Name Min Chun Wu

Math 536 Spring 2016

EXAM 1

Problem	Possible Points	Actual Points
1	10	10
2	10	10
3	10	10
4	10	10
Total	40	40

You may use results proved in class or on the homework, but you should indicate clearly what you are using.

No notes or books allowed. All cell phones and music players must be put away.

1. (10 points) Up to isomorphism, list the non-cyclic abelian groups which could lie inside a group of order 100.

(Here, we use ① Fundamental thm. of f.g. abelian gps and ② if $(p,q)=1$, then $\mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$)

$100 = 2^2 \times 5^2$.

By Lagrange theorem, the orders of subgps could be

$1, 2, 4, 5, 10, 20, 25, 50, 100$.

Gps of order $1, 2, 5$ must be cyclic.

You also need that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is not cyclic (follows from uniqueness part of structure theorem)

For 4, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the only non-cyclic abelian one. (V)

For 10, $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$ would both be cyclic, not our candidate

For $20 = 2^2 \times 5$, $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{20}$ is cyclic.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$ is non-cyclic. (V)

For 25, $\mathbb{Z}_{25}$ is cyclic while $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ is not. (V)

For $50 = 2 \times 5^2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{50}$ is cyclic

$\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ is non-cyclic. (V)

For $100 = 2^2 \times 5^2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$: non-cyclic (V)

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: non-cyclic (V)

$\mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$: non cyclic (V)

$\mathbb{Z}_4 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{100}$: cyclic.

explain why these are non-isomorphic

In summary, the non-cyclic abelian subgps would possibly be

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$, $\mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$,

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$. #

$$\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix} \underbrace{\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}}_{\begin{pmatrix} a & b+dc \\ 0 & c \end{pmatrix}}$$

$$= (\cdot\cdot)^{-1}\left((\cdot\cdot) + \begin{pmatrix} 0 & dc \\ 0 & 0 \end{pmatrix}\right) = \left(I + \begin{pmatrix} 0 & dc/a \\ 0 & 0 \end{pmatrix}\right)$$

2. (10 points) Let $G = \mathrm{GL}_2(k)$, the group of invertible 2×2 matrices with coefficients in the field k. Let B be the subgroup of upper triangular matrices in G, and let U be the subgroup of upper triangular matrices all of whose diagonal entries are equal to 1. Let T be the subgroup of diagonal matrices in G. Thus,

$$B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \quad U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}, \quad T = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}.$$

(a) (7 points) Show that B is a semidirect product of U by T, $B = U \rtimes T$.

$$\left(\begin{array}{cc:cc} a & b & 1 & 0 \\ 0 & c & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc:cc} a & 0 & 1 & -b/c \\ 0 & c & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc:cc} 1 & 0 & 1/a & -b/ac \\ 0 & 1 & 0 & 1/c \end{array}\right).$$

$\Rightarrow$ The inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ in B is $\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$.

($a \neq 0 \neq c$ since $B \subseteq G$).

Thus, for $\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$ in U, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & dc/a \\ 0 & 1 \end{pmatrix} \in U$.

$\Rightarrow U \trianglelefteq B$. ... ①

$U \cap T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ is clear. ... ②

For $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & b/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in UT$.

$\Rightarrow B = UT$ ... ③

By ①, ②, ③, $B = U \rtimes T$. #

(b) (3 points) Is B the direct product of U and T? Explain.

No. Recall that $U \rtimes T = U \times T$ iff $XY = YX$, $\forall X \in U$, $Y \in T$.

However, $X = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in U$, $Y = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in T$ with

$XY = \begin{pmatrix} 2 & 6 \\ 0 & 3 \end{pmatrix}$ but $YX = \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix}$, not equal. #

3. (10 points) Let A be the abelian group with generators a, b, c satisfying the relations

$$\begin{aligned} 2a + 3b + 5c &= 0 \\ a + 3c &= 0 \\ a + 5c &= 0. \end{aligned}$$

Is A cyclic? If so, find a generator for A and say what its order is. If not, give a smallest generating set and the order of the elements. Explain your work.

$$M = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 0 & 3 \\ 1 & 0 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3 \\ 0 & 3 & -1 \\ 0 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & -2 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

Thus, $\exists$ P, Q invertible over $\mathbb{Z}$ s.t. $PMQ = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 6 \end{pmatrix}$.

