Math 122 Midterm 2 Fall 2014 Solutions

Common mistakes

i. Groups of order pq are *not* always cyclic. Look back on Homework Eight. Also consider the dihedral groups D_{2n} for n an odd prime.

ii. If $H \subset G$ and H is abelian, it is *not* true that H is necessarily normal. Every subgroup of an *abelian* G is normal, but a subgroup's "abelianness" does not inform you of its normalcy. Consider for instance the subgroup $H \subset S_n$ generated by (123). H is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ so is abelian, but is not normal in S_n unless $n = 3$.

iii. Along these lines: Being normal is not some absolute property of a group. For example, any group H is normal inside itself—$H \triangleleft H$. But if H can be realized as a subgroup of G, it is not necessarily true that $H \triangleleft G$! Likewise, homomorphisms do not "preserve normal subgroups" — i.e., a homomorphism $G_1 \to G_2$ need not send a normal subgroup of G_1 to a normal subgroup of G_2. This is true, however, in special cases, and also when the homomorphism is a surjection.

iv. If $G_1 \triangleleft G_2$ and $G_2 \triangleleft G_3$, it is *not* necessarily true that $G_1 \triangleleft G_3$. Consider for instance

$$G_1 = \{1, (12)(34)\}, \qquad G_2 = \{1, (12)(34), (13)(24), (14)(23)\}, \qquad G_3 = A_4.$$

Then G_1 is *not* normal in G_3—try conjugating by (123).

v. The Klein four-group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So you shouldn't say that "the" Klein 4-group is the normal, order 4 subgroup of A_4. Rather, there exists a subgroup of A_4 isomorphic to the Klein 4-group, and this subgroup happens to be normal in A_4.

vi. For a commutative ring R, the notation $R^\times$ is *not* equal to $R - \{0\}$. Though we haven't used this notation much, $R^\times$ is the notation for the *units* of R. So if R isn't a field, $R^\times \neq R - \{0\}$.

vii. Some people wrote $G/\ker\phi = \operatorname{image}\phi$. This isn't correct–the two groups are not equal, they are *isomorphic*. Just as when there is a bijection between two sets, it usually does not mean the two sets are equal. As an example—a set of five bananas is not equal to a set of five apples. But the two sets are in bijection.

viii. In the problem about showing G/K is solvable if G is—if $G_0 \subset \ldots \subset G_n$ is a sequence showing G is solvable, the groups G_i/K might not make any sense, because K may not be a subgroup of G_i!

1. Irreducibility

Let F be a field. For any $x \in F$, note that there is a function

$$F[t] \to F,$$

called *evaluation at* x. Explicitly, if $f = a_d t^d + \dots a_1 t + a_0$ is a polynomial, we send f to

$$f(x) = a_d x^d + \dots a_1 x + a_0 \in F.$$

Here, by x^d, we mean of course the element of F obtained by multiplying x with itself d times.

(a) Show that for any $x \in F$, evaluation at x is a ring homomorphism.

If $f(t) = 1$, then $f(x) = 1$. Further, $(f+g)(x) = \sum (a_i + b_i)x^i = \sum a_i x^i + \sum b_i x^i = f(x) + g(x)$. Finally, $fg(x) = \sum_{i+j=k} a_i b_j x^k = (\sum_i a_i x^i)(\sum_j b_j x^j) = f(x)g(x)$.

(b) Show that f can be factored by a linear polynomial if and only if there is some $x \in F$ for which $f(x) = 0$. (Hint: Use the division algorithm and induct on degree.)

We showed this in class. See Lecture 33.

Recall that a polynomial $f(t) \in F[t]$ is *irreducible* if the only polynomials dividing $f(t)$ are degree 0 (i.e., are constants) or have degree equal to f.

(c) If $F = \mathbb{C}$, show that $f(t) = t^2 + 1$ is not irreducible.

The element $x = \sqrt{-1}$ satisfies this polynomial—$f(\sqrt{-1}) = -1 + 1 = 0$. Hence by above, f is not irreducible.

(d) If $F = \mathbb{R}$, show that $f(t) = t^2 + 1$ *is* irreducible. (Hint: If $f(t) = g(t)h(t)$, what can you say about the degrees of g and h? And what does that say about solutions to $f(t)$?)

If f can be factored into non-units, then both g and h in the hint must be degree one polynomials. Hence by (b), there must be some real number such that $x^2 + 1 = 0$. However, for real numbers, x^2 is always non-negative, so this is impossible.

(e) For each of the primes $p = 2, 3, 5, 7$, indicate which of the following polynomials has a solution in $\mathbb{Z}/p\mathbb{Z}$. (You'll need to just compute.)

(a) $t^2 + \bar{1}$ (i.e., which of these finite fields has a square root to -1?)

We can just compute values of x^2 in each field:

$x \backslash p$	2	3	5	7
1	1	1	1	1
2	–	1	4	4
3	–	–	4	2
4	–	–	1	2
5	–	–	–	4
6	–	–	–	1

of these, only $p = 2$ and $p = 5$ has -1 appearing: For instance, $2^2 = 3^2 = 4 = -1 \in \mathbb{Z}/5\mathbb{Z}$. Explicitly, one can also factor the polynomial as below:

$$t^2 + 1 = (t+1)(t+1)$$

in $\mathbb{Z}/2\mathbb{Z}$, and

$$t^2 + 1 = (t-3)(t-2)$$

in $\mathbb{Z}/5\mathbb{Z}$.

