Thursday 10/24/13. 611 Midterm solutions.

Q1. G group, $|G| = 21$, G not abelian.

(a) $Z(G) = \langle e \rangle$.

Proof: $Z(G) \leq G \overset{\text{Lagrange}}{\Rightarrow} |Z(G)| \mid |G|$

$|G| = 21 = 3.7$

$\therefore |Z(G)| = 1, 3, 7$ or 21.

$|Z(G)| \neq 21$ because G not abelian i.e. $Z(G) \neq G$.

$|Z(G)| = 3$ OR $7 \Rightarrow \left| G/Z(G) \right| = 7$ OR 3, prime

$\Rightarrow G/Z(G)$ cyclic $\underset{\text{HW1Q13}}{\Rightarrow}$ G abelian #

(Proof: pick $x \in G$ s.t. $\bar{x} \in G/Z(G)$ is generator.

Then $a, b \in G \Rightarrow a = x^m \cdot z$, $b = x^n \cdot z'$,

some $m, n \in \mathbb{Z}$, $z, z' \in Z(G)$

$\Rightarrow ab = ba$, G abelian.)

Thus $|Z(G)| = 1$, $Z(G) = \{e\}$ $\square$.

(b) Class equation of G?

Class equation is $|G| = \sum_{C \text{ conjugacy class}} |C|$

Note: for $x \in G$, $C(x) = \{gxg^{-1} \mid g \in G\}$ conjugacy class of x

$Z(x) = \{g \mid gxg^{-1} = x\} \leq G$, centralizer of $x \in G$

$|G| = |C(x)| \cdot |Z(x)|$ by orbit-stabilizer theorem

$\Rightarrow \quad |C(x)| \,\Big|\, |G|.$

Also, $|C(x)| = 1 \iff C(x) = \{x\}$

$\iff gxg^{-1} = x \quad \forall\, g \in G$

$\iff x \in Z(G).$

Now, by part (a), $|Z(G)| = 1$,

so class equation is

$$|G| = 21 = 1 + \underbrace{(3 + \cdots + 3)}_{a} + \underbrace{(7 + \cdots + 7)}_{b}$$

some $a, b \in \mathbb{Z}$, $a, b \geq 0$.

(only divisors of $|G| = 21$ are $1, 3, 7, 21$).

By inspection only possibility is $a = b = 2$,

$$21 = 1 + 3 + 3 + 7 + 7.$$

Alternative solution (more work) :—

One can show, using Sylow theorems, that the only non-abelian group G of order 21 is

$$G = \langle a, b \mid a^7 = b^3 = e,\ bab^{-1} = a^2 \rangle$$

$$= \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$$

$\mathbb{Z}/7\mathbb{Z} = \langle a \rangle$, $\mathbb{Z}/3\mathbb{Z} = \langle b \rangle$

$3 \leftrightarrow 1$

$$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}.$$

$$1 \longmapsto (x \mapsto 2x) \longleftrightarrow 2 \longmapsto 2$$

Now can compute the conjugacy classes in G explicitly:

$\{e\}$

$\{a, a^2, a^4\}$, $\{a^3, a^5, a^6\}$

$\{b, ab, \ldots, a^6 b\}$, $\{b^2, ab^2, \ldots, a^6 b^2\}$

$\rightsquigarrow$ Class equation $21 = 1 + 3 + 3 + 7 + 7.$

Q2. $|G|=44$, $\exists\, x\in G$ of order 4. Classify.

$|G| = 2^2 \cdot 11$

$s :=$ # Sylow 2 subgroups.

$s \equiv 1 \bmod 2$, $s \mid 11$ $\Rightarrow$ $s = 1$ OR 11 (using Sylow Thm 3)

$t :=$ # Sylow 11 subgroups

$t \equiv 1 \bmod 11$, $t \mid 4$ $\Rightarrow$ $t=1$.

Let H be unique Sylow 11-subgroup. So H is normal,

$|H| = 11$ $\Rightarrow$ $H \simeq \mathbb{Z}/11\mathbb{Z}$.