$\Rightarrow$ A is generated by a', b', c' subject to

$$\begin{cases} a' = 0 \\ b' = 0 \\ 6c' = 0 \end{cases}$$

$\Rightarrow A \cong (\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}) / (\mathbb{Z} \oplus \mathbb{Z} \oplus 6\mathbb{Z}) \cong \mathbb{Z}_6$.

$\Rightarrow$ A is cyclic, iso. to. $\mathbb{Z}_6$ #.

You were supposed to find a generator for A in terms of the original generators a, b, c

for $x, y \in X$, $\exists g \in G$ s.t. $g(x) = y$.

4. (10 points) Let G be a subgroup of S_n, so there is a natural group action of G on the set $X := \{1, 2, \ldots, n\}$. Suppose that G is abelian and acts transitively on X.

(a) (7 points) Show that each element g of G, $g \neq 1$, moves every element of X.

Let $g \in G$.

Suppose $gx = x$, some $x \in X$. (i.e. some $x \in X$ not moved).

For $y \in X$,

$\because$ G acts transitively $\therefore$ $\exists h \in G$ s.t. $hx = y$

$\Rightarrow gy = ghx = hgx = hx = y$.

$\boxed{G: \text{abelian}}$

Thus, $gy = y$, $\forall y \in X$. $\Rightarrow g = 1$ in G.

Therefore, for $g \neq 1$ in G, g moves every element of X. #

(b) (3 points) Prove that $|G| \leq n$.

By (a), $G_x = \{1\}$, $\forall x \in X$, where G_x = stabilizer of x.

By orbit-stabilizer thm,

$(G : G_x) = |B(x)|$, where $B(x)$ = orbit of x.

$\Rightarrow |G|/1 = |B(x)|$.

$\because B(x) \subseteq X$ $\therefore |B(x)| \leq n$.

Thus, $|G| \leq n$. #

Math 536 **EXAM 1** Spring 2016

1. Up to isomorphism, list the non-cyclic abelian groups which could lie inside a group of order 100.

   Solution: The possible 2-groups contained in a group of order 100 are $\{0\}, C_2, C_2 \times C_2$, and C_4. The possible 5-groups are $\{0\}, C_5, C_5 \times C_5$ and C_{25}. An abelian group H of order dividing $100 = 2^2 \cdot 5^2$ will be cyclic exactly when its 2- and 5-parts are both cyclic. We obtain 4 possibilities with 2-part not cyclic: $C_2 \times C_2, C_2 \times C_2 \times C_5, C_2 \times C_2 \times C_{25}, C_2 \times C_2 \times C_5 \times C_5$ and three further possibilities with 5-part not cyclic: $C_5 \times C_5, C_2 \times C_5 \times C_5$, and $C_4 \times C_5 \times C_5$. By the uniqueness part of the fundamental theorem for finitely generated abelian groups, none of the above groups are isomorphic.

2. Let $G = \mathrm{GL}_2(k)$, the group of invertible 2×2 matrices with coefficients in the field k. Let B be the subgroup of upper triangular matrices in G, and let U be the subgroup of upper triangular matrices all of whose diagonal entries are equal to 1. Let T be the subgroup of diagonal matrices in G.

   Show that B is a semidirect product of U by T, $B = U \rtimes T$.

   Is B the direct product of U and T?

   Solution:

   The inverse of the matrix $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$ is the matrix $A^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix}$. Note that since $A \in G$, both a and c must be nonzero. We have to check that that U is normal in B, that $UT = B$, and that $U \cap T = \{1\}$.

   Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$, let $C = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \in U$. Then $ACA^{-1} = \begin{pmatrix} 1 & ad/c \\ 0 & 1 \end{pmatrix} \in U$, which shows that U is normal.

