Basic Algebra 1
Solutions to Assignment 5

November 22, 2013

Question 1 For $a, b, c, d \in \mathbb{Z}$ let $z = a + ib$ and $w = c + id$ be Guassian integers, then in particular z and w are complex numbers and we can divide z by w as a complex number to get

$$\begin{aligned} z/w &= \frac{a+ib}{c+id} \\ &= \frac{a+ib}{c+id}\frac{c-id}{c-id} \\ &= \frac{(a+ib)(c-id)}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2} \\ &= \alpha + i\beta \end{aligned}$$

Now take q_1 to be the closest integer to α and q_2 the closest integer to β. Then we have $|q_1 - \alpha| \leq 1/2$ and $|q_2 - \beta| \leq 1/2$

$$\begin{aligned} |r| &= |z - qw| \\ &= |w(z/w - q)| \\ &= |w((\alpha - q_1) + i(\beta - q_2))| \\ &= |w||(\alpha - q_1) + i(\beta - q_2)| \\ &= |w|((\alpha - q_1)^2 + (\beta - q_2)^2) \\ &\leq |w|((1/2)^2 + (1/2)^2) \\ &< |w| \end{aligned}$$

as desired.

Note that, we are using the fact that the norm function is multiplicative:

$$\begin{aligned} |z_1 z_2| &= (z_1 z_2)(\overline{z_1 z_2}) \\ &= z_1 z_2 \overline{z_1}\,\overline{z_2} \\ &= (z_1\overline{z_1})(z_2\overline{z_2}) \\ &= |z_1||z_2| \end{aligned}$$

Question 2 Take I to be an ideal in $R = \mathbb{Z}[i]$. Now take $S = \{|z| \mid z \in I, z \neq 0\}$, then S is a subset of $\mathbb{N}$.

If I is the zero ideal, then I is generated by 0 and there is nothing to prove. So we assume that $I \neq 0$ which implies that S is non-empty.

Now by the well-ordering principle (which states that every non-empty subset of $\mathbb{N}$ has a minimal element,) S has a minimal element, say $|d|$. So d is the nonzero element in our ideal I with least norm. We will show that the ideal I is generated by d. Since d is an element of I, the ideal generated by d is included inside I. We need to prove the converse;

Take an arbitrary element $z \in I$. then by question 1, we have q and r in $\mathbb{Z}[i]$, such that

$$z = dq + r \qquad |r| < |d|.$$

But since $z \in I$ and $d \in I$, which implies that $dq \in I$, we have

$$r = z - dq \in I.$$

If $r \neq 0$, then $|r|$ is a natural number in S and has norm less than that of d, which is a contradiction! So $r = 0$ and $z = dq$. In other words, $z \in (d)$, the ideal generated by d.

This proves that $I \subset (d)$, and hence we have equality, $I = (d)$.

Question 3 As suggested by the hint, take $I = (p, t + i) \subset \mathbb{Z}[i] = R$, where $t = (2m)!$. Note that we have $t^2 + 1 \equiv 0 \bmod p$, as we have seen in assignment 3, question 4. By the previous question, I is generated by one element, say $d = a + ib$, in R. We will show that $p = |d| = a^2 + b^2$. Remember a and b are integers.

We have $p, t + i \in I = (d)$, so we can write

$$d|p \qquad d|t + i \tag{1}$$

which implies that

$$|d| \mid |p| = p^2 \tag{2}$$

$$|d| \mid |t + i| = (t + i)(t - i) = t^2 + 1 \equiv 0. \tag{3}$$

(2) implies that $|d|$ is 1, p or p^2. But if $|d| = d\overline{d} = 1$ then d is a unit in R, in which case I would be the whole ring, R. But we have:

Claim $1 \notin I$.

