MIDTERM2

$\alpha\beta\gamma$

Problem 1

Festival of finite abelian groups.[1]

a.

> Please prove that $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/49\mathbb{Z}$.

By Proposition 5.2.6 we known $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/49\mathbb{Z}$ if and only if $gcd(7,7) = 1$, but clearly $gcd(7,7) = 7$, so we conclude that $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \ncong \mathbb{Z}/49\mathbb{Z}$.

b.

> Let A be an abelian group of order 392. List all possible isomorphism classes of A.

By the fundamental theorem of finite abelian groups, we will first consider the factorization of $|A| = 392 = 2^3 \cdot 7^2$. Thus the list of all isomorphism classes of A are given below

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
- $\mathbb{Z}_8 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{49}$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{49}$
- $\mathbb{Z}_8 \times \mathbb{Z}_{49}$

c.

> Assume further that A contains an element of order 196. List the possible isomorphism classes of A.

To enforce the existance of an element of order $196 = 2^2 \cdot 7^2$ so thus we know that this element is the pair of an element of order 4, and an element of order 49. So from the list constructed in (1.b), we will select the options with groups contaiings elements of these orders.

- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{49}$.
- $\mathbb{Z}_8 \times \mathbb{Z}_{49}$.

Date: 2020-04-15.

[1] I used $\mathbb{Z}_i$ and $\mathbb{Z}/i\mathbb{Z}$ interchanably, for eash of typing, sorry.

d.

> Let $G = \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Find subgroup H, K of G both of order 2 so that G/H and G/K are not isomorphic.

Consider $H = 1 \times \langle 2 \rangle \times 1$, and $K = 1 \times 1 \times \mathbb{Z}_2$. It is clear to show that both H and K have order two by their construction. Now we consider $G/H \cong (\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})/(1 \times \langle 2 \rangle \times 1)$, which is inturn isomorphic to

$$G/H \cong ((\mathbb{Z}/49\mathbb{Z})/1) \times ((\mathbb{Z}/4\mathbb{Z})/\langle 2 \rangle) \times ((\mathbb{Z}/2\mathbb{Z})/1) \cong \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Repeating this for G/K we find

$$G/K \cong \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times 1.$$

Then by a simmilar argument to (1.a), we can conclude that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z} \times 1$, and so we can thus conclude that there is indeed no isomorphism between G/H and G/K.

Problem 2

> Suppose a group of prime order p acts on a finite set. What are the possible sizes of the orbits of this action?

Given some group G of prime order p, acting on a finite set S, then By propositin 4.1.2, we known that $|\mathcal{O}(s)| = |G : G_s|$ for all $s \in S$. and we know that $|G| = |G : G_s||G_s|$. Thus we are able to express

$$|\mathcal{O}(s)| = \frac{|G|}{|G_s|}$$

Since, $G_s \leq G$, then $|G_s| \big| |G|$, by lagranges theorem, since $|G|$ is prime, then we must have $|G_s| = 1$ or $|G_s| = p$. Thus we conclude that

$$|\mathcal{O}(s)| = \frac{|G|}{1} = |G| = p$$
$$|\mathcal{O}(s)| = \frac{|G|}{p} = 1.$$

so the orbits of this action must be of order 1 or p.

Problem 3

> Here is a nice fact: "If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p". There are many proofs of this fact. For this problem, please follow the steps below to prove this result.

a.

> Let S denote the set of ordered p-tuples of element sof G the product of whose coordinates is 1. So
>
> $$S = \{(x_1, x_2, \ldots, x_p) : x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$
>
> Show that S contains $|G|^{p-1}$ elements.

We can consider the produce $x_1x_2\cdots x_p = 1$, as $(x_1x_2\cdots x_{p-1})\cdot x_p = 1$. In this case we can see that x_p must be the inverse of the product of all the elements that come prior to it. This means that after picking any value for x_1 to x_{p-1}, then x_p is forced to be a specific value. Thus we are able to select $p-1$ elements from G. So we can see that $|S| = |G|^{p-1}$.

b.

> We would like to define an action of the cyclic group of order p, C_p, on S. Do this by letting a permutation act on the indices of an element of S. Please prove that this is a group action.

To prove that this is a group action, we will first show that for some element $a_1, a_2 \in C_p$, and $(x_1,\ldots,x_p) \in S$, then $a_1.(a_2.(x_1\ldots,x_p)) = (a_1a_2).(x_1,\ldots,x_p)$. First we note, that $a_1 = a^\alpha$, and $a_2 = a^\beta$. Now let us compute

$$\begin{aligned} a^\alpha.(a^\beta.(x_1,\ldots,x_p)) &= a^\alpha.(x_{1+\beta},\ldots,x_{p-\beta}) \\ &= (x_{1+\beta+\alpha},\ldots,x_{p-\beta-\alpha}) \\ &= (x_{1+(\beta+\alpha)},\ldots,x_{p-(\beta+\alpha)}) \\ &= (a^(\alpha+\beta))(x_1,\ldots,x_p) \\ &= (a^\alpha a^\beta)(x_1,\ldots,x_p). \end{aligned}$$

Now it remains to show that $a^0.(x_1,\ldots,x_p) = (x_1,\ldots,x_p) \quad \forall(x_1,\ldots,x_p) \in S$. So let us compute

$$a^0.(x_1,\ldots,x_p) = (x_1,\ldots,x_p).$$

Thus we can conclude that this is indeed a group action.

c.

