Math 4320 : Introduction to Algebra

Prelim II (Chapter 2& 3)

Part I. Group theory

1. (2.88) Show that a finite group G generated by two elements of order 2 is isomorphic to a dihedral group D_{2n} for some n.

Proof. Let G be generated by c, b, where $c^2 = b^2 = 1$. Let $a = cb$ be an element of order, say n. (The element a is of finite order since G is finite.) G is clearly generated by a, b, since $c = cbb = ab$ is generated by a, b. Note that $a^{-1} = bc$ since $bca = bccb = 1$. Therefore $bab = bcbb = bc = a^{-1}$. Therefore we can find a homomorphism ϕ from G to D_{2n} sending a to a and b to b. Since all the relations of D_{2n} are also relations in G, $\ker \phi = \{1\}$, i.e. ϕ is injective.

To show that ϕ is surjective, it is enough to show that G has exactly $2n$ elements. Using the relation $ba = a^{-1}b$ (which tells us how to exchange the order of elements a and b), we can express every element of G as $a^i b^j$ where $0 \leq i < n$ and $0 \leq j < 2$. Thus G has at most $2n$ elements. The group G contains two subgroups $H_1 = \langle a \rangle$ and $H_2 = \langle b \rangle$, of order n and 2, respectively. Note that $H_1 \cap H_2 = 1$ since $a \neq b$, and if $a^i = b$ for some $2 \leq i \leq n/2$, then $a^{i-1} = a^i bc = bbc = c$, which is a contradiction to the fact that a is of order n. (If $a^i = b$ for some $i > n/2$ then $a^{n-i} = a^{-i} = b$, which is a similar contradiction.) Therefore G contains the subgroup $H_1 H_2$ which has $2n$ elements.Thus G has exactly $2n$ elements. □

2. Let G be a group of order n, and let F be any field. Prove that G is isomorphic to a subgroup of $GL_n(F)$.

Proof. By Cayley theorem, G is isomorphic to a subgroup of S_n. By mapping $\sigma \in S_n$ to a permutation matrix (permuting rows according to σ), S_n is isomorphic to a subgroup of $GL_n(F)$.

3. Rule out as many of the followings as possible as Class Equations for a group of order 10:

$$3 + 2 + 5,\ 1 + 2 + 2 + 5,\ 1 + 2 + 3 + 4,\ 2 + 2 + 2 + 2 + 2.$$

Proof. The first and the third expressions is ruled out because 3 does not divide 10.
$2 + 2 + 2 + 2 + 2$ is ruled out (5pts) : from the first term of the expression, the center (which is a group) has order 2, so there is an element a of order 2 in the center. There is an element b of order 5 in the group by Cauchy theorem. Since they are of order coprime, they generate a group of order 10, thus the whole

group. Since b commutes with b and with a (since a is in the center), b is in the center. Thus the center contains the group generated by b, thus has order at least 5, a contradiction.

4. Determine the class equation for each of the following groups.

(3) D_{2n} (5 pts)

Answer : For n odd, the conjugacy classes are $\{1\}, \{a^i, a^{-i}\}(i \leq (n-1)/2)$ and $\{a^ib\}$. The class equation is $1 + 2 + \cdots + 2 + n$ (there are $(n-1)/2$ two's).
For n even, the conjugacy classes are $\{1\}, \{a^{n/2}\}, \{a^i, a^{-i}\}(i < n/2), \{a^{2i+1}b\}$, and $\{a^{2i}b\}$. The class equation is $2+2+\cdots+2+n/2+n/2$ (there are $n/2$ two's).

