MATH 4041 HW 11

David Chen, dc3451

November 23, 2020

Problem 1

i

We want to compute $5^{143} \pmod{29}$. Since 29 is prime, we have that, (mod 29),

$$5^{143} \equiv 5^{5\cdot 28+3} \equiv (5^{28})^5 \cdot 5^3 \equiv 1^5 \cdot 5^3 \equiv 125 \equiv 9 + 29 \cdot 4 \equiv 9$$

so the remainder is 9 after 5^{143} is divided by 29.

ii

Consider the group $(\mathbb{Z}/100\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^*$, where $\gcd(a, 100) = 1 \implies a \in (\mathbb{Z}/100)^*$. $f([a]_{100}) = ([a]_4, [a]_{25})$ is an isomorphism as shown in class. Then, we have that since $\varphi(4) = 2$ and $\varphi(25) = 20$, both divisors of 20, that in both $(\mathbb{Z}/4\mathbb{Z})^*$ and $(\mathbb{Z}/25\mathbb{Z})^*$, $a^{20} = 1$. In particular,

$$[a^{20}]_4 = [a]_4^{20} = ([a]_4^2)^{10} = [1]_4^{10} = [1]_4$$

and

$$[a^{20}]_{25} = [a]_{25}^{20} = [1]_{25}$$

since for any group G and $g \in G$, $g^{|G|} = 1$.

Then, we have clearly that $f([1]_{100}) = ([1]_4, [1]_{25})$, so since f is injective and $f([a^{20}]_{100}) = ([a^{20}]_4, [a^{20}]_{25}) = ([1]_4, [1]_{25}) = f([1]_{100})$, $a^{20} = 1$ as well in $(\mathbb{Z}/100\mathbb{Z})^*$.

Problem 2

We have that since H_1, H_2 are subgroups, then $H_1 \cap H_2$ is a subgroup of G as well, and are also then subgroups of H_1 and H_2 respectively since it is clearly a subset of both. Then, $|H_1 \cap H_2|$ divides both $|H_1|$ and $|H_2|$; however, $\gcd(|H_1|, |H_2|) = 1$, so $|H_1 \cap H_2| = 1$ as well.

Then, every subgroup contains the identity, so $1 \in |H_1 \cap H_2|$, but then no other element can be a member of $H_1 \cap H_2$, or else it will have order > 1.

Problem 3

Consider any element $g \in G$. Then, we have that $\langle g \rangle \leq G$, and in particular, $|g| = |\langle g \rangle|$ must divide $|G| = p^n$. But then, since p is prime, the only possible divisors of p^n are p^k for $k \leq n$; in particular, (this is not the most parsimonious solution) $a \mid p^k$ being divisible by a prime $q \neq p$ would gives that $p^k = q \cdot \prod_i q_i$ where the latter term is the prime factorization of p^n/q, contradicting the uniqueness of prime factorization.

Then, since $|G| = p^n > 1$, pick some non-identity $g \in G$. Then, $|g| = p^k$, for $k \geq 1$ (since the only element with order 1 is the identity). Now, if $k = 1$, then we are done. Otherwise, consider $g^{p^{k-1}}$. We have that $(g^{p^{k-1}})^p = g^{p^{k-1} \cdot p} = g^{p^k} = 1$, and if $(g^{p^{k-1}})^r = 1$ for $1 \leq r \leq p-1$, then we have that $g^{p^{k-1} \cdot r} = 1$ so g has order at most $p^{k-1} \cdot r \leq p^{k-1} \cdot p - 1 < p^{k-1} \cdot p = p^k$. $\Rightarrow\Leftarrow$, so $g^{p^{k-1}}$ has order p in G.

Problem 4

Recalling the definition of $\equiv_\ell$ and $\equiv_r$, we have that $g_1 \equiv_\ell g_2 \bmod H \iff g_2 = g_1 h$ for some $h \in H$; then, taking inverses, $g_2 = g_1 h \iff g_2^{-1} = (g_1 h)^{-1}$, but $(g_1 h)^{-1} = h^{-1} g_1^{-1}$; since $h \in H \implies h^{-1} \in H$, we have that $g_2^{-1} = h^{-1} g_1^{-1} \iff g_1^{-1} \equiv_r g_2^{-1} \bmod H$ as well.

