Yale University Department of Mathematics
**Math 350 Introduction to Abstract Algebra**
Fall 2015

Midterm Exam Review Solutions

**Practice exam questions:**

**1.** Let $V_1 \subset \mathbb{R}^2$ be the subset of all vectors whose slope is an integer. Let $V_2 \subset \mathbb{R}^2$ be the subset of all vectors whose slope is a rational number. Determine if $V_1$ and/or $V_2$ is a subgroup of $\mathbb{R}^2$, with usual vector addition.

**Solution.** $V_1$ contains zero (if one defines the slope of the origin to be 0), is closed under taking inverses (negation actually preserves slope), but is not closed under addition. For example, $v = (1, 2)$ has slope 2 and $w = (1, 1)$ has slope 1, but $v + w = (3, 2)$ has slope $3/2$.

$V_2$ contains zero, is closed under taking inverses, but is not closed under addition. For example, $v = (1, 0)$ has slope 0 and $w = (\sqrt{2}, \sqrt{2})$ has slope 1, but $v + w$ has slope $\sqrt{2}/(1 + \sqrt{2}) = 2 - \sqrt{2}$, which is not rational.

**2.** Write down a nontrivial homomorphism $\varphi : \mathbb{Z}/36\mathbb{Z} \to \mathbb{Z}/48\mathbb{Z}$ and compute its image and kernel.

**Solution.** Since the domain is a cyclic group, we only need to specify where a generator is sent, and verify the relations. So we need to choose $\varphi(1)$ whose order divides 36. For example, $\gcd(36, 48) = 12$, so we could choose $\varphi(1)$ to be any element of order 12 in $\mathbb{Z}/48\mathbb{Z}$, for example, $48/12 = 4$ has order 12. So the choice of $\phi(1) = 4$ will produce a well defined (and nontrivial) homomorphism $\varphi : \mathbb{Z}/36\mathbb{Z} \to \mathbb{Z}/48\mathbb{Z}$. The image is the cyclic subgroup $\langle 4 \rangle \leqslant \mathbb{Z}/48\mathbb{Z}$, which is itself a cyclic group of order 12. Since $\varphi(1)$ has order 12, it shows that $\varphi(12) = 0$ and in fact that the $\ker(\varphi)$ is the cyclic subgroup $\langle 12 \rangle \leqslant \mathbb{Z}/36/\mathbb{Z}$, which is itself a cyclic group of order $36/12 = 3$. Of course, any choice of element of $\mathbb{Z}/48\mathbb{Z}$ whose order divides 36 would have worked, for example, $24 \in \mathbb{Z}/48\mathbb{Z}$ has order 2, which gives another nontrivial example.

**3.** How many elements of order 6 are there in $S_6$? In $A_6$?

**Solution.** Considering the disjoint cycle decomposition, and the formula for the order of a product of disjoint cycles as the lcm of the cycle lengths, the only elements of order 6 in $S_6$ are the 6-cycles or the $(2, 3)$-cycles. There are 5! choices of 6-cycles, indeed, a 6-cycle must contain all numbers $1, \ldots, 6$ and we can always cyclically permute so that 1 is the first number, then there 5! distinct choices for the rest of the numbers. There are $2 \cdot \binom{6}{2}\binom{4}{3}$ choices of $(2, 3)$-cycles, indeed, choosing a 2-cycle is equivalent to choosing 2 elements out of 6 and then 3 elements out of the remaining 4, with the understanding that for each choice there is a unique 2-cycle and two possible 3-cycles with those given sets of numbers. (Or you can memorize formulas in the book for the number of $n$-cycles in a symmetric group.) In total, there are $120 + 120 = 240$ elements of order 6 in $S_6$ (which is 1/3 of the elements!).

**4.** Prove that $11^{104} + 1$ is divisible by 17.

**Solution.** We use Euler's theorem to compute $11^{104}$ mod 17. Since $11^{16} \equiv 1 \pmod{17}$ we reduce $104 = 6 \cdot 16 + 8$ mod 16, so that $11^{104} \equiv 11^8 \pmod{17}$. Now $11^8 = (11^2)^4 = 121^8$, so we can simplify by reducing $121 = 7 \cdot 17 + 2$ mod 17, so that $11^8 \equiv 121^4 \equiv 2^4 \equiv 16 \pmod{17}$. Then $11^{104} + 1 \equiv 16 + 1 \equiv 0 \pmod{17}$, implying that $11^{104}$ is divisible by 17.