Let K be Sylow 2-subgroup. So $|K|=4 \Rightarrow K \simeq \mathbb{Z}/4\mathbb{Z}$ OR $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

But $\exists\, x\in G$ of order 4 $\Rightarrow$ $\underset{\underset{\mathbb{Z}/4\mathbb{Z}}{\shortparallel}}{\langle x\rangle} \leq G$,

i.e. $\exists$ Sylow 2-subgp $\langle x\rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

All Sylow p-subgroups are conjugate, so in particular isomorphic.

Thus $K \simeq \mathbb{Z}/4\mathbb{Z}$.

$$\left.\begin{aligned} &\text{Now } \gcd(|H|,|K|)=1 \overset{\text{Lagrange}}{\Rightarrow} H\cap K = \{e\} \\ &H \trianglelefteq G \Rightarrow HK \leq G \end{aligned}\right\} \Rightarrow$$

$$\begin{aligned} H \rtimes_\varphi K &\xrightarrow{\sim} HK, \quad \text{where } \varphi: K \to \mathrm{Aut}(H) \\ (h,k) &\longmapsto hk \qquad\qquad\qquad k \mapsto (h \mapsto khk^{-1}) \end{aligned}$$

Finally $|HK| = |H \rtimes_\varphi K| = |H|\cdot|K| = |G| \Rightarrow HK = G$

$\Rightarrow H \rtimes_\varphi K \xrightarrow{\sim} G$.

Remains to classify possible homs $\varphi: K \to \mathrm{Aut}(H)$.

$$\begin{array}{ccccc} K & \xrightarrow{\varphi} & \mathrm{Aut}(H) & & \\ \wr\wr & & \wr\wr & & \\ \mathbb{Z}/4\mathbb{Z} & & \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) & \simeq (\mathbb{Z}/11\mathbb{Z})^\times & \simeq \mathbb{Z}/10\mathbb{Z} \end{array}$$

$\tilde{\varphi}: \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$

$4 \cdot \tilde{\varphi}(1) = 0 \implies \tilde{\varphi}(1) = 0$ OR 5.

$\tilde{\varphi}(1) = 0 \iff \varphi(k) = id_H \quad \forall k \in K$

$\iff khk^{-1} = h \quad \forall\ h \in H,\ k \in H$

$\iff H \rtimes_\varphi K \simeq H \times K.$

i.e. $G \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \underset{\substack{| \\ \gcd(4,11)=1.}}{\simeq} \mathbb{Z}/44\mathbb{Z}$

$\tilde{\varphi}(1) = 5 \iff$ writing $K = \langle b \rangle$, $\varphi(b)$ is element of $\mathrm{Aut}(H)$ of order 2,

i.e., writing $H = \langle a \rangle$, $\underset{\substack{\| \\ bab^{-1}}}{\varphi(b)(a)} = a^{-1}$

$\iff G \simeq \langle a, b \mid a^{11} = b^4 = e,\ bab^{-1} = a^{-1} \rangle.$

Q3. $G = \langle x, y \mid x^2, y^2 \rangle.$

Identify with semidirect product of abelian groups.

Notice that any element of G can be written as

$(x \text{ OR } y) \cdots xyxyxy \cdots (x \text{ OR } y).$

$= (y \text{ OR } e)\,(xy)^n\,(y \text{ OR } e). \qquad (*) \quad n \in \mathbb{Z}, \geq 0.$

So G is generated by the two elements xy & y, of orders ∞ & 2.

Also, $y(xy)y^{-1} = yx = (xy)^{-1}$

using $x^2 = y^2 = e$.

So, define $H = \langle a, b \mid b^2 = e,\ bab^{-1} = a^{-1} \rangle$

$$\cong \underset{\langle a \rangle}{\mathbb{Z}} \rtimes_{\varphi} \underset{\langle b \rangle}{\mathbb{Z}/2\mathbb{Z}}$$

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}^{\times} = \{\pm 1\}$$
$$1 \longmapsto (x \mapsto -x) \mapsto -1$$

$\theta : G \longrightarrow H$

$\theta(x) = ab$ (so $\theta(xy) = abb = a$.)