(b) $t^3 - \overline{2}$ (i.e., which of these fields has a cube root to 2?)
We can just compute values of x^3 in each field:

$x \backslash p$	2	3	5	7
1	1	1	1	1
2	–	2	3	1
3	–	–	2	6
4	–	–	4	1
5	–	–	–	6
6	–	–	–	6

of these, only $p = 3$ and $p = 5$ has 2 appearing: Namely, $2^3 = 3^2 = 4 = -1 \in \mathbb{Z}/5\mathbb{Z}$. Also note that $t^3 - 2$ factors in $\mathbb{Z}/2\mathbb{Z}$, since $x = 0$ is a root. Explicitly, we have the following factorizations:

$$t^3 - 2 = t^3 = t \cdot t \cdot t \qquad \text{in } \mathbb{Z}/2\mathbb{Z}.$$

$$t^3 - 2 = (t-2)(t^2 + 2t + 1) = (t+1)^3 \qquad \text{in } \mathbb{Z}/3\mathbb{Z}.$$

$$t^3 - 2 = (t-3)(t^2 + 3t + 4) \qquad \text{in } \mathbb{Z}/5\mathbb{Z}.$$

(c) t^2+t+1 (i.e., for which of these fields does this polynomial factor?)
We can just compute values of $x^2 + x + 1$ in each field:

$x \backslash p$	2	3	5	7
1	1	0	3	3
2	–	1	2	0
3	–	–	3	6
4	–	–	1	0
5	–	–	–	3
6	–	–	–	1

of these, only $p = 3$ and $p = 7$ has 0 appearing. We have explicit factorizations:

$$t^2 + t + 1 = (t-1)^2 \qquad \text{in } \mathbb{Z}/3\mathbb{Z}.$$

$$t^2 + t + 1 = (t-2)(t-4) \qquad \text{in } \mathbb{Z}/7\mathbb{Z}.$$

2. Principal ideal domains

Let R be an integral domain. We call R a *principal ideal domain* if every ideal $I \subset R$ is equal to (x) for some $x \in R$. That is, every ideal is generated by a single element.

(a) Show that $\mathbb{Z}$ is a principal ideal domain. (We've done this in class, so you can do it, too!)

See class notes. Any subgroup of $\mathbb{Z}$ is equal to $(n) = n\mathbb{Z}$, so in particular, any ideal must also be generated by some single element N.

(b) Let F be a field. Show that $F[t]$ is a principal ideal domain. (Hint: If $I \neq (0)$, let n be the least degree for which a degree n polynomial is in I. If $p(t)$ and $q(t)$ are both degree n polynomials, how are they related? Finally, given any $f(t) \in I$, what happens when you divide $f(t)$ by $p(t)$ and look at the remainder?)

Following the hint: Let n be the smallest degree among non-zero elements in I. Let $p(t)$ be a polynomial in I of degree n. If you divide any $f(t) \in I$ by $p(t)$, the division algorithm tells us that we end up with polynomial of degree less than n—but then we have that

$$f(t) = p(t) \cdot g(t) + r(t), \qquad \deg r(t) < n$$

while

$$r(t) = f(t) - p(t)g(t)$$

must be in I by definition of ideal. This means that $r(t)$ must be zero, or that every polynomial $f(t) \in I$ is divisible by p. Hence $I = (p(t))$. (The hint about $p(t)$ and $q(t)$ to be equal-degree polynomials was unnecessary.)

3. The second isomorphism theorem

Fix a group G. Let $S \subset G$ be a subgroup, and $N \triangleleft G$ be a normal subgroup.

(a) Let SN be the set of all elements in G of the form sx where $s \in S$ and $x \in N$. Show this is a subgroup of G.

Given $s_1, s_2 \in S$ and $x_1, x_2 \in N$, we have that

$$s_1 x_1 s_2 x_2 = s_1 s_2 s_2^{-1} x_1 s_2 x_2 = s_1 s_2 x' x_2$$

for some $x' \in N$ (since N is normal). And $s_1 s_2 \in S$ and $x' x_2 \in N$ since both are closed under multiplication. The identity is in SN since $1 \in S, N$ and $1 \cdot 1 = 1$. Finally, SN contains inverses because

$$x^{-1} s^{-1} = (s^{-1} x' s) s^{-1} = s^{-1} x'$$

where $x' \in N$ is the element such that $x' = s x^{-1} s^{-1}$.

(b) Show that N is a normal subgroup of SN.

We know $gxg^{-1} \in N$ for every $g \in G$ and $x \in N$. Since $SN \subset G$, we in particular have that $gxg^{-1} \in N$ for any $g \in SN$.

(c) Show that $S \cap N$ is a normal subgroup of S.

If $x \in S \cap N$, then for all $s \in S$, we know $sxs^{-1} \in N$ since N is normal in G. On the other hand, S is closed under multiplication, so $sxs^{-1} \in S$ as well. This shows $sxs^{-1} \in N \cap S$.

(d) Exhibit an isomorphism between $S/(S \cap N)$ and SN/N. (Hint: Does the equivalence class $[s]$ in the former group define an equivalence class $[sn]$ in the latter group? Does the n in $[sn]$ matter?)