**5.** Let $G$ be a finite group and $x, y \in G$ be nonidentity elements such that $xyx^{-1} = y^{-1}$. Show that $G$ has an element of order 2. Find an infinite group $G$ where this breaks down.

**Solution.** If $y$ has order 2 we are done, so we can assume that $|y| > 2$, in which case $y \neq y^{-1}$. Now consider the subgroup $H \leqslant G$ generated by $x$ and $y$. The crucial observation is that $H$ acts on the set $A = \{y, y^{-1}\}$ by conjugation. Indeed, $x$ acts by exchanging the elements of $A$ and $y$ does nothing, so any element in $H$ either exchanges the elements of $A$ or leaves them fixed. We get a permutation representation $\sigma : H \to S_A \cong \mathbb{Z}/2\mathbb{Z}$, which is surjective, since $x$ maps to the nonidentity element. By the 1st isomorphism theorem, we have that $|H| = |\ker(\sigma)||\mathbb{Z}/2\mathbb{Z}|$ is even. By Cauchy's theorem, $H$ has an element of order 2, hence so does $G$.

The second part is really hard (must harder than what you'll find on the midterm), but I wanted you to try to get it! To find an infinite group where the conclusion fails, build the universal group where $xyx^{-1} = y^{-1}$ holds, namely, the group with presentation

$$G = \langle x, y \,|\, xyx^{-1} = y^{-1} \rangle.$$

First we can argue that this group is nontrivial and that both $x$ and $y$ have infinite order. To see this, we can define a homomorphism $G \to D_{2n}$ by specifying where the generators are sent: $x \mapsto s$ and $y \mapsto r$. The relation is clearly satisfied by the usual presentation of the dihedral group, so this defines a homomorphism, which is clearly surjective. So $G$ cannot be the trivial group and, in fact, $G$ must be nonabelian (it maps surjectively to a nonabelian group). Also, neither $x$ nor $y$ can be the identity, and moreover, $y$ has infinite order (since it map to elements of any given order, it cannot itself have finite order). We can also define a surjective homomorphism $G \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by sending $x \mapsto (1, 0)$ and $y \mapsto (0, 1)$ and checking the relation. Thus shows that $x$ also has infinite order. Next, considering the same conjugation action on the set $\{y, y^{-1}\}$ as before, we get a surjective permutation representation homomorphism $\sigma : G \to \mathbb{Z}/2\mathbb{Z}$. One can check that $K = \ker(\sigma)$ is generated by $x^2$ and $y$. One thing you might have noticed while playing around with the relation is that it implies that $yx^2 = x^2y$. Thus $K$ is generated by two commuting elements, i.e., has a presentation $K = \langle u, v \,|\, uv = vu \rangle$. Thus, in fact, $K$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. In particular, $K$ has no elements of finite order. Now assume that $G$ has some element $z$ of order 2, then $z \notin K$. As $K \trianglelefteq G$ has index 2, we have a disjoint union $G = K \cup xK$, hence $z \in xK$. Write $z = xu$ for some $u \in K$. Then $1 = z^2 = xuxu = xux^{-1}x^2u = xux^{-1}ux^2$, since $u$ and $x^2$ are in $K$, so commute. Note that, for a general $u \in K$, we have that $xux^{-1}u$ is a power of $x^4$. Indeed, since we can write $u = y^n x^{2m}$, we have that $xux^{-1} = xy^n x^{-1} x^{2m} = y^{-n} x^{2m}$, so that $xux^{-1}u = x^{4m}$. However, assuming the existence of $z$, we got that $xux^{-1}u = x^{-2}$, which is impossible. Hence there is no element $z$ of order 2 in $G$.

**6.** Write down two elements of $S_{10}$ that generate a subgroup isomorphic to $D_{10}$. (Hint: Use the left multiplication action on $D_{10}$.)

