$, so there are $p(1)p(2)p(1) = p(2) = 2$ abelian groups of size 84. They are given by:

$$\mathbb{Z}_7 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \quad \text{and} \quad \mathbb{Z}_7 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 .$$

HW 7 Solutions M31 F11

Section 14

(7) To find the number of abelian groups of order 108 with exactly 1 subgroup of order 3, we start by using the FTFAG to find all abelian groups of order 108.

Since $108 = 4 \cdot 27 = 2^2 3^3$, ~~the possible~~ any abelian groups of order 108 will be isomorphic to one of the following:

$$\mathbb{Z}_4 \times \mathbb{Z}_{27}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$$
$$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

Now, we observe that each subgroup of order 3 will have exactly 2 elements of order 3, so to find the number of subgroups of order 3 in each of these direct products, we can calculate the number of elements of order 3 and divide by 2.

§14

(2) cont'd

Theorem 6.1 tells us that the order of an element $g=(g_1, g_2, \dots, g_n)$ in a direct product is given by

$$o(g) = \operatorname{lcm}(o(g_1), o(g_2), \dots o(g_n)),$$

and Corollary 10.4 tells us that the order of an element must divide the size of the group. Therefore, if g is an element of order 3, in one of the direct products listed above, the entries from the 2-groups must be 0, because no other element will have an order dividing 3.

Group	Elements of order 3
$\mathbb{Z}_4 \times \mathbb{Z}_{27}$	(0, 9) (0, 18)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$	(0,0,9) (0,0,18)
$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9$	(0,1,0) (0,2,0) (0,1,3) (0,2,3) (0,1,6) (0,2,6) (0,0,3) (0,0,6)
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$	(0,0,1,0) (0,0,2,0) (0,0,1,3) (0,0,2,3) (0,0,1,6) (0,0,2,6) (0,0,0,3) (0,0,0,6)
$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	(0,1,0,0) (0,2,0,0) (0,1,0,1) (0,2,0,1) (0,1,1,0) (0,2,1,0) (0,1,1,1) (0,2,1,1) (0,1,0,2) (0,2,0,2) (0,2,2,0) (0,2,2,2) (0,1,2,0) (0,1,2,2) (0,1,1,2) (0,1,2,1) (0,2,1,2) (0,2,2,1) (0,0,1,0) (0,0,2,0) and others

8.14
2 cont'd

Thus, we see that there are exactly 2 groups of order 108 with 2 elements (and hence one subgroup) of order 3: $\mathbb{Z}_4 \times \mathbb{Z}_{27}$ & $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$.

An alternate argument would be to observe that in a direct product $G \times H$, if $A \leq G$, then $A \times \{0\} \leq G \times H$. Moreover, Any cyclic 3-group ~~abelian~~ has a unique subgroup of order 3 by Theorem 5.5. Hence, the groups isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ will all have at least two subgroups of order 3, since they all have at least two factors ($\mathbb{Z}_3$ and/or $\mathbb{Z}_9$) with subgroups of size 3.

§14

3 The same argument as in Exercise 2 tells us that there are exactly 2 abelian groups of order 108 that have exactly 4 subgroups of order 3:

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9$$

because these groups have exactly 8 elements of order 3.

The other groups have too few elements of order 3 ($\mathbb{Z}_4 \times \mathbb{Z}_{27}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$) or too many ($\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$)

Alternatively, one could observe that since there are 2 elements of order 3 and one element of order 1 in any cyclic 3-group, an abelian group with k factors ~~groups~~ of 3-power order in its FTFAG decomposition will have $3^k - 1$ elements of order 3. (any combination of elements of order 3 and elements of order 1 will work, save for the one consisting solely of elements of order 1.)

Thus, it is precisely the groups with 2 factors of 3-power order that will have $4 = \frac{3^2-1}{2}$ gps of order 3.

HW 7 Solutions M31 F11

On $\mathbb{Q}$, define $a * b = a+b-1$; $a \square b = a+b-ab$

(i–4) Claim $(\mathbb{Q}, *, \square)$ is a field.