Proof: if $1 \in I$, then $1 = p(r+is)+(t+i)(u+iv) = (pr+tu-v)+i(ps+tv+u)$ which implies

$$1 = pr + tu - v$$
$$0 = ps + tv + u.$$

But if these equations have a solution with $r.s, u, v \in \mathbb{Z}$, then the equations hold modulo p, so we should have

$$1 \equiv tu - v \tag{4}$$
$$0 \equiv tv + u. \tag{5}$$

Multiplying the first equation by t and adding it to the second we get

$$t \equiv t^2u + u = (t^2 + 1)u \equiv 0,$$

where the latter equality holds because we know $t^2 + 1 \equiv 0$. But this is a contradiction since t is not divisible by p.

So d cannot have norm 1. But it also can not have norm p^2 as if it did, we would have $p = dd'$ with $|d'| = 1$. So d' would be a unit and p and d would be associate. This implies that $p \mid t + i$, as $d \mid t + i$, by (1). But for p to divide $t + i, p$ should divide t and 1, neither of which is true.

So the only possibility left for $|d|$ is p and we have $a^2 + b^2 = |d| = p$, and p is a sum of two squares.

Question 4 First we observe that ϕ sends the additive (resp. multiplicative) identity in R to the additive (resp. multiplicative) identity in $\mathbb{Z}/p\mathbb{Z}$;

$$\phi(0) = \phi(0 + 0i) = [0 - 0t]_p = [0]_p$$
$$\phi(1) = \phi(1 + 0i) = [1 - 0t]_p = [1]_p.$$

Next, we check that it respects addition and multiplication:

$$\begin{aligned}\phi((a + bi) + (c + di)) &= \phi((a + c) + (b + d)i) \\ &= [(a + c) - (b + d)t]_p \\ &= [a - bt]_p + [c - dt]_p \\ &= \phi(a + bi) + \phi(c + di),\end{aligned}$$

and

$$\begin{aligned}\phi((a + bi)(c + di)) &= \phi((ac - bd) + (ad + bc)i) \\ &= [(ac - bd) - (ad + bc)t]_p \\ &= [(ac + bdt^2) - (ad + bc)t]_p \\ &= [(a - bt)(c - dt)]_p \\ &= [a - bt]_p[c - dt]_p \\ &= \phi(a + bi)\phi(c + di).\end{aligned}$$

So ϕ is a homomorphism. Now we compute its kernel; take $a + bi \in ker(\phi)$. We have

$$[0]_p = \phi(a + bi) = [a - bt]_p.$$

So $a - bt = pk$. Now we can write

$$a + bi = a - bt + bt + bi = (a - bt) + b(t + i) = pk + b(t + i) \in I,$$

so $ker(\phi) \subset I$. Conversely, we have

$$\begin{aligned} \phi(p) = \phi(p + 0i) = [p - 0t]_p = [0]_p \\ \phi(t + i) = [t - t]_p = [0]_p \end{aligned}$$

and so $I \subset ker(\phi)$, and hence we have the equality $I = ker(\phi)$.

Further, note that $[n]_p = \phi(n+0i)$ for all $[n]_p \in \mathbb{Z}/p\mathbb{Z}$. Hence ϕ is surjective.

Now by the (first) Isomorphism Theorem, we have

$$R/I \cong \mathbb{Z}/p\mathbb{Z}.$$

Question 5

Claim A 2×2 matrix is invertible, if and only if its rows are linearly independent.

Proof: First we have $det \begin{pmatrix} a & b \\ \lambda a & \lambda b \end{pmatrix} = a\lambda b - b\lambda a = 0$. And $det \begin{pmatrix} \lambda a & \lambda b \\ a & b \end{pmatrix} = \lambda ab - \lambda ba = 0$. So if a matrix has linearly dependent rows, then it's not invertible.

Conversely, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/p\mathbb{Z}$ is not invertible, then $ad - bc = 0$. If $(a, b) = (0, 0)$ then rows of A are linearly dependent and there is nothing to prove. If not, then assume $a \neq 0$, (the case $b \neq 0$ is similar.) We have $d = bc/a$ and taking $\lambda = c/a \in F$ we have $(c, d) = (ac/a, bc/a) = \lambda(a, b)$ and hence rows of A are linearly dependent.

This proves the claim.