(4) the group of upper triangular matrices in $GL_2(\mathbb{F}_3)$ (5 pts)

Answer: The elements of $GL_2(\mathbb{F}_3)$ can be written as $\begin{pmatrix} \pm1 & \pm1 \\ 0 & \pm1 \end{pmatrix}$ and $\begin{pmatrix} \pm1 & 0 \\ 0 & \pm1 \end{pmatrix}$.
Thus the group is of order 12. Note that $C = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ both have order 2 and B, C generate the whole group. By problem 1, $GL_2(\mathbb{F}_3)$ is isomorphic to a dihedral group D_{2n}. Since $|G| = 12$, $n = 6$. Thus the class equation is $2 + 2 + 2 + 3 + 3$ by part (3).

5. Show that A_n is a simple group for all $n \geq 5$ by showing Exercise **2.127**.

Proof. Any product of two transposition is a product of 3-cycles (proof of Lemma 2.155). Any two 3-cycles are conjugate in S_n (Prop. 2.33), but the point here is to show that they are conjugate in A_n. This is achieved by showing that any 3-cycle (ijk) is conjugate to (123) by $(1i)(2j)(3k) \in S_n$. Thus any $(ijk), (i'j'k')$ are cojugate by $(1i)(2j)(3k)(st)$.

6. Determine all finite groups which contain at most three conjugacy classes.
Proof : Divide according to the number c of conjugacy classes. Let $|G| = n$.
$c = 1$: trivial group, as $\{1\}$ is always one conjugacy class.
$c = 2$: $n = 1 + (n-1)$, $n - 1|n$ thus $n = 2$, and $G = \mathbb{I}_2$.
$c = 3$: $n = 1 + a + b$, say $a \leq b$. Since $a|n$ and $b|n$, thus $a|(b+1)$ and $b|(a+1)$. It follows that $\{(a, b)\} = \{(1, 1), (1, 2), (2, 3)\}$.

1. If $n = 1 + 1 + 1$, then G is abelian (since $G = Z(G)$), thus $\mathbb{I}_3$.
2. If $n = 1 + 1 + 2$, then G is a group of order 4 which is not abelian. There is no such group (Prop. 2.134).
3. If $n = 1 + 2 + 3$, then G is a group of order 6, thus isomorphic to $\mathbb{I}_6$ or S_3. Since it is not abelian, it is isomorphic to S_3. We've already seen in

Problem 4 that $1+2+3$ is the class equation of D_3 which is isomorphic to S_3, thus S_3 indeed has 3 conjugacy classes.

Answer :$\{1\}, \mathbb{I}_2, \mathbb{I}_3$ and S_3.

Part II. Rings and fields

7. Let $F = \{a + b\sqrt{-19} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

(a) Show that R is a ring, $R \subset F$ and F is a field. Conclude that R is an integral domain. Show that F is the field of fractions of R.

(b) Define $N(a + b\sqrt{-19}) = a^2 + 19b^2$. Prove that $N(\alpha) > 0$ for $\alpha \in F - \{0\}$, and that N is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$. Also prove that $N(\alpha)$ is a positive integer for every $\alpha \in R$.

(c) Prove that ± 1 are the only units in R.

Proof. (a) $R \subset F$, and R is contains $1, a-b, ab$ if $a, b \in R$, thus it is a subring of F which is a field. Thus R is an integral domain. By definition, $Frac(R) \subset F$. If $a + b\sqrt{-19} \in F$, then by using the common denominator, we can express it as a quotient α/β where $\alpha \in R$, and $b \in \mathbb{Z} \subset R$. Thus $F \subset Frac(R)$.
(b) $N(\alpha) > 0$ since it is sum of squares of real numbers. $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta)$. $N(a + b\theta) = a^2 + ab + 5b^2 \in \mathbb{Z}$.
(c) If u is a unit, say $uv = 1$, then from $N(u) \geq 1$, $N(v) \geq 1$, and $N(u)N(v) = N(uv) = 1$, it follows that $N(u) = 1$. Let $u = a + b\theta$ so that $a^2 + ab + 5b^2 = 1$. Since a, b are integers, the only solutions are $(a, b) = (\pm 1, 0)$, i.e. $u = \pm 1$.

8, 9, 10 *Proof. Just follow the hint.*