Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2016

Midterm Exam Review Solutions

Practice exam questions:

2. 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.

3. 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.

If there was an injective homomorphism, its image would be a subgroup of $\mathbb{Z}/48\mathbb{Z}$ of order 36, which cannot exist by Lagrange's theorem. No surjective homomorphism can exist because $|\mathbb{Z}/36\mathbb{Z}| < |\mathbb{Z}/48\mathbb{Z}|$.

4. 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!).

The elements of order 6 in A_6 are the even permutations of order 6 in S_n. But none of them are even! So there are no elements of order 6 in A_6!

5. 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.

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 σ be an n-cycle and z any element of S_n. Then the cycle containing z in the permutation induced by left multiplication by σ 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 σ 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 σ is any element of order k in S_n, then the cycle type of the permutation induced by σ 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 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 on a previous 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.