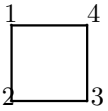
Now we can use the claim to count the elements in $GL_2(F)$;

First we have $p^2 - 1$ possibility for the first row, since (a, b) can be anything (p choices for each a and b,) except for $(0, 0)$.

After we have chosen the first row, the second row can be anything (p^2 choices) except for any multiple of (a, b). But there are p multiples $\lambda(a, b)$ as λ runs over all elements of F. So for the second row we have $p^2 - p$ choices.

So overall, cardinality of $GL_2(F)$ would be $(p^2 - 1)(p^2 - p)$.

Question 6 We have $D_8 = \{1, r, r^2, r^3, V, H, D_1, D_2\}$. Considering the following labeling of vertices of the square



D_8 can be realised as a subgroup of S_4 by looking at how it permutes the vertices. So we have

$$\begin{aligned} r &= (1,2,3,4) \\ r^2 &= (1,3)(2,4) \\ r^3 &= (1,4,3,2) \\ V &= (1,4)(2,3) \\ H &= (1,2)(3,4) \\ D_1 &= (2,4) \\ &\quad \text{reflection with respect to the diagonal passing through (1)} \\ D_2 &= ((1,3) \\ &\quad \text{reflection with respect to the diagonal passing through (2).} \end{aligned}$$

So, since r, r^3, D_1 and D_2 are cycles, their order is equal to their length. In particular, D_1 and D_2 are of order 2. The identity has order one. And the other three elements are each composition of two cycles of length two , and so their order is $lcm(2,2) = 2$. So the set of elements of order 2 in D_8 is $\{r^2, V, H, D_1, D_2\}$.

Now we consider Q_8; We have $ord(1) = 1$ and $ord(-1) = 2$ and $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1$ so $ord(\pm i) = ord(\pm j) = ord(\pm k) = 4$. So the only element of order 2 is -1.

Now we use this to show that the two groups are not isomorphic.

Claim If $f : G \to H$ is an isomorphism of groups, and $g \in G$ then $ord(g) = ord(f(g))$.

Proof: $g^n = e_G$ if and only if $(f(g))^n = f(g^n) = e_H$, since f is a group homomorphism (only if part) and is injective (if part.) So for all $n < ord(g)$ we have $(f(g))^n \neq 0$ as $g^n \neq 0$. And $f(g)^{ord(g)} = f(g^{ord(g)}) = f(e_G) = e_H$. And hence $ord(g)$ is the smallest integer, d, such that $(f(g))^d = e_H$.

So if we have an isomorphism from D_8 to Q_8, it should send elements of order 2 in D_8 to element(s) of order 2 in Q_8. But there are 5 elements of order 2 in the former and only one in the latter, and this contradicts injectivity of the isomorphism.

Question 7 As suggested by the hint, we look at the action of $GL_2(F)$ ($F = \mathbb{Z}/2\mathbb{Z}$) on the set of three elements $\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$ of nonzero column vectors in F^2. We label the elements of this set $\{1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$ (any ordering would do,) Now any element $A \in GL_2(F)$ permutes this set since an invertible matrix gives a linear map $F^2 \to F^2$ which is

invertible and so sends the zero vector to the zero vector and permutes the other three vectors. This gives a map $\phi : GL_2(F) \to S_3$ which is a homomorphism as it sends the identity matrix to the trivial permutation and multiple of two matrices correspond to composition of the maps they induce on F^2. Now we show ϕ is bijective; if a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $ker(\phi)$ then

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

and

$$\begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

and so A is the identity matrix. To show ϕ is surjective, take any permutation $\sigma \in S_3$ let

$$\sigma(1) = \begin{pmatrix} a \\ c \end{pmatrix}$$

and

$$\sigma(2) = \begin{pmatrix} b \\ d \end{pmatrix}$$

and take

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then A is an invertible matrix since its columns are nonzero and not equal, σ being a permutation (remember that scalars here are just 0 and 1 and so two nonzero columns are linearly dependant if and if they are equal.) And $\phi(A) = \sigma$.

This proves that ϕ is an isomorphism of groups, as desired.