Proof We start by checking that $(\mathbb{Q}, *, \square)$ is a ring: that is, that (1) $*$ & $\square$ are associative binary operations, that (2) $(\mathbb{Q}, *)$ is an abelian group, and that (3) $*$ & $\square$ satisfy the distributive laws.

(1) Since addition & multiplication & subtraction are all binary operations on $\mathbb{Q}$, it follows that both $*$ & $\square$ take elements of $\mathbb{Q}$ to elements of $\mathbb{Q}$ - hence, they are binary.

Next we check associativity:

$$\begin{aligned}(a*b)*c &= (a+b-1)*c = (a+b-1+c-1)\\ &= a+(b+c-1)-1\\ &= a*(b*c)\end{aligned}$$

Thus $*$ is associative.

To see that $\square$ is associative, observe that

$$\begin{aligned}a\square(b\square c) &= a\square(b+c-bc) = a+(b+c-bc)\\ &\qquad -a(b+c-bc)\\ &= (a+b-ab)+c-bc-ac+abc\\ &= (a+b-ab)+c-(a+b-ab)c\\ &= (a\square b)\square c.\end{aligned}$$

Therefore $\square$ is associative.

(16.4) cont'd

Next we need to check that $(\mathbb{Q}, *)$ is an abelian group.

1) Identity element: 1

Note that $a*1 = a+1-1 = a$ for any $a \in \mathbb{Q}$

2) For any $a \in \mathbb{Q}$, $-a_*$ (the inverse of a under $*$) is given by $2-a$:

$a*(2-a) = a+2-a-1 = 1$

Thus $(\mathbb{Q}, *)$ has an identity and inverses, so it's a group. This group is abelian because addition is commutative:

$$a*b = a+b-1 = b+a-1 = b*a.$$

To see that $(\mathbb{Q}, *, \square)$ is a ring, we need to check the distributive laws. However, since $\square$ is commutative $\left(a \square b = a+b-ab = b+a-ba = b \square a\right)$ we only need check the left distributive law:

$$a \square (b*c) \stackrel{?}{=} (a \square b) * (a \square c)$$

Observe that

$$\begin{aligned} a \square (b*c) = a \square (b+c-1) &= a+(b+c-1) - a(b+c-1) \\ &= a+b-ab+ac-1-ac+a \\ &= (a \square b) + (a \square c) - 1 \\ &= (a \square b) * (a \square c). \end{aligned}$$

Thus, since the distributive laws hold, $(\mathbb{Q}, *, \square)$ is a (commutative) ring.

To see that it is a field, we must check that $(\mathbb{Q}, *, \square)$ has a unity and that every element save 1 (the identity for $*$; the "additive identity" or "zero element") has an inverse for $\square$.

Observe that 0 is the unity for $(\mathbb{Q}, *, \square)$:

$$a \square 0 = a + 0 - a \cdot 0 = a$$

for any $a \in \mathbb{Q}$.

Furthermore, if $a \neq 1$, then $\frac{a}{a-1} \in \mathbb{Q}$, and

$$a \square \left(\frac{a}{a-1}\right) = a + \frac{a}{a-1} - \frac{a^2}{a-1} = \frac{a^2 - a + a - a^2}{a-1}$$

$$= \frac{0}{a-1} = 0,$$

and so $\left(\frac{a}{a-1}\right)$ is the inverse for a under $\square$.

Since every element save 1 has a "multiplicative" inverse, we see that $(\mathbb{Q}, *, \square)$ is a field as claimed. $\boxtimes$

HW 7 Solutions M31 F11

(6.9) a) If $a \in (\mathbb{Z}_n, \oplus, \odot)$, then a is a unit iff $(a,n)=1$.