A solution without using the hint: Consider the composition of homomorphisms

$$S \to SN \to SN/N$$

where the latter is the quotient map, and the former is simply the inclusion (note that $S \subset SN$). This composition is a surjection since for any $n \in N$, the element $[sn] \in SN/N$ is equal to the element $[s] \in SN/N$. Its kernel is the set of those elements s which are in N—i.e., $S \cap N$. So we are finished by the first isomorphism theorem.

Alternative proof: This is an explicit construction of the inverse map—illustrated here in case you wanted something more hands-on. Given $[sn] \in SN/N$, consider $[s] \in S/(S \cap N)$.

- We claim the assignment $\phi : [sn] \mapsto [s]$ is well-defined. For if $sn = s'n'x$ with $x \in N$, then

$$s = s'(n' x n^{-1}).$$

We must show that the element $n' x n^{-1}$ is in $S \cap N$. Well, we see it must be in S by multiplying both sides on the left by s'^{-1}. We know that it's in N since the elements n', x, n^{-1} are all in N and N is closed under multiplication.

- Now we show it is a group homomorphism:

$$\begin{aligned}\phi([s_1 n_1][s_2 n_2]) = \phi([s_1 n_1 s_2 n_2)] &= \phi([s_1 s_2 (s_2^{-1} n_1 s_2 n_2)]) \\ &= \phi([s_1 s_2 (n' n_2)]) \\ &= [s_1 s_2] \\ &= [s_1][s_2] \\ &= \phi([s_1 n_1])\phi([s_2 n_2]).\end{aligned}$$

- To show it is an injection, we must show that the kernel is trivial. Well, if $\phi([sn]) = [x]$ for $x \in S \cap N$, then $[sn]$ has a representative of the form xn'; but $x \in X \cap N, n' \in N$ implies $xn' \in N$ by the fact that N is closed under multiplication, so $[sn] = [sn'] = 1 \in SN/N$.
- To show surjection, note that for any $s \in S$, we have that $s = s1_G \in SN$. So $\phi([s1_G]) = \phi(s)$.

4. Subgroups descend to quotient groups

Let G be an arbitrary group, and $H \triangleleft G$.

(a) Show that there is a bijection between the set of subgroups in G containing H, and the set of subgroups in G/H.

Let $p : G \to G/H$ be the group homomorphism given by sending $g \mapsto [g]$.

- Given a subgroup $K \subset G$, note the composition of group homomorphisms
$$K \hookrightarrow G \to G/H.$$
Since the image of any group homomorphism is a subgroup, this shows that $p(K)$ is a subgroup of G/H. So we have a function $\{\text{subgroups of } G\} \to \{\text{subgroups of } G/H\}$ given by sending $K \mapsto p(K)$.
- We show it is a surjection: Given $K' \subset G/H$, consider the pre-image $p^{-1}(K') \subset G$. This is a subgroup of G since if $p(x), p(y) \in K'$, then $p(xy) = p(x)p(y) \in K'$ (because K' is closed under multiplication).
- Now it suffices to show that $p^{-1}(p(K)) = K$ for all subgroups $K \subset G$. Obviously $K \subset p^{-1}(p(K))$. To show the other inclusion, let $x \in p^{-1}(p(K))$. We know by definition of $p(K)$ that there is some $y \in K$ for which $p(x) = p(y)$. Then $p(xy^{-1}) = 1_{G/H}$, so $xy^{-1} \in H$. Since K contains H, $xy^{-1} \in K$, hence $x \in K$.

(b) Show that there is a bijection between the set of *normal* subgroups in G containing H, and the set of normal subgroups in G/H. (This time, this isn't extra credit.)

- We show that if K is normal, then $p(K)$ is normal. (This proves we have a function
$$\{\text{normal subgroups of } G\} \to \{\text{normal subgroups of } G/H\}.)$$
Well, if $[k] \in p(K)$, then $[g][k][g]^{-1} = [gkg^{-1}] = [k']$ for some $k' \in K$ since K is normal in G. So $p(K) \subset G/H$ is normal. (Note we are using the fact that $G \to G/H$ is a surjection here—otherwise, we wouldn't know that every element of G/H is in the image of $p(G)$.)
- Surjectivity: We show that if $p(K)$ is normal, then $K = p^{-1}(p(K))$ is normal (this equality follows from part (c) above). If $k \in K$ and $g \in G$, we have that $[gkg^{-1}] = [g][k][g^{-1}] = [k']$ for some $[k'] \in p(K)$—i.e., for some $k' \in K$. So $gkg^{-1} \in p^{-1}(p(K)) = K$.
- We know that this assignment is an injection by part (c) from the previous problem's solution. So we are finished.

5. Solvable groups

A group G is called *solvable* if there exists a finite sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian.

(a) Show that any abelian group is solvable. (If this seems trivial, it's because it is.)

If G is abelian, take $G_0 = 1$ and $G_n = G_1 = G$. This shows G is solvable.

(b) Show any group of order pq, where p and q are distinct primes, is solvable.

Assume $p < q$. We know any such group G has a normal subgroup H of order q—hence, a normal subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z}$ (since any group of prime order is cyclic). We know the existence of such a normal subgroup by applying the Sylow theorems—see Lecture 22—or by 5(b) of Homework Five. This guarantees that we have a short exact sequence

$$1 \to H \to G \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

(Note that G/H must have order $|G|/|H_q| = pq/q = p$, so we know it has to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$.) So take

$$1 = G_0 \subset G_1 = H \subset G_2 = G.$$

Then $G_1/G_0 \cong H \cong \mathbb{Z}/q\mathbb{Z}$ is abelian, and $G_2/G_1 \cong \mathbb{Z}/p\mathbb{Z}$ is, too.