Question 8 Let $F = \mathbb{Z}/3\mathbb{Z}$.

We first show that for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F)$ the map $\sigma_A : P \to P$ which sends $j \in P$ to $\frac{aj+b}{cj+d}$ is a permutation, i.e. it's a bijective map on P. Since P is finite, it suffices to show σ_A is injective, and surjectivity will automatically follow. So assume $\sigma_A(j) = \sigma_A(k)$ for $j, k \in P$. Then we have

$$\begin{aligned} \frac{aj+b}{cj+d} &= \frac{ak+b}{ck+d} \\ (aj+b)(ck+d) &= (ak+b)(cj+d) \\ acjk + adj + bck + bd &= acjk + adk + bcj + bd \\ 0 &= (ad-bc)(k-j) \end{aligned}$$

now since A is invertible, its determinant $ad - bc$ is nonzero and the above equality implies $j = k$. So we have a map $\phi : GL_2(F) \to S_P$. We now show

this map is a homomorphism. First it sends the identity matrix to the trivial permutation, as for any $j \in P$

$$\phi(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})(j) = \frac{1*j+0}{0*j+1} = j.$$

Second, we should show multiple of two matrices is send to composition of their images, under ϕ. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Then $AB = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & ab'+dd' \end{pmatrix}$, and for any $j \in P$

$$\begin{aligned}
\phi(AB)(j) &= \frac{(aa'+bc')j + ab' + bd'}{(aa'+bc')j + ab' + dd'} \\
&= \frac{a(a'j+b') + b(c'j+d')}{c(a'j+b') + d(c'j+d')} \\
&= \frac{a\frac{a'j+b'}{c'j+d'} + b}{c\frac{a'j+b'}{c'j+d'} + d} \\
&= \frac{a[\phi(B)(j)] + b}{c[\phi(B)(j)] + d} \\
&= \phi(A)(\phi(B)(j)).
\end{aligned}$$

So ϕ is a homomorphism of groups.

Next, we compute the kernel. Assume $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in the kernel, then $\phi(A)$ is the trivial permutation and we have $\frac{aj+b}{cj+d} = j$ for all $j \in P$. Plugging in different values for j in this equation we get

$$\begin{aligned}
j = 0 &\implies b = 0 \\
j = \infty &\implies a/c = \infty \implies c = 0 \\
j = 1 &\implies a = d \\
j = 2 &\implies 2a = 2d
\end{aligned}$$

so A is a (nonzero) multiple of the identity matrix

$$ker(\phi) = \{Id, 2*Id\}.$$

Now we have a group homomorphism from a group of order 48 (refer to question 5) to a group of order 24, and the kernel has 2 elements. The image of ϕ is a subgroup of S_4 (and hence of cardinality dividing 24) which is, by Isomorphism Theorem, isomorphic to $GL_2(F)/ker(\phi)$. But the latter group has cardinality $48/2 = 24$ and so $Im(\phi)$ has cardinality 24 and hence is the whole group S_4.

Question 9 To show a subset of a group is a subgroup we need to check it contains the identity element and it's closed under multiplication and that it contains inverses of its elements; paragraph$e_g \in Z(S)$ Since the identity element in G commutes with every element of G ($e_G g = g e_G = g$) it, in particular, commutes with all elements in S and is, hence, in $Z(S)$.

$Z(S)$ is closed under multiplication If $g, h \in Z(S)$ then for every $s \in S$ we have

$$gs = sg$$
$$hs = sh.$$

So for all $s \in S$ we have

$$s(gh) = (sg)h = (gs)h = g(sh) = g(hs) = (gh)s$$

and so gh is in $Z(S)$. Now we show $a = g^{-1}s$ is equal to $b = sg^{-1}$

$$\begin{aligned} ga = g(sg^{-1}) &= (gs)g^{-1} \\ &= (sg)g^{-1} \\ &= s(gg^{-1}) \\ &= s = (gg^{-1})s \\ &= g(g^{-1}s) = gb \end{aligned}$$

so $ga = gb$ and multiplying both sides by g^{-1} from left, we get $a = b$, as desired.