Proof Suppose $(a,n)=1$. Then we can use the Euclidean Algorithm (Theorem 4.2) to find integers b, m such that

$$ab + mn = 1.$$

Therefore, $a \cdot b \equiv 1 \pmod n$. Note that b need not be in $\mathbb{Z}_n$, but we can use the Division Algorithm to write

$$b = qn + b'$$

for some $0 \le b' < n$, so $b' \in \mathbb{Z}_n$. Moreover,

$$a \cdot b = a(qn + b') \equiv ab' \pmod n$$

and so $ab' \equiv 1 \pmod n$ as well.

Therefore, b' is a multiplicative inverse for a, & hence a is a unit.

(..9) a) Cont'd

To see the other implication, suppose that a is a unit. Then, there exists b such that $ab \equiv 1 \pmod{n}$; in other words, $ab = 1 + n\ell$ for some $\ell \in \mathbb{Z}$.

Let $d = (a,n)$. Then d divides $(ab - n\ell)$, and therefore d must divide 1 - but this tells us that $d = 1$, since the gcd of two integers is always positive.

Therefore, if a is a unit then $(a,n) = 1$, and we have proved both implications of the iff. statement.

b) Claim If $b \in \mathbb{Z}_n$ is not a unit, then b is a zero divisor.

Proof Notice that proving this Claim will tell us that every element of $\mathbb{Z}_n$ is either a unit or a zero divisor.

We know by part (a) that the units in $\mathbb{Z}_n$ are precisely the elements a with $(a,n) = 1$. Thus, suppose $(b,n) > 1$ for some $b \in \mathbb{Z}_n$.

We will show that b is a zero divisor in $\mathbb{Z}_n$.

Let $d=(b,n)$; then $\frac{n}{d}\in\mathbb{Z}_n$ is an integer, and is strictly smaller than n because $d>1$. Also,

$$b\cdot\frac{n}{d}=\frac{b}{d}\cdot n\equiv 0 \pmod n$$

since $\frac{b}{d}$ is also an integer. We have found an element namely $\frac{n}{d}$ of $\mathbb{Z}_n$ such that $\frac{n}{d}\cdot b\equiv 0$, and hence b is a zero divisor by definition.

Consequently, any non-unit is a zero divisor in $\mathbb{Z}_n$.

c) Write $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, where p_i is a prime for $1\le i\le k$. The nilpotent elements of $\mathbb{Z}_n$ are precisely the integers of the form

$$d=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}q_1^{g_1}q_2^{g_2}\cdots q_\ell^{g_\ell},$$

where the q_i are primes, & where $1\le f_i\le e_i$ for all i between 1 & k.

In words, each prime factor of n also divides d.

Proof If $d\in\mathbb{Z}_n$ has the form indicated above, then let $e=\max\{e_1,e_2,\dots,e_k\}$.

Observe that $d^e\equiv 0 \pmod n$; (cont'd)

16.9 c) cont'd

we know that d^e is divisible by $(p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k})^e = (p_1^e)^{f_1}(p_2^e)^{f_2} \cdots (p_k^e)^{f_k}$

$$= (p_1^{e_1+s_1})^{f_1}(p_2^{e_2+s_2})^{f_2} \cdots (p_k^{e_k+s_k})^{f_k}$$

$$= (p_1^{e_1})^{f_1}(p_2^{e_2})^{f_2} \cdots (p_k^{e_k})^{f_k}(p_1^{s_1})^{f_1} \cdots (p_k^{s_k})^{f_k}$$

Where $s_i = e - e_i$ for each i (so $0 \le s_i < e$).