(c) Show that if G is simple and non-abelian, G cannot be solvable.

Since G is simple, it has no normal subgroups aside from G and $\{1\}$. So if $G_{i-1} \triangleleft G_i$ with $G_i = G$ and $G_{i-1} \neq G_i$, we must have that $G_{i-1} = \{1\}$. But then $G_i/G_{i-1} \cong G$ is not abelian, so G is not solvable.

The following is a great application of the isomorphism theorems, and of the previous problem.

(d) Show that if G is solvable, so is any subgroup of G.

Let $S \subset G$ be a subgroup. If G is solvable, there is some sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian. So consider the sequence

$$1 = S_0 \subset S_1 \subset \ldots \subset S_n = S, \qquad S_i = S \cap G_i.$$

- We know $S_{i+1} \subset G_{i+1}$ is a subgroup, and $G_i \triangleleft G_{i+1}$, so by 3(c) of this midterm, we conclude that $S_{i+1} \cap G_i = S_i$ is normal in S_{i+1}.

- So we must now show that S_{i+1}/S_i is abelian. Consider the composition
$$S_{i+1} \hookrightarrow G_{i+1} \to G_{i+1}/G_i$$
which we call ϕ. (The first homomorphism is the inclusion, while the second is the quotient homomoprhism.) By definition of the quotient, the kernel of ϕ is the set of all elements in S_{i+1} that are also in G_i—that is, the kernel is S_i. Hence S_{i+1}/S_i is isomorphic to the image of ϕ by the first isomorphism theorem. But any subgroup of any abelian group is abelian, and the image of ϕ is a subgroup of G_{i+1}/G_i—which is abelian by assumption.

(e) Show that if G is solvable, and $K \subset G$ is normal, then G/K is solvable.

Let $p : G \to G/K$ be the quotient homomorphism. Since G is solvable, we can find a sequence of subgroups
$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$
such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian. Consider the sequence
$$1 = H_0/K \subset H_1/K \subset \ldots \subset H_n/K = G/K, \qquad H_i = G_iK,$$
We claim this sequence satisfies the properties necessary to show that G/K is solvable. Note that since K is normal in G and $G_i \triangleleft G_{i+1}$, we see that $H_i \triangleleft H_{i+1}$. (Explicitly: If $X \in G_{i+1}$ and $Y \in K$, with $x \in G_i, y \in K$, we have
$$\begin{aligned}
(XY)xy(XY)^{-1} &= XYxyY^{-1}X^{-1} \\
&= Xxx^{-1}YxyY^{-1}X^{-1} \\
&= XxY'yY^{-1}X^{-1} \\
&= XxX^{-1}XY'yY^{-1}X^{-1} \\
&= x'X(Y'yY^{-1})X^{-1} \\
&= x'y'.
\end{aligned}$$
When we replace Y by Y', or x by x', we are using the normalcy of the subgroup containing Y, or x.) So by 4(b), we know that $H_i/K \triangleleft H_{i+1}/K$. By the third isomorphism theorem, we know
$$(H_{i+1}/K)/(H_i/K) \cong H_{i+1}/H_i$$
but this latter group is $G_{i+1}K/G_iK$. Setting $S = G_{i+1}$ and $N = G_iK$ (which is normal in $G_{i+1}K$), note that $G_{i+1}K = SN$. (This is because $G_i \subset G_{i+1}$.) So the second isomorphism theorem gives us the isomorphism in the following line:
$$G_{i+1}K/G_iK = SN/N \cong S/(S \cap N) = G_{i+1}/(G_{i+1} \cap G_iK).$$

But since $G_i \subset (G_{i+1} \cap G_i K)$, this last group receives a surjective homomorphism

$$G_{i+1}/G_i \to G_{i+1}/(G_{i+1} \cap G_i K).$$

Any group receiving a surjective homomorphism from an abelian group must be an abelian group.

6. $GL_n(\mathbb{F}_q)$

Let $\mathbb{F}_q$ be a finite field with q elements.

(a) Let $V = \mathbb{F}_q^n = \mathbb{F}_q^{\oplus n}$ be an n-dimensional vector space over $\mathbb{F}_q$. Show that $G = GL_n(\mathbb{F}_q)$ acts *transitively* on $V - \{0\}$. (That is, show that for any pair $x, y \in V$, there is some group element g so that $gx = y$.)

Fix x. If we can show that for all y, there exists g so that $gx = y$, we're finished. For given another element x', we are guaranteed an element h so that $hx' = x$. Then

$$(gh)x' = g(hx') = gx = y.$$

So let x be the standard column vector

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

If y is any non-zero vector, note that it alone forms a linearly independent set. But any linearly independent collection of vectors can be completed to a basis (29.18 from Lecture 29)—so let $y_1, y_2, \ldots, y_n$ be some basis where $y_1 = y$. Then the matrix g whose ith column is y_i is invertible. (Page 3, Lecture 36.) Moreover, by definition of matrix multiplication, $gx = y_1 = y$.