   It is clear that U and T intersect trivially. Also, given $A = \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} \in B$, we have $A = CD$ with $C = \begin{pmatrix} 1 & b/c \\ 0 & 1 \end{pmatrix} \in U$ and $D = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in T$, which shows $B = UT$. This proves that $B = U \rtimes T$.

   The group B is not the direct product of U and T since T is not normal in B. To see this we can check that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \notin T$.

3. (10 points) Let A be the abelian group with generators a, b, c satisfying the relations

$$
\begin{aligned}
2a + 3b + 5c &= 0 \\
a + 3c &= 0 \\
a + 5c &= 0.
\end{aligned}
$$

   Is A cyclic? If so, find a generator for A and say what its order is. If not, give a smallest generating set and the order of the elements.

Name Min Chan Wu

Math 536 Spring 2016

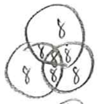
EXAM 2

Problem	Possible Points	Actual Points
1	10	7
2	10	8
3	10	10
4	10	10
Total	40	35

You may use results proved in class or on the homework unless indicated otherwise. Please state clearly what results you are using.

No notes or books allowed. All cell phones and music players must be put away.

24
8
24 24
80



56

$X = \{A\ B\ C\}$

G acts on X by conj.

1, 2, 4, 8.

$G \to S_3$

$\shortparallel$

6

$|G/\ker| \leq 6$

$96/\ker$

G acts on cosets.

1, 4, 7, 10, 13, 16, 19,
22, 25, 28, 31.

$n_3 \equiv 1 \mod 3$

1. (10 points) Show that a group G of order 96 must have a normal subgroup of order 16 or 32.

$96 = 2^5 \times 3$.

$n_2 :=$ the number of Sylow 2-subgps of G.

By Sylow thm, $n_2 \equiv 1 \mod 2$ and $n_2 \mid 3$.

$\Rightarrow n_2 = 1$ or 3.

case 1 $n_2 = 1$.

Then we only have one Sylow 2-subgps, which is of order 32.

By Sylow thm, all Sylow 2-subgps are conjugates.

$\Rightarrow$ This unique Sylow 2-subgp is normal.

case 2 $n_2 = 3$.

Let $X = \{$all Sylow 2-subgps$\}$. (Hence, $|X| = 3$).

Let G act on X by conjugation.

This induces a gp hom. $G \overset{\Phi}{\Rightarrow} S_X \cong S_3$.

By iso. thm, ~~_~~ $G/\ker(\Phi) \cong \operatorname{im}(\Phi)$.

$\Rightarrow |G/\ker(\Phi)| \leq 6. \Rightarrow |\ker\Phi| \geq |G|/6 = 16$.

Note, $\ker(\Phi) \subseteq$ intersect'n of all ~~2-gp~~ Sylow 2-gps.

(Recall the prop. that the gp normalizing p-gps must be contained in the p-gp).

~~Then~~ Q Thus, according to this, their ~~ord~~

finish this case

2. (10 points) Find the GCD of $x^3 + x^2 - x + 1$ and $x^4 - x^2 + x + 1$ in $\mathbb{Q}[x]$. Justify your answer.

$\because$ $\mathbb{Q}[x]$ is an ED $\therefore$ We can use Euclid's algorithm to find gcd.

1 1 -1 1	1 0 -1 1 1
1 0 0 -1	1 1 -1 1
1 -1 2	-1 0 0 1
+1 -2 -1	-1 +1 -2
1 3	-1 2 1
1	-1 -3
3	5 1
3	5 15
0	-14
	1

?? Explain your work.
$\therefore$ I don't understand what your computation does.

Thus, they are relatively prime and their GCD is 1. #

8

3. (10 points) Let $R := \mathbb{Q}[x]/(x^3 - 3x - 2)$.