Note that this also immediately gives that $g_1^{-1} \equiv_\ell g_2^{-1} \bmod H \iff g_1 \equiv_r g_2 \bmod H$ since $(g^{-1})^{-1} = g$.

To check that defining $f : G/H \to H \backslash G$ on representatives is well-defined, we need to show that if $g_1 \equiv_\ell g_2 \bmod H$ (equivalent to $g_1 H = g_2 H$), then $f(g_1 H) = f(g_2 H)$. We have that $f(g_1 H) = H g_1^{-1}$ and $f(g_2 H) = H g_2^{-1}$. Then, since we have that $g_1 \equiv_\ell g_2 \bmod H \implies g_1^{-1} \equiv_r g_2^{-1} \bmod H \implies g_2^{-1} = h g_1^{-1}$ for some $h \in H \implies H g_2^{-1} = H g_1^{-1}$, we have what we want.

To find an inverse, consider $f^{-1}(Hg) = g^{-1} H$. Checking that this is well defined, we have that again,

$$g_1 \equiv_r g_2 \bmod H \implies g_1^{-1} \equiv_\ell g_2^{-1} \bmod H \implies f^{-1}(H g_1) = g_1^{-1} H = g_2^{-1} H = f^{-1}(H g_2)$$

as desired.

Then, we have that

$$f(f^{-1}(Hg)) = f(g^{-1} H) = H(g^{-1})^{-1} = Hg, f^{-1}(f(gH)) = f^{-1}(Hg^{-1}) = (g^{-1})^{-1} H = gH$$

as desired.

Problem 5

i

Put 1 as the identity. Then, $i_1(x) = 1(x)1^{-1} = (1x)1 = x1 = x = \mathrm{id}_G$, and clearly $\mathrm{id}_G \circ i_g = i_g \circ \mathrm{id}_G = i_g$.
Computing,

$$(i_{g_1} \circ i_{g_2})(x) = i_{g_1}(g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2)x(g_2^{-1}g_1^{-1}) = (g_1 g_2)x(g_1 g_2)^{-1}$$

ii

Explicitly, $i_g \circ i_{g^{-1}} = i_{gg^{-1}} = i_1 = \mathrm{id}_G$, so $(i_g)^{-1} = i_{g^{-1}}$.

iii

Since i_g admits an inverse, it is a bijection. Then,

$$i_g(xy) = gxyg^{-1} = g(x \cdot 1 \cdot y)g^{-1} = g(x(g^{-1}g)y)g^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$$

iv

($\implies$) Since G is abelian, $i_g(x) = gxg^{-1} = gg^{-1}x = 1x = x = \mathrm{id}_G$.
($\impliedby$) We have that for any $g_1, g_2 \in G$, $i_{g_2}(g_1) = g_2 g_1 g_2^{-1} = g_1$ since $i_{g_2} = \mathrm{id}_G$. Then, $g_2 g_1 g_2^{-1} = g_1 \implies g_2 g_1 = g_2 g_1 g_2^{-1} g_2 = g_1 g_2$, so G is abelian.

v

These statements both follow from the "beautiful formula", which gives that for $\sigma \in S_n$, $\rho = (a_1, \ldots, a_k)$,

$$i_\sigma(\rho) = \sigma\rho\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

which is another k-cycle. Now, if ρ is the product of r disjoint cycles (say $\rho = \prod_{i=1}^r \rho_i = \rho_1\rho_2\ldots\rho_r$ where ρ_i is a cycle of length k_i), we can induct on r. The earlier case shows what we want for $r = 1$. If it holds for r, then if $\rho = \prod_{i=1}^{r+1} \rho_i$,

$$i_\sigma(\rho) = i_\sigma\left(\prod_{i=1}^{r+1} \rho_i\right) = i_\sigma\left(\prod_{i=1}^{r} \rho_i \cdot \rho_{r+1}\right) = \left(\prod_{i=1}^{r} i_\sigma(\rho_i)\right) \cdot i_\sigma(\rho_{r+1})$$

from part iii. Then, by the inductive hypothesis, $(\prod_{i=1}^r i_\sigma(\rho_i))$ is the product of r disjoint cycles of lengths $k_1, \ldots, k_r$, and from the earlier case, $i_\sigma(\rho_{r+1})$ is a k_{r+1}-cycle. The only thing left is to show that all the cycles are disjoint. By the inductive hypothesis, all of the $i_\sigma(\rho_i)$ for $1 \le i \le r$ are disjoint.