- - - -For an alternative proof: If y is a column vector whose top entry is $y_1 \neq 0$, then the matrix g whose first column is given by y, and is otherwise a diagonal matrix with 1 along the diagonal:

$$g = \begin{bmatrix} y_1 & 0 & 0 & \ldots & 0 \\ y_2 & 1 & 0 & \ldots & 0 \\ y_3 & 0 & 1 & \ldots & 0 \\ \vdots & \ldots & \ldots & \ldots & \vdots \\ y_n & 0 & 0 & \ldots & 1 \end{bmatrix}$$

This is invertible since its determinant is $y_1 \neq 0$, and satisfies $gx = y$. On the other hand, if $y_1 = 0$, there is some entry of y with $y_i \neq 0$ since $y \neq 0$. In this case, let g' be the matrix whose ith column is y, and which is otherwise a diagonal matrix with 1 along the diagonal. This is invertible because its determinant is $y_i \neq 0$. Also consider the matrix h which swaps the ith standard basis vector with the 1st, and leaves all other standard basis vectors intact. (This is the matrix corresponding to the permutation (1i).) Then we have that $(gh)x = y$.

- - - - For another proof: Some people wanted to show that if x_i form a basis and y_i form a basis, there is some invertible transformation A

taking $x_i \mapsto y_i$. (This is overkill, but yields the result we need: Given x and y, complete each of them to a basis, and use the matrix A.) So let's prove the claim. Well, by definition, a basis $x_1, \ldots, x_n$ determines an $\mathbb{F}$-module isomorphism

$$T_x : \mathbb{F}^n \to \mathbb{F}^n, \qquad e_i \mapsto x_i$$

where e_i are the standard basis vectors. Likewise, the basis $y_1, \ldots, y_n$ determines an $\mathbb{F}$-module isomorphism

$$T_y : \mathbb{F}^n \to \mathbb{F}^n, \qquad e_i \mapsto y_i.$$

You can check that the inverse of an $\mathbb{F}$-module homomorphism is again an $\mathbb{F}$-module homomorphism, and that the composition of invertible $\mathbb{F}$-module homomorphisms is again invertible. So consider

$$A = T_y \circ (T_x)^{-1}.$$

This is an invertible transformation that takes y_i to x_i by definition.

(b) Prove that $G = GL_n(\mathbb{F}_q)$ has

$$\left(\prod_{k=1}^{n}(q^k - 1)\right)\left(\prod_{k=1}^{n-1} q^k\right)$$

elements in it. (You can either count intelligently, or apply the orbit-stabilizer theorem inductively. Either way, use matrices.)

First note that if $n = 1$, we have that $GL_1(\mathbb{F}_q)$ is the set of invertible 1×1 matrices—that is, the set of all invertible elements in $\mathbb{F}_q$. Since $\mathbb{F}_q$ is a field, this means that $|GL_1(\mathbb{F}_q)| = q - 1$.

Now: Let $x = e_1$ be the standard basis vector with 1 in the first entry and 0 elsewhere. The stabilizer of x is the set of all matrices g for which $gx = x$—that is, the set of all matrices whose first column is given by e_1. (This is because ge_1 always equals the first column of g—if you're not sure why, try writing it out.) How many such invertible matrices are there? Well, writing

$$g = \begin{bmatrix} 1 & -\vec{u}- \\ 0 & A \end{bmatrix}$$

where $\vec{u}$ is some row vector with $n-1$ entries, and A is a $(n-1)\times(n-1)$ matrix, we see that $\det g = \det A$. So g is invertible if and only if A is, while the entries of $\vec{u}$ have no effect on whether g is invertible. By the orbit stabilizer theorem,

$$|GL_n(\mathbb{F}_q) = |\mathcal{O}_x| \cdot |\text{Stabilizer}(x)|.$$

By above, the orbit of x is all of $\mathbb{F}_q^n - \{0\}$—but $\mathbb{F}_q^n$ has q^n elements in it, so removing $\{0\}$ yields an orbit with size $q^n - 1$. On the other hand, an element of the stabilizer is determined uniquely by a choice of A and of $\vec{u}$—there are $|GL_{n-1}(\mathbb{F}_q)|$ choices for A, and q^{n-1} choices for $\vec{u}$. Thus we have that

$$|GL_n(\mathbb{F}_q)| = (q^n - 1) \cdot (q^{n-1})(|GL_{n-1}(\mathbb{F}_q)|).$$

Now you can check that the formula holds as claimed, by induction.

(c) Show that $GL_n(\mathbb{F}_q)$ has a normal subgroup of index $q-1$. (Hint: The determinant is still a group homomorphism.)

The group homomorphism $GL_n(\mathbb{F}_q) \to (\mathbb{F}_q - \{0\})$ is a surjection. (For instance, take the diagonal matrix with diagonal entries given by 1 and by a single appearance of a. This has determinant a.) Hence the index of its kernel is given by the size of the target group, which is $q-1$.

(d) Consider $G = GL_2(\mathbb{F}_q)$. Assume p is the unique prime number dividing q. [1] Show that $|\operatorname{Syl}_p(G)|$ cannot equal 1. (Try thinking about upper-triangular and lower-triangular matrices, then think about special cases of them.)

The group $GL_2(\mathbb{F}_q)$ has size

$$(q^2-1)(q-1)q$$

according to the previous problem. So any subgroup of size q is a Sylow p-subgroup. (If q is divisible by only p, then no number of the form $q^k - 1$ is divisible by p.) We claim that the set of all upper-triangular matrices with 1 along the diagonal, and the set of all lower-triangular matrices with 1 along the diagonal, each form a subgroup of order q—thus $\operatorname{Syl}_p(\mathbb{F}_q)$ has more than one element.

