MAT313 Fall 2017
Practice Midterm I

Problem 1. Explain which of the following subsets $R \subset X \times X$ define equivalence relation

(1) $X = \mathbb{R}$ and $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = x^2\}$.
(2) $X = \mathbb{Z}$ and $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x = 0 \text{ or } y = 0 \text{ or } x = y\}$.
(3) $X = \mathbb{C}$ and $R = \{(x, y) \in \mathbb{C} \times \mathbb{C} | x^2 = y^2\}$.

Solution. (1) R in 1 is not an equivalence relation because $(2, 4) \in R$ but $(4, 2) \notin R$.
(2) R in 2 is not an equivalence relation because $(2, 0) \in R$ and $(0, 3) \in R$ doesn't imply $(2, 3) \in R$
(3) R in 3 is an equivalence relation because it is induced by the map $f(z) = z^2$ $f : \mathbb{C} \to \mathbb{C}$.

□

Problem 2. Find $\gcd(1025, 2300)$ and $\gcd(1257, 2301)$

Solution. Use the obvious property $\gcd(a, b) = \gcd(b, a) = \gcd(a, b + ka)$. This way $\gcd(1025, 2300) = \gcd(1025, 2300 - 2 * 1025) = \gcd(1025, 250) = \gcd(1025 - 4 * 250, 250) = \gcd(25, 250) = 25$.

Similarly $\gcd(1257, 2301) = 3$. □

Problem 3. Find all integral solutions (x, y) of the equation

(1) $10x + 13y = 1$.
(2) $11x + 19y = 1$

Solution. (1) If (x_0, y_0) and (x_1, y_1) are two solutions then $(w, u) = (x_0 - x_1, y_0 - y_1)$ is a solution of $10w + 13u = 0$. if (w, u) is a solution then (kw, ku) is also a solution. We see that all (w, u) must be proportional to (w_0, u_0) with $gcd(w_0, u_0) = 1$. We choose $(-13, 10)$ for (w_0, u_0). It remains to find a particular (x_0, y_0). Note $10x_0 + 13y_0 = 1 \Rightarrow 10(x_0 + y_0) + 3y_0 = 1 \Rightarrow 1(x_0 + y_0) + 3(y_0 + 3(x_0 + y_0)) = 1$. Solve under assumption $x_0 + y_0 = 1$ $y_0 + 3(x_0 + y_0) = 0 \Rightarrow y_0 = -3$ and $x_0 = 4$.

Finally the full set of solutions is $\{4-13k, -3+10k | k \in \mathbb{Z}\}$

(2) $11x_0 + 19y_0 = 1 \Rightarrow 11(x_0+y_0) + 8y_0 = 1 \Rightarrow 3(x_0+y_0) + 8(y_0+(x_0+y_0)) = 1 \Rightarrow 3((x_0+y_0)+2(y_0+(x_0+y_0))) + 2(y_0+(x_0+y_0)) = 1 \Rightarrow 1((x_0+y_0)+2(y_0+(x_0+y_0))) + 2(y_0+(x_0+y_0)+((x_0+y_0)+2(y_0+(x_0+y_0)))) = 1$

Make assumptions $((x_0+y_0)+2(y_0+(x_0+y_0))) = 1$ and $(y_0+(x_0+y_0)+((x_0+y_0)+2(y_0+(x_0+y_0)))) = 0 \Rightarrow y_0+(x_0+y_0) = -1 \Rightarrow x_0+y_0 = 3 \Rightarrow y_0 = -4 \Rightarrow x_0 = 7$
The set of solutions is $\{(-19k+7, 11k-4) | k \in \mathbb{Z}\}$

□

Problem 4. Give an example of a non commutative group that contains a subgroup of prime order.

Solution. $H = \{\left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right)\} \subset \mathrm{SL}(2, \mathbb{Z}_p)$. Its contains a subgroup $K = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\}$ of order p. □

Problem 5. Describe all the subgroups in $\mathbb{Z}_{18}$ and their generators.

Solution. Fact: Subgroups of a cyclic group G are $1:1$ with divisors of $|G|$. In our case $|G| = 18 = 2 \cdot 3^2$. This means that we have the following subgroups $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_6, \mathbb{Z}_9$.

