Final exam / 2008.5.9 / Modern abstract algebra / MAT 4233.001

Note Title 5/9/2008

1. Suppose G is a group such that $\forall a,b,c \in G$ $ab = ca \Rightarrow b = c$. Prove that G is abelian.

Suppose $a, b \in G$. Let $c = aba^{-1}$.

Then $ca = ab$, so $b = c$, so $ab = ba$ ☺

2. Show that in a finite group the number of all elements of order 3 is even.

Suppose G is a group. If $a \in G$ with $|a| = 3$, then $\langle a \rangle = \{e, a, a^2\} \cong \mathbb{Z}_3$. Suppose $b \in G$ with $|b| = 3$.

If $b \in \langle a \rangle$, then $b = a$ or $b = a^2$ so $\langle b \rangle = \langle a \rangle$

If $b \notin \langle a \rangle$, then $\langle b \rangle \cap \langle a \rangle = \langle e \rangle$

$\therefore$ Elements of order 3 come in pairs! ☺

3. Let $G = GL(n, \mathbf{Q})$ be the multiplicative group of invertible $n \times n$ matrices with rational coefficients and $H = SL(n, \mathbf{Q}) = \{A \in G\colon \det A = 1\}$. Prove that H is a subgroup of G. Prove or disprove that H is normal in G.

$H < G$

* **Identity:** $\det I = \det \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = 1$ $\therefore$ $I \in H$ ✓

* **Closure:** if $A, B \in H$, then $\det A = \det B = 1$,
so $\det(AB) = \det A \det B = 1 \cdot 1 = 1$ so $AB \in H$ ✓

Claim: For any $B \in G$, $\det(B^{-1}) = \dfrac{1}{\det B}$

Proof: $BB^{-1} = I$ $\therefore$ $1 = \det I = \det(BB^{-1}) = \det B \cdot \det B^{-1}$

* **Inverses:** If $A \in H$, then $\det A = 1$, so $\det A^{-1} = 1$, so $A^{-1} \in H$ ✓

Claim: $H \lhd G$. Let $A \in H$, then $\det A = 1$.

If $B \in G$, then $\det(BAB^{-1}) = \cancel{\det B} \underbrace{\det A}_{1} \cancel{\det B^{-1}} = 1$

so $BAB^{-1} \in H$. ☺

4. Let G and H be as in the preceding problem. Suppose $A, B \in G$ and $\det A = \det B$. Prove that A and B belong to the same left coset of H.

If $\det A = \det B$, then $\det(AB^{-1}) = \det A \det B^{-1} = \dfrac{\det A}{\det B} = 1$

$\therefore$ $AB^{-1} \in H$ ☺

5. Prove that for $n \geq 3$ the symmetric group S_n has trivial center. What is $Z(S_2)$?

Suppose $\alpha \in S_n$ $\alpha \neq ()$. Then for some $i \leq n$, $\alpha(i) \neq i$

Let $j = \alpha(i)$. Since $n \geq 3$ $\exists\, k \leq n$ with $k \notin \{i, j\}$

Let $\beta = (j\ k)$. Then $\alpha\beta(i) = \alpha(i) = j$

while $\beta\alpha(i) = \beta(j) = k \neq j$. $\therefore$ $\alpha\beta \neq \beta\alpha$ $\therefore$ $\alpha \notin Z(S_n)$ ☺

$S_2 \cong \mathbb{Z}_2$, so $Z(S_2) = S_2$ ☺

6. Let A be the set of all elements of the ring $\mathbf{Z} \oplus \mathbf{Z}$ whose first coordinate is even. Prove that A is an ideal. Is it maximal? Prove your assertion.

ideal

* Identity: 0 is even, so $[0,0] \in A$. ✓
* Differences: if $[a,b], [c,d] \in A$, then a, c are even so $a-c$ is even, so $[a,b]-[c,d] = [a-c, b-d] \in A$ ✓
* Absorption: if $[a,b] \in A$, $[c,d] \in \mathbb{Z} \oplus \mathbb{Z}$, then since a is even, so is ac, so $[a,b][c,d] = [ac, bd] \in A$ ✓

Maximal: Suppose B is an ideal of $\mathbb{Z} \oplus \mathbb{Z}$, with $A \subsetneq B$.

Let $[a,b] \in B \setminus A$. Then a is odd, so $a+1$ is even,

so $[a+1, b+1] \in A \subset B$, so $[a+1, b+1] - [a,b] = [1,1] \in B$.

$\therefore$ $B = \mathbb{Z} \oplus \mathbb{Z}$ ☺

7. Suppose $\varphi: R \to S$ is a ring homomorphism from a ring with unity R to an integral domain S such that $\varphi(R) \neq \{0\}$. Prove that $\varphi(1) = 1$.

Claim: φ preserves idempotents.

If $a \in R$ with $a^2 = a$, then $\varphi(a) = \varphi(a^2) = \varphi(aa) = \varphi(a)\varphi(a) = \varphi(a)^2$ ☺

Claim: the only idempotents of S are 0 and 1.

If $y \in S$ with $y^2 = y$, then $y^2 - y = 0$, so $y(y-1) = 0$.

Since S is a domain, $y = 0$ or $y - 1 = 0$ ☺

Since $1^2 = 1$, $\varphi(1)$ is an idempotent in S.

$\therefore$ $\varphi(1) = 0$ or $\varphi(1) = 1$

If $\varphi(1) = 0$, then $\forall a \in R$ $\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = \varphi(a) \cdot 0 = 0$ ☹

8. Prove that $x^p + x + 1$ and $2x + 1$ determine the same function $\mathbf{Z}_p \to \mathbf{Z}_p$.

If $a \in \mathbb{Z}_p$, the By Fermat's Little Theorem $a^p = a$

so $a^p + a + 1 = a + a + 1 = 2a + 1$ ☺