- - - Note that the size of each set is obviously q. The determinant of an element in either of these sets is 1, and the identity matrix is in both sets, so we just need to prove that both are closed under multiplication:

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}.$$

The proof for the lower-triangular case is identical; just take the transpose of each matrix.

- - - - By the way, you can show that for any n, the upper-triangular matrices with 1 along the diagonal constitute a q-Sylow subgroup of $GL_n(\mathbb{F}_q)$.

- - - - - Another proof, even without producing a Sylow subgroup: Note that the sizes of the set of upper-triangular and lower-triangular matrices are divisible by q, so these must contain p-Sylow subgroups, H and

[1] One can prove that any finite field has size p^k for some prime p.

As pointed out to me by Kevin, it's not hard—a finite field of characteristic p is a module over $\mathbb{Z}/p\mathbb{Z}$, so is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. But how many elements must such a set have?

K. But the intersection of the upper-triangular and lower-triangular matrices are the diagonal matrices, of which there are $(q-1)^n$ (a number not divisible by q). Hence the p-Sylow subgroups contained in H and K must be distinct.

(e) How many elements of order 3 are in $GL_2(\mathbb{F}_3)$? (You may want to start by determining the number of Sylow 3-subgroups. Either way, dig in.)

Note that the 3-Sylow subgroups of $GL_2(\mathbb{F}_3)$ are given by subgroups of order 3. Note also that if two subgroups of order 3 have an intersection that contains more than the identity, then the two subgroups must be equal (you can check this). Moreover, for each distinct 3-Sylow subgroup H, the generator $x \in H$ and its square, x^2, represent distinct elements of order 3. Conversely, any element of order 3 determines a 3-Sylow subgroup by looking at the subgroup it generates. Hence the number of elements of order 3 is given by $2 \cdot |\,\mathrm{Syl}_3(GL_2(\mathbb{F}_3))|$.
- - - - By (d), we know that $s := |\,\mathrm{Syl}_3(GL_2(\mathbb{F}_3))| \geq 2$. By the Sylow theorems, the number s must divide

$$(q^2-1)(q-1) = 8 \cdot 2 = 16$$

and must equal 1 modulo 3. This leaves the options of $s = 4$ or $s = 16$. Claim: $s = 16$ is impossible. Note that then we would have $2 \cdot 16 = 32$ elements of order 3. And the Sylow Theorem guarantees that we have at least one group of order 16—the 2-Sylow subgroup. Since $32 + 16 = 48 = |GL_2(\mathbb{F}_3)|$, this implies there can be no elements of order other than 3 (those elements in a subgroup of order 3), or some power of 2 (those elements in the Sylow 2-subgroup). But there is in fact an element of order 6 in $GL_2(\mathbb{F}_3)$, given by

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}.$$

To see this, note

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

while

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & an \\ 0 & 1 \end{bmatrix}$$

in general. So $s = 16$ leads to a contradiction, and we conclude that $s = 4$. this means that there are $2 \cdot 4 = 8$ elements of order 3.
- - - - Another proof that $s = 16$ is impossible: Any element of order 3 must have determinant 1—after all, $(\det g)^3 = \det g^3 = \det I = 1$, and the only cube root of 1 in $\mathbb{F}_3$ is 1. But the kernel of the determinant has $|GL_2(\mathbb{F}_3)|/|\mathbb{F}_3 = \{0\}| = 48/2 = 24$ elements in it, so it couldn't contain 32 elements.

- - - - Yet another proof that $s = 16$ is impossible: From the proof of the Sylow theorems, we know that $[GL_2(\mathbb{F}_3) : N(H)] = s$, where $N(H)$ is the normalizer of the Sylow 3-subgroup H. But the elements

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

all normalize the 3-Sylow subgroup H of upper triangular matrices with 1 along the diagonal. Hence $|N(H)| \geq 4$, and s must be less than 16.
- - - - - Another proof: Let K be the kernel of the determinant map. It's a normal subgroup of index 2, so of order 24. By Sylow's theorems, you can see that K must contain either 1 or 4 subgroups of order 3 (check this yourself). But the upper and lower-triangular matrices with 1 along the diagonal are both subgroups of K, so there must be 4 subgroups of order 3 in K. Since any 3-Sylow subgroup of $GL_2(\mathbb{F}_q)$ must be conjugate by Sylow's theorems, they must all be contained in K since K is closed under conjugation. So these 4 subgroups in K are also all the 3-Sylow subgroups of $GL_2(\mathbb{F}_q)$, and we have that $s = 4$.

No more collaboration

7. Ring homomorphisms

(a) Show that a composition of two ring homomorphisms is a ring homomorphism.

Let $f : R \to S$ and $g : S \to T$ be ring homomorphisms. We know the composition of two group homomorphisms is a group homomorphism, we know that $g \circ f$ is a group homomorphism under addition. Thus we need only check that $g \circ f(r_1 r_2) = (g \circ f(r_1))(g \circ f(r_2))$, and that $g \circ f(1_R) = 1_T$. The first equality follows because

$$g \circ f(r_1 r_2) = g(f(r_1) f(r_2)) = g(f(r_1)) g(f(r_2)).$$

The last follows because $gf(1_R) = g(1_S) = 1_T$.

