Homework 5 due Wed, Oct 20th by 11am in Gradescope

Name: Sean Eva
GTID: 903466156
Collaborators:
Outside resources:

INSERT a "pagebreak" command between each problem (integer numbers). Problem subparts (letter numbered) can be on the same page.

REMOVE all comments (within "textit{}" commands) before submitting solutions.

DO NOT include any identifying information (name, GTID) except on the first/cover page.

1. Problem 4.1 # 20. *Hint: Compute a product table.*

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

(a) Let assumptions be as in problem 4.1 # 20. In order to show this is a group, we need to show that it is nonempty, closed under the operation, contains an identity, contains inverses, and is associative. The identity of this group is 1 by the definition of quaternions. Similarly, by the definition of quaternions it is nonempty. By creating the product table above, we can see that the group is closed under multiplication. We can also see that for every element a, there is another element b such that $ab = 1$, the identity. Specifically, -1 is its own inverse, i is the inverse of $-i$, j is the inverse of $-j$, and k is the inverse of $-k$. It is also then true by the definition of quaternions that for $x, y, z \in G$ that $(xy)z = x(yz)$ and is therefore associative. Since the quaternions are nonempty, contain an identity, contains inverses, is closed under multiplication, and are associative they are a group under the operation of multiplication.

(b) There is the obvious trivial subgroup $< 1 >$. Then we have the cyclic groups $< -1 >$ $, < i >, < j >, < k >, < -i >, < -j >, < -k >$. However, if we write out $< i >= \{1, i, -1, -i\}$ and similarly for $< j >$ and $< k >$. This then means that $< i >=< -i >$. Therefore, the subgroups of G are $< 1 >, < -1 >, < i >, < j >$, and $< k >$.

(c) The center of G is $\{a \in G | ax = xa, \forall x \in G\}$. By inspecting the product table above, this is true for 1 and -1. Therefore, $Z(G) = \{1, -1\}$.

(d) It is easy to see that G is nonabelian. For example, $i * j = k \neq j * i = -k$. However, the subgroup $< -1 >= \{1, -1\}$ we can see that $\forall x \in G, x * 1 * x^{-1} = x * x^{-1} = 1 \in < -1 >$, and $x * -1 * x^{-1} = -x * x^{-1} = -1 \in < -1 >$ which then shows that $< -1 >$ is a normal subgroup. Then we can show that $< i >, < j >$, and $< k >$ are normal too by looking at the product table above. This then shows that for the group G which is nonabelian, all its subgroups are normal.

2. Prove that a division ring is a domain directly from the definitions.

   Let R be a ring such that R is a division ring. That is to say that R has a unit and that for every $a \in R, a \neq 0$ there is a corresponding $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$, the unit in R. This means that R has a multiplicative identity. Let $a, b \in R$ such that $a \cdot b = 0$ where $a \neq 0$. This then implies, by the definition of a ring, that a^{-1} exists. Then we can say that $a^{-1}(ab) = a^{-1}(0) = 0 = (1)b = (a^{-1}a)b$. This implies that whenever $ab = 0$ either $a = 0$ or $b = 0$ which means that R is an integral domain.

3. Give an example, in the quaternions, of a noncommuative domain that is not a division ring.

   Consider $\{a + bi + cj + dk | a, b, c, d \in \mathbb{Z}\}$ which is a subset of the quaternions. It is easy to see that this is a noncommutative domain because $ij \neq ji$, and since it does not contain 2^{-1} it cannot be a division ring.

4. Let R be the ring of 2×2 matrices over the reals. Prove that $S = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ is a field.