Then, consider any ρ_i, $1 \le i \le r$. Then, if some element a is moved by both $i_\sigma(\rho_i)$ and $i_\sigma(\rho_{r+1})$, then by the earlier beautiful formula, $a = \sigma(a_i)$ and $a = \sigma(a_{r+1})$ for some a_i, a_{r+1} in the supports of ρ_i, ρ_{r+1} respectively. Since $\sigma(a_i) = \sigma(a_{r+1}) \implies a_i = a_{r+1}$ since $\sigma \in S_n$ is a bijection, then ρ_i, ρ_{r+1} are not disjoint, since they both move $a_i = a_{r+1}$. $\Rightarrow\Leftarrow$, so ρ_{r+1} is disjoint with any of the ρ_i, and combining with the inductive hypothesis, they are all disjoint, which finishes the induction and gives us what we want.

vi

We need closure, inverses, and the identity. Clearly $\mathrm{id}_G : G \to G$ is a bijection and $\mathrm{id}_G(xy) = xy = \mathrm{id}_G(x)\,\mathrm{id}_G(y)$, so $\mathrm{id}_G \in \operatorname{Aut} G$. Then, the composition of isomorphisms is itself an isomorphism (from a few classes ago), and so $f, g \in \operatorname{Aut} G \implies f \circ g$ takes $G \to G$, and is an isomorphism, so $f \circ g \in \operatorname{Aut} G$.

Inverses follow since any isomorphism admits an inverse that is itself an isomorphism, and so $f \in \operatorname{Aut} G \implies f^{-1} : G \to G$ is an isomorphism, so $f^{-1} \in \operatorname{Aut} G$.

vii

Directly computing,

$$F(g_1 g_2) = i_{g_1 g_2} = i_{g_1} \circ i_{g_2} = F(g_1)F(g_2)$$

where the middle equality comes from part i, so F is a homomorphism.

The kernel is the center of the group, i.e. any element that commutes with every other element. (This gives, for example, that the kernel of F when G is abelian is all of G, as shown above.) The center is defined by

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

but $gx = xg \iff gxg^{-1} = xgg^{-1} = x$. Then, if $i_g(x) = gxg^{-1} = x = \mathrm{id}_G(x)$ for all $x \in G$, we have that $g \in Z(G)$.

Problem 6

First, we compute the inverse:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \frac{1}{1-0} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

Then,

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}$$

but we have that $\sqrt{1^2 + 1^2} = \sqrt{2}$, so the columns are not orthonormal; thus, for $g = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in GL_2(\mathbb{R})$, and $h = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in O_2, SO_2$, we have that $ghg^{-1} \notin O_2, SO_2$, so $gHg^{-1} \not\subseteq H$, and thus O_2, SO_2 are not normal subgroups.

Problem 7

i

First, note that H is easily checked to be the group of all products between disjoint transpositions in S_4 and the identity. As a counting problem, there are $4 \cdot 3/2 = 6$ ways to pick the two pairs; since we discard the order of the transpositions since they commute when disjoint, this gives us $6/2 = 3$ distinct products at most, and we can see that H contains exactly 3 products that are distinct, so H must contain all products of disjoint transpositions in S_4.