Since $1 \le f_i \le e_i$ for all i, we know $f_i - 1 \ge 0$, and therefore $(p_i^{e_i})^{f_i-1}$ is an integer (possibly 1) for each i. Consequently, d^e is divisible by

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} (p_1^{e_1})^{f_1-1}(p_2^{e_2})^{f_2-1} \cdots (p_k^{e_k})^{f_k-1}(p_1^{s_1})^{f_1} \cdots (p_k^{s_k})^{f_k}$$

$$= n \cdot (p_1^{e_1})^{f_1-1} \cdots (p_k^{e_k})^{f_k-1}(p_1^{s_1})^{f_1} \cdots (p_k^{s_k})^{f_k},$$

and therefore

$$d^e \equiv 0 \pmod{n}.$$

Therefore, if d is an element of $\mathbb{Z}_n$, such that any prime factor of n also divides d, we know d^e is nilpotent. However, if p_i is a prime factor of n that does not divide d, then no power of d will have a factor of p_i, and so n will not divide d^e for any $e \in \mathbb{Z}^+$. Therefore, d is not a zero divisor

(cont'd)

(16.9) c) cont'd

unless d has the form specified above, so the nilpotent elements of $\mathbb{Z}_n$ are precisely the elements which are divisible by all the prime factors of n. ⊠

Rubric for 16.9 [5 pts]

(a) $(a,n)=1 \Rightarrow a$ a unit - 1pt (*)

a a unit $\Rightarrow (a,n)=1$ - 1 pt

(b) $(b,n)>1 \Rightarrow$ b a zero divisor - 1pt

(c) Correct assertion - 1pt

Proof - 1pt

Feel free to take off 1-2 pts if the writing isn't clear.

(*) If students say that $(a,n)=1 \Rightarrow a^{\phi(n)} \equiv 1$ because $a \in U(n)$, no point! They should prove that $(a,n)=1$ is a characterization of the units of $\mathbb{Z}_n$ (this was stated but not proved in class)

HW 7 Solutions M31 F11

Section 16

(?) Let $R = \left\{ \begin{bmatrix} a & a+b \\ a+b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\} \subseteq M_2(\mathbb{Z})$.

Then R is a subring of $M_2(\mathbb{Z})$.

Proof We must show that $(R,+)$ is a subgroup of $(M_2(\mathbb{Z}),+)$, and that R is closed under matrix multiplication.

To see that $(R,+)$ is a subgroup, we check that it's closed under addition & under (additive) inverses: Suppose $\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix}$ & $\begin{pmatrix} c & c+d \\ c+d & c \end{pmatrix} \in R$.

Then their sum is $\begin{pmatrix} a+c & a+b+c+d \\ a+b+c+d & a+c \end{pmatrix} = \begin{pmatrix} a+c & (a+c)+(b+d) \\ (a+c)+(b+d) & a+c \end{pmatrix}$,

and since all entries will be integers, it follows that $\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix} + \begin{pmatrix} c & c+d \\ c+d & c \end{pmatrix} \in R$. Moreover, the additive inverse of $\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix}$ is $\begin{pmatrix} -a & -a-b \\ -a-b & -a \end{pmatrix}$,

which is also in R because $-a, -b \in \mathbb{Z}$ if $a, b \in \mathbb{Z}$.

Thus $(R,+) \leq (M_2(\mathbb{Z},+)$.

To see that R is closed under matrix multiplication, consider the product

$$\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix}\begin{pmatrix} c & c+d \\ c+d & c \end{pmatrix} = \begin{pmatrix} ac+(a+b)(c+d) & a(c+d)+c(b+a) \\ (a+b)c+a(c+d) & (a+b)(c+d)+ac \end{pmatrix}$$

Section 16 **HW 7 Solutions** M31F11

(2) con't Observe that

$$ac + (a+b)(c+d) = a(c+d) + c(a+b) + (bd),$$

and so

$$\begin{pmatrix} a & a+b \\ a+b & a \end{pmatrix}\begin{pmatrix} c & c+d \\ c+d & c \end{pmatrix} = \begin{pmatrix} e & e+f \\ e+f & e \end{pmatrix} \in R,$$

where $e = ac + (a+b)(c+d)$ and $f = -bd$ are both integers.