10

(a) (4 points) Find the maximal ideals in R.

$$\begin{array}{cccc|c} 1 & 0 & -3 & -2 & \\ & -1 & 1 & 2 & -1 \\ \hline 1 & -1 & -2 & ,0 & \end{array}$$

$x^3-3x-2 = (x+1)(x^2-x-2)$

$= (x+1)(x-2)(x+1) = (x+1)^2(x-2).$

By correspondence thm, max. ideals of R would correspond to max. ideals of $\mathbb{Q}[x]$ containing (x^3-3x-2).

$\because \mathbb{Q}[x]$: PID $\therefore$ max. ideals are generated by irr. poly.

Moreover, ideals containing (x^3-3x-2) would be generated by a poly. g w/ $g \mid x^3-3x-2$.

Thus, the max. ideals of R are $(x+1)/(x^3-3x-2)$ and $(x-2)/(x^3-3x-2)$.

#

(b) (4 points) Let $\overline{x}$ denote the image of x under the canonical ring mapping $\mathbb{Q}[x] \to R$. Is $\overline{x} + 2$ a unit in R? If so, give its inverse. If not, prove why not.

Yes. Reason: $x+2$ and x^3-3x-2 are rel. prime (which can be seen by the decomp. of x^3-3x-2).

$$\begin{array}{cccc|cc} 3 & 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & -3 & -2 & 1 & 2 \\ 1 & 2 & & & & \\ \hline & -2 & -3 & -2 & & \\ & -2 & -4 & & & \\ \hline & & 1 & -2 & & \\ & & 1 & 2 & & \\ \hline & & & -4 & & \end{array}$$

$f(x) := x^3-3x-2$

$g(x) := x+2.$

$f(x) = g(x)(x^2-2x+1) - 4.$

Thus,

$$1 = \frac{x^2-2x+1}{4} g(x) + \frac{-1}{4} f(x).$$

Let $y = \dfrac{\overline{x}^2 - 2\overline{x} + 1}{4}$.

Then $y \cdot (\overline{x}+2) = y \cdot g(\overline{x})$

$= y \cdot g(\overline{x}) + \frac{-1}{4} f(\overline{x}) = 1$ in R.

i.e. y is its inverse. #

(c) (2 points) Is $\overline{x} - 2$ is a zero-divisor in R? If so, find a nonzero element $y \in R$ with $(\overline{x} - 2)y = 0$ in R. If not, prove why not.

Yes.

Consider $(\overline{x}+1)^2 \in R$. $\because \deg (x+1)^2 = 2 < 3 = \deg (x^3-3x-2)$

$\therefore (\overline{x}+1)^2 \neq 0$ in R.

However, $(\overline{x}+1)^2(\overline{x}-2) = \overline{x}^3 - 3\overline{x} - 2 = 0$ in R.

Taking $y = (\overline{x}+1)^2$, we are done. #

4. (10 points)

(a) Prove or disprove: If I is a nonzero prime ideal in $\mathbb{Q}[X]$, then $\mathbb{Q}[X]/I$ is a unique factorization domain.

Yes, this statement is true.

$\because$ $\mathbb{Q}[X]$: PID $\therefore$ nonzero prime ideals are max. ideals.

$\Rightarrow$ $\mathbb{Q}[X]/I$: field. $\Rightarrow$ $\mathbb{Q}[X]/I$: UFD. #

(b) Prove or disprove: If I is a nonzero prime ideal in $\mathbb{Z}[X]$, then $\mathbb{Z}[X]/I$ is a unique factorization domain.

No.

In H.W., we proved that $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD.

Consider $I = \langle X^2+5 \rangle$, which is prime since X^2+5 : prime.

Note the ring hom.

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{-5}]$$
$$X \longmapsto \sqrt{-5}$$

has kernel I.