(b) For a ring R, let $M_{k\times k}(R)$ denote the ring of $k \times k$ matrices with entries in R. Specifically, if (a_{ij}) is a matrix whose i, jth entry is a_{ij}, we define

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \qquad (a_{ij})(b_{ij}) = (\sum_{l=l}^{k} a_{il} b_{lj}).$$

Show that if $f : R \to S$ is a ring homomorphism, then the function

$$F : M_{k\times k}(R) \to M_{k\times k}(S), \qquad (a_{ij}) \mapsto (f(a_{ij}))$$

is a ring homomorphism.

To show that F is a group homomorphism with respect to addition, let a_{ij} and bij be the i, jth entries of matrices A, B having entries in R. Then

$$F(A + B)_{ij} = f(a_{ij} + b_{ij}) = f(a_{ij}) + f(b_{ij}) = (F(A) + F(B))_{ij}.$$

Since the i, jth entries of both matrices agree, we have that $F(A+B) = F(A) + F(B)$. To show that the multiplicative identity is mapped to the multiplicative identity, note that the identity of the ring of $k \times k$ matrices is given by the diagonal matrix with diagonal entries 1_R and 1_S, respectively. But since f is a ring homomorphism, F sends the identity of $M_{k\times k}(R)$ to that of $M_{k\times k}(S)$. Finally, we must show that F respects multiplication. To see this, note

$$F(AB)_{ij} = f(\sum_{l=1}^{k} a_{il} b_{lj}) = \sum_{l=1}^{k} f(a_{il}) f(b_{lj}) = \sum_{l=1}^{k} F(A)_{il} F(B)_{lj} = (F(A)F(B))_{ij}.$$

(c) Prove that

$$f(\det A) = \det(F(A)).$$

You may want to start by proving it for $k = 1$, then perform induction using the cofactor definition of determinants.

This is true for $k = 1$, since a 1×1 matrix A is the data of choice of an element $a \in R$, and its determinant is equal to a. Hence

$$f(\det A) = f(a) = \det F(A).$$

By induction, assume the equality holds for matrices of dimension $\leq k - 1$. We have that

$$f(\det A) = f(\sum_{i=1}^{k} (-1)^{i+1} a_{0i} \det C_{0i})$$

where C_{0i} is the matrix obtained by deleting the 0th row and ith column of A. Since f is a ring homomorphism, we have that this in turn equals

$$\sum_{i=1}^{k} (-1)^{i+1} f(a_{0i}) f(\det C_{0i}) = \sum_{i=1}^{k} (-1)^{i+1} F(A)_{0i} \det F(C_{0i}).$$

Noting that $F(C_{0i})$ is the cofactor matrix of $F(A)$ given by deleting the 0th row and ith column, we are finished.

8. Invertible matrices

Let S be a ring. We say $x \in S$ is a *unit* if there is a multiplicative inverse to x—i.e., an element $y \in S$ so that $xy = yx = 1_S$. As an example, if S is the ring of $k \times k$ matrices in some ring R, then a matrix is invertible if and only if it is a unit.

(a) Determine which of the following matrices is a unit in $M_{k\times k}(\mathbb{Z})$:

$$\begin{pmatrix} 2 & 5 \\ 4 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix}$$

None of them. A matrix with coefficients in R is a unit if and only if its determinant is a unit in R. But the determinant of the above three matrices are

$$8 - 20 = 12, \qquad 8 - 45 = -37, \qquad 21 - 24 = 3$$

respectively. However, the only units in $\mathbb{Z}$ are ± 1.

(b) For the primes $p = 2, 3, 5$, consider the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ sending $a \mapsto \overline{a}$. This induces a ring homomorphism $M_{k\times k}(\mathbb{Z}) \to M_{k\times k}(\mathbb{Z}/p\mathbb{Z})$ by the previous problem. Determine which of the matrices above is sent to a unit for each choice of $p = 2, 3, 5$.

Modulo p, the integer determinants $12, -37, 3$ above are given respectively by

$$\begin{array}{cccc} 0, & 1, & 1 & (mod 2) \\ 0, & 2, & 0 & (mod 3) \\ 2, & 3, & 3 & (mod 5). \end{array}$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the invertible matrices are those who determinants are non-zero, (since, in a field, any non-zero element is a unit).

9. Bases

Let $M = \mathbb{Z}/n\mathbb{Z}$.

(a) Show that M admits no basis as a module over $\mathbb{Z}$.

The easiest proof: Any basis induces an isomorphism $\mathbb{Z}^k \to M$. But M is finite, while $\mathbb{Z}^k$ is finite if and only if $k = 0$.

- - - - A more hands-on proof: For any element $x \in M$, we have that $nx = 0 \in M$. Hence M does not admit any non-empty sets of linearly independent elements, hence admits no basis.

(b) Show that M admits a basis as a module over the ring $R = \mathbb{Z}/n\mathbb{Z}$.

Let $x = \overline{1}$. This is a spanning set because for any $\overline{j} \in M$, we know that $\overline{j} = \overline{j} \cdot x$. It is linearly independent because $\overline{a}x = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ means that $a \cdot 1$ is a multiple of n. But this means a itself must be a multiple of n, hence $\overline{a} = \overline{0} \in R$.