Therefore, R is closed under multiplication and hence is a subring of $M_2(\mathbb{Z})$. ⊠

Rubric [5 pts]

- Correct assertion
- State what they have to show
- Show $(R, +) \leq (M_2(\mathbb{Z}, +)$
- Show R closed under multiplication
- Writing

One point each

HW 7 Solutions M31F11

Presentations

(1) To show that $H = \langle F \rangle$ is not normal in $G = \langle F, B, L, R, U, D \rangle$, it suffices to show that $L\langle F \rangle \neq \langle F \rangle L$. This argument will work for any choice of $H = \langle s \rangle$ for $s \in \{F, B, L, R, U, D\}$ and any coset $a\langle s \rangle$ where a is not directly opposite s. (That is, you can take L, R, U, D for $H = \langle F \rangle$; anything but L for $H = \langle R \rangle$; and anything but D for $H = \langle U \rangle$.)

Observe that $L\langle F \rangle = \{LF, LF^2, LF^3, LF^4 = L\}$, since each rotation has order 4. Moreover, in cycle notation,

Students may permute the letters in these labelings; that's ok. df = fd.

$$F = (lfu\ ufr\ dfr\ dfl)(lf\ uf\ rf\ df)(f)$$

and $L = (blu\ ulf\ fld\ dlb)(lb\ lu\ lf\ ld)(l)$

Then $LF = (blu\ ufr\ dfr\ dfl\ dlb)(ulf)$

$(lb\ lu\ uf\ rf\ df\ lf\ ld)(f)(l)$

Similarly, $FL = (lfu\ ufr\ dfr\ dlb\ ulb)(dfl)$

$(lf\ uf\ rf\ df\ ld\ lb\ lu)(f)(l)$

resentations

① cont'd

Since $F^2 = (lfu\ dfr)(ufr\ dfl)(lf\ rf)$
$(uf\ df)\ (f)$,

we have

$$LF^2 = (blu\ dfr\ ulf\ urf\ dlf\ dlb)$$
$$(lb\ lu\ rf\ lf\ ld)\ (uf\ df)\ (f)(l)$$

and

$$F^3 = F^{-1} = (lfu\ dfl\ dfr\ ufr)(lf\ df\ rf\ uf)$$

so

$$LF^3 = (blu\ dfl\ dlb)(lfu\ dfr\ ufr)$$
$$(lb\ lu\ df\ rf\ uf\ lf\ ld)\ (f)(l)$$

Since $FL \notin L\langle F\rangle = \{L, LF, LF^2, LF^3\}$

we cannot have $\langle F\rangle L = L\langle F\rangle$, so the left & right cosets of $\langle F\rangle$ by L differ, and so $\langle F\rangle$ is not normal in G. ☒

M31 F11

Homework 7 Solutions

Presentations

2) a) If $p = 23$, $q = 41$, $e = 7$, then the public key is $(p \cdot q, e)$ or $(943, 7)$.

b) To encode 432, Bond calculates $(432)^7 \bmod 943$:

Since $432^7 = 432 \cdot 432^2 \cdot 432^4$, we calculate

$432^2 \pmod{943} \equiv 853$

$853^2 \equiv 556 \pmod{943}$

$432 \cdot 853 \cdot 556 \equiv 52 \pmod{943}$

So, M would receive the message 52

c) To decrypt the message, M would want to use the multiplicative inverse of $e \pmod{22 \cdot 40}$, that is, the inverse of $7 \pmod{880}$.

Trial and error (and Google Calculator) gives that $7^{20} \equiv 1 \pmod{880}$, so our value of f is $7^{19} \pmod{880} = 503$.

Presentations | Homework 7 Solutions M31F11

(2) cont'd

To confirm that we have the correct answer for the decoding key, we calculate:

$$52^{503} \pmod{943} \equiv 432,$$

the original coordinates, as desired.

Rubric [5 pts]

1 - Public key (include both n & e)

1 - Correct encoding procedure ($432^7 \bmod 943$)

1 - Correct encoded message

1 - Correct procedure for finding f (mult. inverse of e. mod 880)

1- Check that f correctly decodes message

Writing - Deduct a point if writing isn't clear.