Then part v of the earlier problem says that for any $\tau \in S_4$ (and thus for any $\tau \in A_4$) we have that $\tau\sigma\tau^{-1}$ for $\sigma = H$ is either the identity if $\sigma = 1$ (since $\tau \cdot 1 \cdot \tau^{-1} = \tau\tau^{-1} = 1$), or the product of two disjoint transpositions since the other elements of H are the product of two disjoint tranpositions, so $\tau\sigma\tau^{-1} \in H$ from above and $\tau H \tau^{-1} \subset H$, so H is normal.

ii

We have that $|A_4/H| = |A_4|/|H| = (4!/2)/4 = 3$, and $|S_4/H| = |S_4|/|H| = 4!/4 = 6$.

iii

We can directly compute here: clearly for the identity, $\tau \cdot 1 \cdot \tau^{-1} = 1 \in K$, so we are only concerned with $(1,2)(3,4)$. For $\tau \in H$, we compute all the possible $\tau \cdot (1,2)(3,4) \cdot \tau^{-1}$ with liberal use of the fact that $(a,b) = (b,a)$, $(a,b)(b,c) = (a,b,c)$, $(a,b,c)(c,d) =$

$(a,b)(b,c)(c,d) = (a,b,c,d)$, and $(a,b)(b,c,d) = (a,b)(b,c)(c,d) = (a,b,c,d)$:

$$\begin{aligned}
(1,2)(3,4)(1,2)(3,4)(3,4)(1,2) &= (1,2)(3,4)(1,2)(1,2) = (1,2)(3,4) \\
(1,3)(2,4)(1,2)(3,4)(2,4)(1,3) &= (1,3)(4,2,1)(3,4,2)(1,3) = (3,1,4,2)(4,2,3,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4) \\
(1,4)(2,3)(1,2)(3,4)(2,3)(1,4) &= (1,4)(3,2,1)(4,3,2)(1,4) = (4,1,3,2)(3,2,4,1) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4)
\end{aligned}$$

so $\tau\sigma\tau^{-1} \in K$ for $\sigma \in K$, $\tau \in H \implies \tau K \tau^{-1} \subseteq K$ and K is normal.

For A_4, consider that

$$(1,2,3)(1,2)(3,4)(3,2,1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1,4)(2,3) \neq (1,2)(3,4)$$

so for $\tau\sigma\tau^{-1} \notin K$, so K is not a normal subgroup of A_4.

Problem 8

i

Pick any element $x \in H \cap K$, and $g \in G$. Then, we need to show that $gxg^{-1} \in H \cap K$, but since $x \in H$, $gxg^{-1} \in H$ since H is normal, and similarly, $x \in K \implies gxg^{-1} \in K$ since K is normal, and so we get that $gxg^{-1} \in H \cap K$.

ii

We want that for any $x \in H \cap K$ and $g \in K$, that $gxg^{-1} \in H \cap K$. In particular, since $x \in H$, we have that $gxg^{-1} \in H$, and since $x \in K$ as well as $g \in K \implies g^{-1} \in K$, we have that $gxg^{-1} \in K$ as well. This gives that $gxg^{-1} \in H \cap K$.

iii

Since H, K are subgroups, we have that $1(k) = k \in HK$ for any $k \in K$, and similarly, that $h(1) = 1 \in HK$ for any $h \in H$, so HK contains both H and K. Note that this gives immediately that $1 \in HK$ as well.

For closure, consider the product $(h_1k_1)(h_2k_2)$. Since H is normal, the left coset k_1H is the same as the right coset Hk_1, and so $h_2k_2 = k_2h_2'$ for some $h_2' \in H$. Then,

$$(h_1k_1)(h_2k_2) = (h_1k_1)(k_2h_2') = h_1kh_2'$$

where $k = k_1k_2 \in K$ since K is a subgroup. Then, again, since H is normal, $kh_2' = h_2''k$ for some $h_2'' \in H$, so

$$h_1kh_2' = h_1h_2''k = hk$$

where $h = h_1h_2'' \in H$ since H is a subgroup. Then, we have that $(h_1k_1)(h_2k_2) \in HK$ as well. For inverses, consider that for any element hk, that $(hk)^{-1} = k^{-1}h^{-1}$, and since H is normal, $k^{-1}h^{-1} = h'k^{-1}$ for some $h \in H$, and so $k^{-1}h^{-1} \in HK$ as well, so we have what we want.