**Solution.** If we order the elements of $D_{10} = \{1, r, \ldots, r^4, s, sr, \ldots, sr^4\}$ in the usual way, then we can compute the permutations induced the elements of $D_{10}$ by left multiplying by

$r$ and $s$. We see that $r$ corresponds to the permutation $(12345)(10\,9876)$ and $s$ corresponds to the permutation $(16)(27)(38)(49)(5\,10)$. Since the left multiplication action is always faithful, the image of its permutation representation is a subgroup of $S_{10}$ isomorphic to $D_{10}$ and generated by the images of $r$ and $s$.

**7.** Consider the left regular permutation representation $S_n \to S_{n!}$. Describe the cycle type in $S_{n!}$ of the image of an $n$-cycle in $S_n$.

**Solution.** Let $\sigma$ be an $n$-cycle and $z$ any element of $S_n$. Then the cycle containing $z$ in the permutation induced by left multiplication by $\sigma$ on $S_n$, is just $\{z, \sigma z, \sigma^2 z, \ldots, \sigma^{n-1} z\}$. Indeed, if $\sigma^i z = \sigma^j z$, then $i \equiv j \pmod{n}$. If we imagined ordering all $n!$ elements of $S_n$, then we see that $\sigma$ would permute the elements as a disjoint product of $n$-cycles, in fact $(n-1)!$ of them. In fact, the same argument shows that if $\sigma$ is any element of order $k$ in $S_n$, then the cycle type of the permutation induced by $\sigma$ via left multiplication, is a product of $n!/k$ disjoint $k$-cycles. This makes all permutation in $S_n$ look "regular."

**8.** Prove that $C_{S_n}\big((12)(34)\big)$ has $8\,(n-4)!$ elements for $n \geq 4$ and explicitly determine all of them.

**Solution.** We know that the size of the conjugacy class in $S_n$ containing $\sigma = (12)(34)$ is $[S_n : C_{S_n}((12)(34))]$. But we also know that this conjugacy class consists of all type $(2,2)$-cycles. We can count the number of them. Choosing a type $(2,2)$-cycle is equivalent to choosing 2 elements out of $n$ and then 2 elements out of the remaining $n-2$, and remembering that we can switch the order of the two disjoint 2-cycles we've just chosen. So the number is $\frac{1}{2}\binom{n}{2}\binom{n-2}{2}$. Thus

$$|C_{S_n}((12)(34))| = \frac{n!}{\frac{1}{2}\binom{n}{2}\binom{n-2}{2}} = 8\,(n-4)!$$

Explicitly, $C_{S_n}((12)(34)) = C_{S_4}((12)(34)) \cdot S_{n-4}$, where $S_{n-4}$ is the symmetric subgroup on $\{4, 5, \ldots, n\}$, and $C_{S_4}((12)(34)) = \{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$.

**9.** Show that the set of nonzero matrices of the form

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$. What is the order of this subgroup?

**Solution.** Let's denote this matrix by $M(a,b)$. First, note that there are 24 such choices of nonzero matrices $M(a,b)$, since each of $a$ and $b$ can range over $\mathbb{F}_5$, but both can't be zero. Next, note that $\det M(a,b) = a^2 - 3b^2$ is only zero when $a = b = 0$, which we can check directly, noting that the only squares in $\mathbb{F}_5$ are 0, 1, and 4. So these 24 matrices are certainly contained in $\mathrm{GL}_2(\mathbb{F}_5)$. We also see that $M(a,b)M(c,d) = M(c,d)M(a,b) = M(ac + 3bd, ad + bc)$, hence this subset is closed under multiplication and all elements commute, so it forms an abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$. To prove that it is cyclic, we need to show that (at least) one of these elements has order 24.

We first note that 2 and 3 have order 4 in $\mathbb{F}_5^\times$, so $|M(2,0)| = |M(3,0)| = 4$. Next, let's look at the next easiest case, $M(0,a)^2 = M(3a^2, 0)$, hence $|M(0,b)| = 8$ for any $b \in \mathbb{F}_5^\times$, in view of the fact that $3a^2$ is always either 3 or 2. Now, if we can also find an element of order 3, then its product with an element of order 8 will have order 24, by PS 1 (we are in

an abelian group). To find an element of order 3, we are looking for a matrix that satisfies the polynomial $x^3 - 1 = (x-1)(x^2+x+1)$. So if it satisfies $x^2+x+1$, then it will have order 3. The characteristic polynomial of $M(a,b)$ is $x^2 - 2ax + a^2 - 3b^2$, so that choosing $(a,b) = (2,1)$, for example, gives a matrix $M(2,1)$ that satisfies the correct polynomial (by the Cayley–Hamilton theorem) so has order 3. Hence $M(0,1)M(2,1) = M(3,2)$ has order 24, and we've just proved that this subgroup is cyclic of order 24.