Let assumptions be as above. In order to prove that S is a field, we need to prove that it is a ring, commutative ring, and that is a division ring. First, in order to prove that S is a ring, or more specifically a substring, we need to show that $ab, a+b, a+(-b) \in S$ for $a, b \in S$. Consider $a = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, b = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ for $a, b, c, d \in \mathbb{R}$, then we can see that $a+b = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b+-d & a+c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in S$. Similarly, $a + (-b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} -c & -d \\ d & -c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -b+d & a-c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix} \in S$. Lastly, $ab = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \in S$. Therefore, since for some $a, b \in S$ we found that $ab, a+b, a+(-b) \in S$, we know that S is a subring of R. We will next show that S is commutative. For $a, b \in S$, we can see that $ab = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} = ba \in S$. Thus, S is commutative. Lastly, we need to show that S is a division ring. It would be helpful to first find the unit element of S. This is trivial in this ring because it is just $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ the identity matrix. Consider $a = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, using the properties of matrices $\det(a) = a^2 + b^2 \neq 0$ if either a or $b \neq 0$ if this is true, then a^{-1} exists in the form $\frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in S$. By definition of matrices $aa^{-1} = 1$. If $a, b = 0$, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ which is the 0 or the additive identity in S and by the definition of a division ring is not included. Therefore, S is a division ring. Since S is a ring, is commutative, and is a division ring, we know that S is a field.

5. Let R be a finite integral domain. Prove that R is a field.

   Let assumptions be as above. That is to say that in the ring R, if $a \cdot b = 0$ then either $a = 0$ or $b = 0$ for $a, b \in R$. In order to prove that R is a field, R needs to be a ring, R needs to be commutative, and R needs to be a division ring. Given the definition of being an integral domain, R is a ring and R is commutative. That leaves to prove that R is a division ring. Let $1 \in R$ be the unit element in R. Consider the elements of $R = \{a_1, a_2, a_3, ..., a_n\}$ for $n \in \mathbb{Z}$. Let us take arbitrary $a \in R$ and multiply all elements by a. Since R is a finite integral domain, it is true to say then that $R = \{aa_1, aa_2, aa_3, ..., aa_n\}$. For some a_i where $1 \leq i \leq n$ we have that $aa_i = 1$ which means that $aa^{-1} = 1$ has a solution in R and R is a division ring. Therefore, since R is a finite integral domain and we proved that R is a division ring, we know that R is a field.

6. Problem 4.2 # 8.

   (a) Let assumptions be as in the problem, that is F is a finite field. Let us say that $|F| = n$ and $1 \in F$ is the multiplicative identity of F. We know that $F = \{1, 2 \cdot 1, 3 \cdot 1, ..., n \cdot 1 n + 1 \cdot 1\}$. However, since F has n elements, we know that there is a non-distinct element in the previous statement such that $k \cdot 1 + m \cdot 1 = 0$ for some $k \neq m$. Then we know that $(k - m) \cdot 1 = 0$. Let $(k + m) = p$ such that p is the least positive integer such that $p \cdot 1 = 0$. Now we need to show that p is prime. Suppose not, then $p = ns$ where $1 < s < p, 1 < n < p$. Then, $p \cdot 1 = p \cdot 1^1 = (ns) \cdot (1 \cdot 1) = (n \cdot 1)(s \cdot 1) = 0$. Since F is a we know that either $n \cdot 1 = 0$ or $s \cdot 1 = 0$ which is a contradiction because we said that p is the least integer such that $p \cdot 1 = 0$. Therefore, there exists p which is prime such that $p \cdot 1 = 0$. Then we know that for any $a \in F$ we can see that $a + a + a + a ... + a = a \cdot 1 + a \cdot 1 + ... + a \cdot 1 = a(1 + 1 + 1 + ... + 1) = a(p \cdot 1) = a \cdot 0 = 0$. Therefore, we know that there exists a prime p such that $pa = 0$ for all $a \in F$.

   (b) Let assumptions be as in the problem, that is F is a finite field. We proved in part a that there exists a prime p such that $p \cdot 1 = 0$. Again, let p be the least integer for which $p \cdot 1 = 0$. Therefore, 1 has order p. Let p' be any prime dividing $|F| = q$. By Cauchy's Theorem, we know that there is an element $b \in F$ that has order p'. Since, from part a, $pa = 0$ for all $a \in F$, then we know that $pb = 0$. Since the order of b is p', then $p'|p$ which implies that $p' = 1$ or $p' = p$ but since p' is prime, we know that $p' \neq 1$, and therefore, $p' = p$. Thus, any prime dividing q must be p and it follows that $q = p^n$.