Question 9 First we observe that for every element $a \in H$ and $g \in G$ $a^{g^{-1}} \in H$ y definition of a normal subgroup. So for $a \in H$ conjugacy class of a, $[a] = \{gag^{-1} \mid g \in G\}$ is a subset of H.

Now we show for $a, b \in H$, $[a]$ and $[b]$ are either disjoint or equal;

Assume $[a] \cap [b]$ is not empty so we have

$$g_1 a g_1^{-1} = g_2 b g_2^{-1},$$

then

$$a = g_1^{-1} g_2 b g_2^{-1} g_1 = gbg^{-1}$$

for $g = g_1^{-1} g_2$.

Then we show that every conjugate of a is in $[b]$ and every conjugate of b is in $[a]$. Take $h \in G$,

$$\begin{aligned} hah^{-1} &= h(gbg^{-1})h^{-1} \\ &= (hg)b(hg)^{-1} \in [b] \end{aligned}$$

and

$$\begin{aligned} hbh^{-1} &= h(g^{-1}bg^{)}h^{-1} \\ &= (hg^{-1})b(hg^{-1})^{-1} \in [a] \end{aligned}$$

and so $[a] = [b]$.

Hence H can be written as a disjoint union of it's conjugacy classes.

Now take $G = S_n$. First we have the following general facts. Any element in G is a product of disjoint cycles, and if $\sigma \in G$ is any permutation and $\tau = (i_1, \ldots, i_t)$ a cycle of length t then $\sigma\tau\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_t))$, is a cycle of the same length.

And for τ_1 and τ_2 two (disjoint) cycles, we have $\sigma(\tau_1\tau_2)\sigma^{-1} = (\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1})$. And so conjugating multiple of (disjoint) cycles result in a multiple of cycles of the same length.

Further any two cycles of the same length $\tau_1 = (i_1, \ldots, i_t)$ and $\tau_2 = (j_1, \ldots, j_t)$ are conjugate: for $\sigma = \begin{pmatrix} i_1 & \cdots & i_t \\ j_1 & \cdots & j_t \end{pmatrix}$ we have $\tau_2 = \sigma\tau_1\sigma^{-1}$.

Let $n = 4$; then $G = \{Id, (i,j), (i,j,k) = (i,k)(i,j), (i,j,k,l) = (i,l)(i,k)(i,j), (i,j)(k,l) \mid i,j,k,l$ different elements in$\{1,2,3,4\}\}$, and by what we said above conjugacy classes of G are $Id, [(i,j)]$ = set of all 2-cycles, $[(i,j,k)]$ = set of all 3-cycles, $[(i,j,k,l])$ = set of all 4-cycles, $[(i,j)(k,l)]$ = set of all multiples of two disjoint 2-cycles.

Now from this we can see that normal subgroups of G are $\{Id\}, K = \{Id\} \cup [(i,j)(k.l)], A_4 =$ set of even permutations, S_4, since

1.if a subgroup contains the conjugacy class of 2-cycles, it will contain the whole group as everything is generated by 2-cycles

2.if a subgroup contains conjugacy class of multiple of two 2-cycles and nothing else, then it's the Klein subgroup K. If it contains conjugacy class of 3-cycles then it's A_4. If it contains any of the odd conjugacy classes then it's S_4.

3.if it contains the conjugacy class of 3-cycles, then it will contain $[(i,j)(k,l)]$ so it will either be A_4 or S_4.

4.if it contains the 4-cycles, then since a 4-cycle multiplied by itself is multiple of 20cycles, the subgroup will contain $[(i,j)(k,l)]$ and hence will be S_4.

Now if $n = 5$, conjugacy classes are identity, 2-cycles, 3-cycles, 4-cycles, 5-cycles, $[(i,j)((k,l)$ =multiples of two disjoint 2-cycls and $[i,j)(k,l,m)]$ = multiples of a 2-cycle and a 3-cycle. Normal subgroups are$\{Id\}, A_5$ and S_5.