> Using your work above, including Problem 2, prove the nice fact.

From problem 2, we know that the order of orbits in S of this action must be either 1 or p. We can see that the size of an orbit is 1 is true only for tuples of the form $(x,x,\ldots,x)$, with $x^p = 1$. Thus if there are any orbits of size 1 other than the orbit of $(1,1,\ldots,1)$, then that element must be of order p. Let us assume that there is no such other orbit, so all orbits are of size p. Let us say that there are k orbits of size p, and m orbits of size 1. Then we can see that $|G|^{p-1} = kp + m$. Then since $p\big||G|$, we can also conclude that $p|m$. Since $(1,1,\ldots,1)$ has an orbit of size 1, then we know that $m \neq 0$, thus we must conclude that there are at least $p-1$ other elements that correspond to an orbit of size 1, and that implies that $x^p = 1$.

Problem 4

> The Class Equation expresses the order of a finite group as the sum of a list of natural numbers $n_1+n_2+\cdots+n_k$. Consider the following sums. Please rule out those that could not appear on the right hand side of the Class Equation. Please explain your reasoning.

a.

$$3+2+5$$

With the equation of the form $|Z(G)|+|G:C_G(g_1)|+|G:C_G(G_2)|$, we know that $Z(G)\leq G$, and so thus $|Z(G)|\big||G|$, thus $|Z(G)|=2$ or $|Z(G)|=5$, Then we know that $|G:C_G(g_i)|=\frac{|G|}{|C_G(g_i)}$, and thus we can conclude that for some i, $3=\frac{10}{|C_G(g_i)}$ and thus $|C_G(g_i)|=\frac{10}{3}$, which is impossible. Thus this cannot appear on the right hand side of the class equation.

b.

$$1+2+2+5$$

This is the class equation.

c.

$$1+2+3+4$$

By a similar argument to (4.a), we know that each n_i must divide $|G|=10$, but 3, and 4 do not divide 10, and so this cannot appear in the class equation.

d.

$$2+2+2+2+2$$

This is not possible, as then $|Z(G)|=2$, and this leads to $|G/Z|=5$, thus G/Z is cyclic, and so we would conclude that G is abelian. If G were abelian, then the class equation would be 10.

Problem 5

> Let E/F be an extension of fields. Suppose $f(x),g(x)\in F[x]$ are not both zero. Let $d_F(x)$ be the gcd of $f(x)$ and $g(x)$ in $F[x]$. Now view $f(x),g(x)$ as elements of $E[x]$, and let $d_E(x)$ be the gcd of $f(x)$ and $g(x)$ in $E[x]$. Show $d_F(x)=d_E(x)$. (This is a bit surprising since various questions involving divisibility such as irreducibility depend on the field be used.)

Consider some $f(x),g(x)\in F[x]$, with $d_F(x)$ be the gcd of the two in $F[x]$. Then by the GCD theorem, we know that we can express this as

$$d_F(x)=d=a(x)f(x)+b(x)g(x).$$

since $d_E(x)$ divides both f and g, then we must conclude that $d_E(x)$ also divides $d_F(x)$. A similar argument can be made to show that $d_F(x)$ divides $d_E(x)$. Thus we can conclude that $d_F(x)=d_E(x)$.

Problem 6

> The algebraic numbers $\mathcal{A}$ are all numbers in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. They are a subfield of $\mathbb{C}$; you can assume this without proof. (Its not a bad proof, feel free to enjoy it in a non-test setting.) Please prove that $\mathcal{A}$ is not a finite extension of $\mathbb{Q}$. Give lots of details.

Let us consider the polynomials given by $f(x) = x^{2n} - 2$. We can see that by using Eisenstein irreducibility criterion, with the prime 2, that $x^{2n} - 2$ is irreducible in $\mathbb{Z}$, and irreducible in $\mathbb{Q}$. We can see that $\sqrt[2n]{2}$ is a root of this polynomial, and thus $\sqrt[2n]{2}$ is algebraic and so $\sqrt[2n]{2} \in \mathcal{A}$.

We see that the degree of the field extension is thus $[\mathbb{Q}(\sqrt{2}, \ldots, \sqrt[2n]{2}) : \mathbb{Q}] = 2n$, as $\left\{1, \sqrt{2}, \ldots, \sqrt[2n]{2}, \sqrt{2}\sqrt[4]{2}, \ldots\right\}$ form a basis. Since $\mathbb{Q}(\sqrt{2}, \ldots, \sqrt[2n]{2}) \subseteq \mathcal{A}$. Then we know that $2n = [\mathbb{Q}(\sqrt{2}, \ldots, \sqrt[2n]{2}) : \mathbb{Q}] \leq [\mathcal{A} : \mathbb{Q}]$, for any $n \in \mathbb{N}$. Thus we can see that $[\mathcal{A} : \mathbb{Q}] \geq 2n$ for all $n \in \mathbb{N}$, and since $\mathbb{N}$ is infinite, then $[\mathcal{A} : \mathbb{Q}]$ must also be infinite.