10. Ideals are like normal subgroups

Let R be a commutative ring. Show that $I \subset R$ is an ideal if and only if it is the kernel of some ring homomorphism. (The kernel of a ring homomorphism $R \to S$ is the set of all elements sent to $0 \in S$.)

Let $\phi : R \to S$ be a ring homomorphism. If $x \in \ker \phi$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0_S = 0_S.$$

So $\ker \phi$ is closed under scaling by arbitrary elements of R. Likewise, the kernel of a ring homomorphism is by definition the kernel of the group homomorphism $\phi : (R, +) \to (S, +)$ so it is a subgroup of R under addition. This proves $\ker(\phi)$ is an ideal. For the converse, we know that any ideal $I \subset R$ of a commutative ring defines a ring homomorphism $R \to R/I$ given by $r \mapsto \bar{r}$. The kernel is precisely those elements in I, so any ideal is a kernel of a ring homomorphism.

11. Characteristic

Let F be a field, and $1 \in F$ the multiplicative identity. The *characteristic* of F is the smallest integer n with $n \geq 1$ such that

$$1 + \ldots + 1 = 0$$

where the summation has n terms in it. For instance, the characteristic of $\mathbb{Z}/p\mathbb{Z}$ is p. If F is a field where $1 + \ldots + 1$ never equals 0 (like $\mathbb{R}, \mathbb{Q}, \mathbb{C}$) we say that F has *characteristic zero*.

Prove that any field (finite or not!) must have either characteristic zero, or characteristic p for some prime number p.

(By the way, there are in fact infinite fields of finite characteristic.)

We first note that n cannot equal 1. If so, we have that $1 = 0$. But then $F - \{0\}$ cannot be a group with F being a ring. To see this, let $e \in F - \{0\}$ be the identity. Then $ex = x$ for all $x \neq 0$, and $e0 = 0$ so e is also the multiplicative unit of F—the contradiction arises by the uniqueness of the multiplicative unit of F, which demands that $e = 1$. So n cannot be 1.
- - - -Clearly $1 + \ldots + 1 = 0$ for some finite summation with n terms in it, assume that n is divisible by two numbers, ab, neither of which is 1. Then we have that

$$(1 + \ldots + 1)(1 + \ldots + 1) = 0$$

where the left factor has a summands, and the right factor has b summands. But since F is a field, if two elements multiply to 0, one of them must equal zero. (As we proved in class, units are not zero divisors, and every non-zero element of a field is a unit.) But then a summation of either a or b terms of 1 equals zero, contradicting the assumption that n is the smallest such number. Hence either a or b must equal 1, meaning n must be prime.

12. Solvability of S_n.

(a) For $n \geq 3$, show that any cycle of length 3 is in A_n.

Let (ijk) be a cycle of length three. It is a composition $(ij) \circ (jk)$, but the sign of (ij) is minus one. Since the sign map from $S_n \to \{\pm 1\}$ is a homomorphism, this means that the sign of $(ij) \circ (jk)$ is given by $-1 \times -1 = 1$; hence (ijk) is in the kernel of the sign map.

(b) Show by example that A_n is not abelian for $n \geq 4$.

Consider the cycles (123) and (234). We have

$$(123) \circ (234) = (21)(34), \qquad (234) \circ (123) = (13)(24)$$

so these two elements of A_n, $n \geq 4$ do not commute.

(c) Assume A_n is simple for $n \geq 5$. (This is a theorem we stated, but never proved.) Explain why S_n is not solvable for any $n \geq 5$.

By 5(c), a non-abelian, simple group is not solvable. So A_n is not solvable for $n \geq 5$. If S_n is solvable, so would any subgroup of it be (by 5(d)), so S_n is not solvable for $n \geq 5$.

(d) Show that S_n is solvable for $n \leq 3$. So all that remains is S_4.

If $n = 1$, S_1 is the trivial group, so one can take $G_0 = G_n$ and we have that S_1 is solvable. $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ so it is solvable, being abelian, by 5(a). Finally, S_3 has order 6, which is solvable by 5(b).

(e) Prove that S_4 is solvable. (One way: You can exhibit an abelian subgroup of order 4 in A_4.)

Suppose there is an abelian, normal subgroup H of order 4 in A_4. Then A_4/H must be a group of order $12/4 = 3$, hence a cyclic (and abelian) group. Then the sequence

$$1 = G_0 \subset G_1 = H \subset G_2 = A_4 \subset G_3 = S_4$$

would show that S_4 is solvable. (Note $G_3/G_2 \cong \mathbb{Z}/2\mathbb{Z}$.) Let

$$H = \{1, a = (12)(34), b = (13)(24), c = (14)(23)\}.$$

Note each element is its own inverse so H is closed under taking inverses. To see it is closed under multiplication, first note

$$(12)(34) \circ (13)(24) = (14)(23), \qquad (13)(24) \circ (12)(34) = (14)(23).$$

Since each of these elements is their own inverse, we see that $ab = c, ba = c$ implies $a = cb = bc$ and $b = ac = ca$; hence this set is abelian and closed under multiplication. (It's in fact isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, though we don't need that.) Finally, to conclude that H is closed under conjugation, recall that in the symmetric group, conjugation preserves cycle shape. And every element whose cycle shape is given by two disjoint cycles of length 2 is in H—so in fact, H is a normal subgroup of S_4. This implies it's a normal subgroup of A_4.