Fact: If $a \in G$ is an element of order n, then a^k has order $\frac{n}{(n,k)}$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$(18,k)$	1	2	3	2	1	6	1	2	9	2	1	6	1	2	3	2	1
order $= \frac{18}{(18,k)}$	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18

The generator of $\mathbb{Z}_2$ is 9 . $\mathbb{Z}_3$ is generated by either element of the set $\{6, 12\}$. $\mathbb{Z}_6$ is generated by either element of the set $\{3, 15\}$. Likewise $\mathbb{Z}_9$ is generated by either of $\{2, 4, 8, 10, 14, 16\}$

Generators of $\mathbb{Z}_{18}$ are $\{1, 5, 7, 11, 13, 17\}$. □

Problem 6. Give your proof that $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$ but $\mathbb{Z}_8 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_4$.

Solution. We have a map $\psi : \mathbb{Z}_2 \oplus \mathbb{Z}_5 \to \mathbb{Z}_{10}$, defined by the formula $\psi(x \oplus y) = 5x + 2y$. The map is correctly defined because $5, 2 \in \mathbb{Z}_{10}$ are elements of order $2, 5$ respectively. $2, 5$

are relatively prime $\Rightarrow -2\times 2+1\times 5=1 \Rightarrow x=2(-2x)+5x \Rightarrow$ the map ψ is onto. $|\mathbb{Z}_2\oplus\mathbb{Z}_5|=|\mathbb{Z}_{10}|=10 \Rightarrow \psi$ is a bijection.

If $2x \cong 0\text{mod}8 \Rightarrow x \cong 0\text{mod}4 \Rightarrow$ the only nontrivial element of order 2 is $4\in\mathbb{Z}_8$. On the other hand $\{(1,0),(0,2),(1,2)\}$ are nontrivial element of order 2 in $\mathbb{Z}_2\oplus\mathbb{Z}_4$. An isomorphism defines a bijection between sets of elements of the same order. $\Rightarrow \mathbb{Z}_8 \ncong \mathbb{Z}_2\oplus\mathbb{Z}_4$ □

Problem 7. Give an example of

a nontrivial subgroup of a multiplicative group $\mathbb{R}^\times=\{x\in\mathbb{R}|x\neq 0\}$

(1) of finite order

(2) of infinite order

Can $\mathbb{R}^\times$ contain an element of order 7?

Solution. $\mathbb{Z}_2\cong\{1,-1\}\subset\mathbb{R}^\times$

$\mathbb{Z}\cong\{\pi^k|k\in\mathbb{Z}\}\subset\mathbb{R}^\times$

If x has order 7 then $x^7=1$. If $x<0$, then $\exp(a)=-x>0$ has order 14. This is impossible since $\exp(14a)=1\Rightarrow 14a=0\Rightarrow a=0$. For $x>0$ the proof is similar. □

Problem 8. Prove that $U(2^n)$ $(n\geq 3)$ is not cyclic.

Solution. There is an onto map $U(2^n)\to U(2^{n-1})$ $x\,\text{mod}2^n \to x\,\text{mod}2^{n-1}$. Indeed if $\gcd(x,2^{n-1})=1\Rightarrow x=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$, primes $p_i>2$. Thus $\gcd(x,2^n)=1$. It suffice to show that $U(2^3)=U(8)$ is not cyclic. It contains elements $\{1,3,5,7\}$, which satisfy $a^2=1\,\text{mod}8$. This equality $(2a=0)$ doesn't hold in $\mathbb{Z}_4$. □

Problem 9. Decompose $\sigma:(1,2,3,4,5,6)\to(2,1,4,6,5,3)$ into product of

(1) disjoint cycles

(2) cycles of order two

What is the order of σ? What is the parity of σ?

Solution. $\sigma=(1,2)(3,4,6)=(1,2)(4,5)(4,6)(5,6)$. The order is $\text{lcm}(2,3)=6$. The parity is $4\,\text{mod}\,2=0$.

$\square$

Problem 10. Find a subgroup G in symmetric (permutation) group S_n such that

(1) $n = 4$ and G is abelian noncyclic group

(2) $n = 8$ and G is dihedral group.

Solution. (1) Choose $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and apply Cayley's Theorem.

(2) Choose G to be a group of symmetries of a square and apply Cayley's Theorem.

$\square$