MATH 251: ABSTRACT ALGEBRA I
FINAL EXAM SOLUTIONS

Problem 1. For (a), we have simply ± 1. For (b), the elements of order 7 are $(x^{105/7})^k = x^{15k}$ with $k = 1, \ldots, 6$, so $x^{15}, x^{30}, \ldots, x^{90}$. For (c), no they are not isomorphic: $(\mathbb{Z}/16\mathbb{Z})^\times$ has at least 3 elements of order 2, namely, the classes of $-1, \pm 7$, and $\mathbb{Z}/8\mathbb{Z}$ as a cyclic group has only one, the class of 4. (They do have the same number of elements, since $\phi(16) = 8$.) For (d), we get $\rho = (1\ 4\ 5)(2\ 6\ 3)$ which is even.

Problem 2. For (a), the order of an element in S_n is equal to the least common multiple of the lengths of its cycles: the largest such lcm is $\operatorname{lcm}(5, 3, 2) = 30$ coming from the product of a 5-cycle, 3-cycle, and 2-cycle. For (b), we see that $1 \in H$ so $H \neq \emptyset$, and that if $x, y \in H$ then $(xy^{-1})^2 = x^2(y^{-1})^2 = x^2(y^2)^{-1} = 1$, since G is abelian. For the counterexample, take $G = S_n$ for $n > 2$: then G is generated by its transpositions, the elements of order 2, so in this case the subgroup generated by the elements of order 2 is all of G!

Problem 3. For (a), suppose $(ab)^n = 1$. Then $abab \cdots ab = 1$, repeated n times. Multiplying on the left by a^{-1} and the right by a, we obtain $baba \cdots ba = (ba)^n = 1$. Interchanging a, b, we see that $(ab)^n = 1$ if and only if $(ba)^n = 1$. Since the order of ab is the smallest such n, we conclude that ab and ba have the same order. (Even easier: $ab = b(ab)b^{-1}$, and conjugate elements have the same order.)

For (b), we compute

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

so $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_A(G)$ if and only if $a = d$ and $b = c$. We have $\det \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a^2 - b^2 = 0$ if and only if $a = \pm b$, so

$$C_G(A) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a \neq \pm b \right\} \subset G.$$

For (c), since $\mathbb{C}$ is a field, its only ideals are (0) and $\mathbb{C}$.

Problem 4. For (a), we have $\operatorname{Inn}(D_8) = D_8/Z(D_8) = D_8/\langle r^2 \rangle \cong V_4$, which is abelian.

For (b), we show that I is a subgroup of $\mathrm{M}_2(R)$ which is closed under left multiplication by R. Since the zero matrix is in I, we have $I \neq \emptyset$, and if $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \begin{pmatrix} a' & 0 \\ b' & 0 \end{pmatrix} \in I$ then

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} a' & 0 \\ b' & 0 \end{pmatrix} = \begin{pmatrix} a - a' & 0 \\ b - b' & 0 \end{pmatrix} \in I.$$

And if $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{M}_2(R)$ and $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in I$ then

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax + by & 0 \\ az + bw & 0 \end{pmatrix} \in I.$$

No, it is not a two-sided ideal, since multiplication on the right gives

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax & ay \\ bx & bw \end{pmatrix} \notin I.$$

Problem 5. First (a). By definition, we have $\phi(1) = 1$ and $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$, so ϕ satisfies the properties of a group homomorphism on $R^\times$. So we need to show that $\phi(R^\times) \subseteq S^\times$ and that ϕ is bijective onto $S^\times$. For the first, suppose that $x \in R^\times$. Then there exists $y \in R^\times$ such that $xy = yx = 1$. Thus $\phi(xy) = \phi(x)\phi(y) = \phi(1) = 1$ and similarly $\phi(y)\phi(x) = 1$, so by definition, $\phi(x) \in S^\times$, thus proving the first claim. Now we consider ϕ^{-1}: it is an isomorphism $\phi^{-1} : S \to R$, so by the same argument,

Date: 16 December 2011.

$\phi^{-1}(S^\times) \subseteq R^\times$, hence $S^\times \subseteq \phi(R^\times)$, so equality holds. The restriction of a bijection is a bijection onto its image, so $\phi : R^\times \to S^\times$ is a bijection.

Now (b). We have $450 = 2 \cdot 3^2 \cdot 5^2$. The elementary divisors and invariant factors are

$$(2, 3^2, 5^2) \cong (450),\ (2, 3, 3, 5^2) \cong (150, 3),\ (2, 3^2, 5, 5) \cong (90, 5),\ (2, 3, 3, 5, 5) \cong (30, 15).$$

Problem 6. For (a), the answer is no. Consider $R = \mathbb{Z}$ and $I = (4) = 4\mathbb{Z}$. Then R is an integral domain, but $R/I = \mathbb{Z}/4\mathbb{Z}$ is not an integral domain, since $2 \cdot 2 \equiv 0 \pmod 4$.