$\theta(y) = b$

θ is well defined: $G = F/N$, F = free group gen'd by x & y

N = smallest normal subgroup containing x^2 & y^2.

We have $\tilde{\theta} : F \longrightarrow H$, $\tilde{\theta}(x) = ab$, $\tilde{\theta}(y) = b$

by universal property of free group.

Check $N \subset \ker(\tilde{\theta})$: $\tilde{\theta}(x^2) = (ab)^2 = abab$

$= a(bab^{-1})$

$= aa^{-1} = e$ ✓

$\tilde{\theta}(y^2) = b^2 = e$.

So $\tilde{\theta}$ induces $\theta : G = F/N \longrightarrow H$.

To show θ is an isomorphism:

$\boxed{\text{Either}}$ observe θ is surjective (because $xy \mapsto a$ & $y \mapsto b$)

& θ is injective (check using expression $(*)$ for elements of G)

$\boxed{\text{Or}}$ (better) define inverse ψ & check

$\psi\theta = id_G$, $\theta\psi = id_H$:-

$\psi : H \longrightarrow G$ $\quad \psi(a) = xy$

$\psi(b) = y$

ψ well defined: $\quad \psi(b^2) = y^2 = e$.

$H = \langle a,b \mid b^2, baba^{-1} \rangle \quad \psi(bab^{-1}a) = yxyy^{-1}xy = e$.

Now $\psi\theta(x) = x$, $\psi\theta(y) = y$ by construction

$\Rightarrow \psi\theta = id_G$

& similarly $\theta\psi = id_H$.

Thus $\psi = \theta^{-1}$, θ is isomorphism.

Q4. Identify quotient rings R/I explicitly.

Determine whether I is prime or maximal (or neither).

a) $\mathbb{R}[x]/(x^3-8)$.

$$x^3 - 8 = (x-2)\underbrace{(x^2+2x+4)}$$

roots $-1 \pm \sqrt{3}i \notin \mathbb{R} \Rightarrow$ irreducible in $\mathbb{R}[x]$.

$\gcd(x-2,\ x^2+2x+4) = 1$ (e.g. because no common roots in $\mathbb{C}$)

$$\Rightarrow \mathbb{R}[x]/(x^3-8) = \mathbb{R}[x]/(x-2)\cdot(x^2+2x+4)$$

$$= \mathbb{R}[x]/(x-2)\cap(x^2+2x+4) \xrightarrow[\text{CRT}]{\sim} \mathbb{R}[x]/(x-2) \times \mathbb{R}[x]/(x^2+2x+4)$$

& $\mathbb{R}[x]/(x-2) \xrightarrow[\text{FIT}]{\overline{\varphi}\ \sim} \mathbb{R}$ induced by $\varphi: \mathbb{R}[x] \to \mathbb{R}$, $x \mapsto 2$

$\ker\varphi = (x-2)$

$\mathbb{R}[x]/(x^2+2x+4) \xrightarrow[\text{FIT}]{\overline{\psi}\ \sim} \mathbb{C}$ induced by $\psi: \mathbb{R}[x] \to \mathbb{C}$, $x \mapsto -1+\sqrt{3}i$

$\ker\psi = (x^2+2x+4)$

Thus $\mathbb{R}[x]/(x^3-8) \xrightarrow{\sim} \mathbb{R}\times\mathbb{C}$.

Recall: an ideal $I \subset R$ is prime $\iff$ R/I is integral domain

maximal $\iff$ R/I is a field.

(in particular, maximal $\Rightarrow$ prime)

Also, a direct product $R_1 \times R_2$ is not an integral domain because $(1,0)\cdot(0,1) = (0,0)$.