**10.** Find square matrices $A$ and $B$ with coefficients in the field $\mathbb{F}_p$ such that $AB - BA = I$. What size do the matrices need to be? (Note that this is impossible for real matrices because $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$!)

**Solution.** Over any scalar field, since $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, we have that $\mathrm{Tr}(AB - BA) = 0$. Hence if $AB - BA = I$ for some $n \times n$ matrices, then $\mathrm{Tr}(I) = n$ must be zero in the field. So, over a field of characteristic zero (i.e., where no integer is zero), no such matrices can exist. Over a field of characteristic $p$, in order to find such matrices, we must have $p \mid n$.

Playing around with matrices, one can, for $p$ small, find explicit $p \times p$ matrices that do the job. For example, for $p = 2$,

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

works. For $p = 3$,

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

works, and going on this way, one could start to see a pattern emerge. However, here is a really nice construction of such matrices. It is not easy to just come up with this out of nowhere, but it's nice so I wanted to show it to you.

First, let $F$ be any field, and let $F[x]$ denote the (countably infinite dimensional) vector space of polynomials $p(x)$ with coefficients in $F$. Define linear maps $A : F[x] \to F[x]$ to be differentiation and $B : F[x] \to F[x]$ to be multiplication by $x$. Then the product rule gives, for any $p(x) \in F[x]$,

$$\frac{d}{dx}(xp(x)) = x\frac{d}{dx}p(x) + p(x)$$

which we can rewrite as $\frac{d}{dx}(xp(x)) - x\frac{d}{dx}p(x) = p(x)$, i.e., $AB - BA = \mathrm{id}$. This gives an infinite dimensional example over any field. We could even write the infinite by infinite matrix representations of these linear maps (with respect to the standard basis of $F[x]$) to get explicit infinite matrices.

Now let $F = \mathbb{F}_p$. Then something special happens, namely, $\frac{d}{dx}x^p = 0$. This gives a clue that we can truncate the infinite dimension example into a $p$-dimensional example. Let $V$ be the $\mathbb{F}_p$-vector space of polynomials of degree at most $p-1$ over $\mathbb{F}_p$. Then $V$ has dimension $p$ with basis $1, x, \ldots, x^{p-1}$. Let $A$ be differentiation again and now let $B$ be multiplication by $x$, but taken "modulo $x^p$" (which later in the semester will actually have a legitimate meaning), by which we mean $B(x^i) = x^{i+1}$ if $i < p-1$ and $B(x^{p-1}) = 0$. Then actually $A$ and $B$ still work, and now they are linear operators on a $p$-dimensional vector space! By looking at the matrix representations of $A$ and $B$ (with respect to the standard basis), we can even get explicit $p \times p$ matrices.

**11.** Find the highest power of $p$ dividing the order of $\mathrm{GL}_n(\mathbb{F}_p)$. Find a Sylow $p$-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. (Hint: Think upper triangular.)

**Solution.** From class, we've seen several times that

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1})$$

we can factor $0 + 1 + 2 + \cdots + (n-1) = n(n-1)/2$ powers of $p$ out and what remains $(p^n - 1)(p^{n-1} - 1)\cdots(p - 1)$ will not be divisible by $p$.

Following the hint, and being inspired by some stuff we did form the last problem set, we can see that the subgroup (you basically checked that this was a subgroup in homework) of all "unipotent" matrices, i.e., upper triangular matrices with ones on the diagonal,

$$\begin{pmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & * \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

has $n(n-1)/2$ spots where any element of $\mathbb{F}_p$ can go, so the order of this subgroup is $p^{n(n-1)/2}$, hence it's a Sylow $p$-subgroup.