For (b), we take $(2 + 3i)(2 - 3i) = 2^2 + 3^2 = 13 = 0 \in \mathbb{Z}/13\mathbb{Z}[i]$, so $2 + 3i$ is a zero divisor.

Problem 7. G/N is abelian if and only if $(aN)(bN) = (bN)(aN)$ for all $aN, bN \in G/N$ if and only if $abN = baN$ for all $a, b \in G$ if and only if $Nab = Nba$ iff $Naba^{-1}b^{-1} = N$ if and only if $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

Problem 8. First, part (a). By Sylow's theorem, the number n_7 of Sylow 7-subgroups, necessarily of order $7 \parallel 42$, divides 6 and is congruent to 1 mod 7, so $n_7 = 1$, and therefore this unique Sylow 7-subgroup H is normal. That's a good start!

Now suppose $H \subseteq Z(G)$; then G/H maps surjectively to $G/Z(G)$, and since $\#G/H = 6$, we have either $G/H \cong Z_6$ or $G/H \cong S_3$. Since G/H is abelian, we have $G/H \cong Z_6$. Then $G/Z(G)$ is the quotient of a cyclic group, and hence cyclic; thus G itself is abelian by that wonderful proposition.

Now part (b). By Sylow's theorem again, we have $n_3 = 1, 7$, $n_5 = 1, 21$, and $n_7 = 1, 15$. If $n_7 = 15$, then there are $15(7 - 1) = 90$ elements of order 7, and if $n_5 = 21$, then there are $21(5 - 1) = 84$ elements of order 5, since $90 + 84 = 174 > 105$, we cannot have both of these occurring. If you got this far, great!

Suppose that $n_5 = 21$; then $n_7 = 1$. So there is a normal 7-Sylow subgroup N. Consider G/N, a group of order 15. Sylow's theorem now says that G/N has a unique subgroup K of order 5. And if $x \in G$ is an element of order 5, then $x \notin N$ since N has order 7, so $xN \in G/N$ has order 5. The preimage of K is KN which has (at most) $5 \cdot 7 = 35$ elements. But any element of order 5 must belong to this pre image, and yet there are 84 elements of order 5. This is a contradiction. Similarly, one obtains a contradiction from $n_7 = 15$ and $n_5 = 1$.

Problem 9. We map

$$\begin{aligned} \phi : G = \langle x, y, z : x^2 = y^3 = z^3 = xyz = 1 \rangle &\xrightarrow{\sim} A_4 \\ x &\mapsto (1\ 2)(3\ 4) \\ y &\mapsto (2\ 3\ 4) \\ z &\mapsto (1\ 2\ 3). \end{aligned}$$

Then we have $\phi(x)^2 = \phi(y)^3 = \phi(z)^3 = 1$ and $\phi(xyz) = (1\ 2)(3\ 4)(2\ 3\ 4)(1\ 2\ 3) = 1$, so this gives a homomorphism $G \to A_4$. Since $\#G = \#A_4 = 12$, this is an isomorphism.

Problem 10. First, (a). We know $N = H \cap K$ is a subgroup of H (or K). Since $\#H = p^2$, by Lagrange we have $\#N \mid p^2$ so $\#N = 1, p, p^2$. If $\#N = p^2$ then $N = H \cap K = H$ so $H = K$, impossible. So suppose $\#N = 1$—we will obtain a contradiction by showing there are too many elements in G. Consider the set of elements $HK = \{hk : h \in H, k \in K\}$. We claim there are $p^2 \cdot p^2 = p^4$ elements in HK; for this, we just need to show they are all distinct. Indeed, if $h_1k_1 = h_2k_2$ then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$, so $h_1 = h_2$ and $k_1 = k_2$. Since $p^4 > p^3 > p^2q = \#G$, we have a contradiction.

Finally for (b), let $g \in G$ and consider gNg^{-1}. By the same argument as above, if $H \cap gNg^{-1} = \{1\}$, then there are $p^2 \cdot p = p^3 > p^2q = \#G$ elements in G, a contradiction. But gNg^{-1} is a group of order p, so the only other alternative is that $H \cap gNg^{-1} = gNg^{-1}$, i.e., $gNg^{-1} \subseteq H$. Similarly, $gNg^{-1} \subseteq K$, so $gNg^{-1} \subseteq N$. Thus N is normal.

There was a typo in this problem: it should have read $p^2 > q$, not $p > q$. By Sylow's theorem, we have $n_p \mid q$ and $n_p \equiv 1 \pmod p$, so if $n_p \neq 1$ then $n_p > p > q$, a contradiction. Thus $n_p = 1$ and the configuration above is impossible! But with the corrected hypothesis, the same proof in (a) works; to prove (b), note that G is generated by H and K (the subgroup generated by H and K has order a multiple of p^2, has order $> p^2$, and divides p^2q), but N is normal in H and K (since H and K have order p^2, they are abelian) so the normalizer $N_G(N)$ contains H and K so is equal to G, which means $N \trianglelefteq G$.