Thus, by iso. thm, $\mathbb{Z}[X]/I \cong \mathbb{Z}[\sqrt{-5}]$, not a UFD. #

$x^2+1 \quad x+1.$

$2x+1.$

$\mathbb{Z}[\sqrt{-5}]$

$2+2\sqrt{-5} = X.$

6

$(x-2)^2 = -20.$

$x^2-4x+24=0.$

$\mathbb{Z}[x]/\langle x^2+5 \rangle$

$\to \mathbb{Z}[\sqrt{-5}].$

Math 536 Spring 2016

Solution Sketches for Exam 2

1. Show that a group G of order 96 must have a normal subgroup of order 16 or 32.

   Solution: Let n_2 denote the number of 2-Sylow subgroups. Then $n_2 \equiv 1 \bmod 2$, i.e. is odd, and $n_2 \mid 96$. Therefore $n_2 = 1$ or 3. If $n_2 = 1$, then there is a unique 2- Sylow subgroup. This is the normal subgroup of order 32. If $n_2 = 3$, then by the Sylow theorem, conjugation gives a homomorphism of G into S_3. In S_3 the only elements of order 2 are transpositions. But the image of G is transitive on the 2-Sylow subgroups since the 2-Sylow subgroups are conjugate. So the image of G cannot have order 2. Thus the image of G in S_3 has order either 3 or 6, and the kernel has corresponding order 32 or 16. Of course the kernel of a homomorphism is normal.

2. Find the GCD of $x^3 + x^2 - x + 1$ and $x^4 - x^2 + x + 1$ in $\mathbb{Q}[x]$.

   Solution: We apply the Euclidean algorithm: $x^4 - x^2 + x + 1 = (x^3 + x^2 - x + 1) \cdot (x - 1) + (x^2 - x + 2)$. Then $(x^3 + x^2 - x + 1) = (x^2 - x + 2)(x + 2) + (-x - 3)$. We have $(x^2 - x + 2) = (-x - 3)(-x + 4) + 14$. Since 14 is a unit in $\mathbb{Q}[x]$, 14 divides $-x - 3$, and the GCD is the class of 1 (= the class of all units) in $\mathbb{Q}[x]$.

3. Let $R := \mathbb{Q}[x]/(x^3 - 3x - 2)$. (a) Find the maximal ideals in R.

   Solution: The ideals of the quotient correspond uniquely to the ideals of $\mathbb{Q}[x]$ (a PID) containing $x^3 - 3x - 2$, i.e to the monic divisors of $x^3 - 3x - 2 = (x + 1)^2(x - 2)$. The maximal ideals correspond to the minimal degree divisors (which are irreducible), i.e. to $x + 1$ and $x - 2$.

   (b) Let $\overline{x}$ denote the image of x under the canonical ring mapping $\mathbb{Q}[x] \to R$. Is $\overline{x} + 2$ a unit in R? If so, give its inverse. If not, prove why not.

   Solution: Since $x^3 - 3x - 2 = (x + 2)(x^2 - 2x + 1) - 4$, and $\overline{x}$ is a root of $x^3 - 3x - 2$, $(\overline{x} + 2)(\overline{x}^2 - 2\overline{x} + 1) = 4$. So $(\overline{x} + 2)[(\overline{x}^2 - 2\overline{x} + 1)/4] = 1$ and $\overline{x} + 2$ is a unit.

   (c) Prove that $\overline{x} - 2$ is a zero divisor in R. **Solution:** Clearly from the factorization in (a), $(\overline{x} - 2)[(\overline{x} + 1)^2] = 0$, so $\overline{x} - 2$ is a zero divisor.

4. (a) Prove or disprove: If I is a nonzero prime ideal in $\mathbb{Q}[X]$, then $\mathbb{Q}[X]/I$ is a UFD.

   True. $\mathbb{Q}[X]$ is a PID, so any nonzero prime ideal is maximal. Thus $\mathbb{Q}[X]/I$ is a field and hence a UFD.

   (b) Prove or disprove: If I is a nonzero prime ideal in $\mathbb{Z}[X]$, then $\mathbb{Z}[X]/I$ is a UFD.

   This is false. Let $I = X^2 + 5$. Then I is a prime ideal since $X^2 + 5$ is irreducible in $\mathbb{Z}[X]$. But the quotient is isomorphic to $\mathbb{Z}[\sqrt{-5}]$, which is not a UFD as we saw in class.