Thus $\mathbb{R}[x]/(x^3-8)$ NOT integral domain, $I=(x^3-8)$ NOT prime (& so also NOT maximal).

b) $\mathbb{Z}[\sqrt{-2}]/(1+3\sqrt{-2})$

Consider the unique homomorphism $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-2}]/(1+3\sqrt{-2})$
(see HW4 Q5(a))

φ is surjective : $1+3\sqrt{-2} = 0$ in $\mathbb{Z}[\sqrt{-2}]/(1+3\sqrt{-2})$

$\Rightarrow \sqrt{-2}\cdot(1+3\sqrt{-2}) = 0$, $-6 = \sqrt{-2}$

$\ker\varphi$: $\varphi(n) = 0 \iff n = (a+b\sqrt{-2})\cdot(1+3\sqrt{-2})$ some $a,b \in \mathbb{Z}$

$= (a-6b) + (3a+b)\sqrt{-2}$ in $\mathbb{C}$

$\iff 3a+b = 0,\ a-6b = n$

$\iff n = a-6(-3a) = 19a.$

Thus $\ker\varphi = 19\mathbb{Z}$.

Now $\bar{\varphi} : \mathbb{Z}/19\mathbb{Z} \xrightarrow[\text{FIT}]{\sim} \mathbb{Z}[\sqrt{-2}]/(1+3\sqrt{-2})$

$\mathbb{Z}/19\mathbb{Z}$ is a field (19 is prime) $\Rightarrow$ $(1+3\sqrt{-2}) \subset \mathbb{Z}[\sqrt{-2}]$ is maximal (& so also prime).

c) $\mathbb{C}[x,y]/(x+y^3)$

$\mathbb{C}[x,y] = (\mathbb{C}[y])[x]$ polynomials in x w/ coeffts in $\mathbb{C}[y]$.

In general, for R a ring, $a \in R$,

$R[x] \xrightarrow{\varphi} R$ has kernel $(x-a)$
$x \longmapsto a$ by division algorithm (see HW4 Q9, Hint.)

$\Rightarrow R[x]/(x-a) \xrightarrow[\text{FIT}]{\overline{\varphi}, \sim} R$

In our case $\mathbb{C}[x,y]/(x+y^3) = (\mathbb{C}[y])[x]/(x-(-y^3)) \xrightarrow[\sim]{\overline{\varphi}} \mathbb{C}[y]$

induced by $\varphi : (\mathbb{C}[y])[x] \longrightarrow \mathbb{C}[y]$
$x \longmapsto -y^3$
(i.e. $f(x,y) \longmapsto f(-y^3, y)$.)

Now $\mathbb{C}[y]$ is an integral domain, but NOT a field.
So $(x+y^3) \subset \mathbb{C}[x,y]$ is prime but NOT maximal.

Q5. $d \in \mathbb{Z}$, $d \geq 3$.
2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-d}]$.

Define $N : \mathbb{Z}[\sqrt{-d}] \longrightarrow \mathbb{Z}_{\geq 0}$

$N(\alpha) = |\alpha|^2 = \alpha\bar{\alpha} = (a+b\sqrt{-d})(a-b\sqrt{-d})$
$\alpha = a+b\sqrt{-d}$ $\quad = a^2 + d \cdot b^2$
$a,b \in \mathbb{Z}$.

Then $N(\alpha\beta) = N(\alpha)N(\beta)$
$N(\alpha) = 1 \iff \alpha$ is a unit in $\mathbb{Z}[\sqrt{-d}]$.

If 2 is reducible, have $2 = \alpha\beta$, α, β not units
$4 = N(2) = N(\alpha)N(\beta)$
$N(\alpha), N(\beta) \neq 1 \Rightarrow N(\alpha) = N(\beta) = 2 \Rightarrow$ ※ $a^2 + d \cdot b^2 = 2$ has no solutions $a,b \in \mathbb{Z}$

Thus 2 is irreducible.

Recall that for an integral domain R we say $p \in R$ is <u>prime</u> if $p \mid ab \Rightarrow p \mid a$ OR $p \mid b$.

Our case: 2 is NOT prime –

d even $\quad \sqrt{-d} \cdot \sqrt{-d} = -d.$

$2 \mid -d, \quad 2 \nmid \sqrt{-d} \qquad \left(\sqrt{-d}/2 \notin \mathbb{Z}[\sqrt{-d}] \right)$

d odd $\quad (1+\sqrt{-d})(1-\sqrt{-d}) = 1+d.$

$2 \mid 1+d, \quad 2 \nmid (1 \pm \sqrt{-d}).$