Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2017

Final Exam Review Sheet Solutions

3. There is an injective homomorphism $S_n \to A_{2n}$ sending each σ permutation of $\{1, \ldots, n\}$ to the product $\sigma\sigma'$, where σ' is the same permutation as σ, except it acts on $\{n+1, \ldots, 2n\}$. The product of two disjoint permutations of the same length is always even. Checking that this defines an injective homomorphism is straightforward (since σ and σ' commute). Then, given any group G of order n, the left regular representation yields an injective homomorphism $G \to S_n$, which we can then compose with $S_n \to A_{2n}$.

4. Using Euler's theorem, $13^{35} \equiv 13^5 \bmod 31$ since $35 \equiv 5 \bmod 30$, and $\varphi(31) = 30$. Now $13^2 = 169 \equiv 14 \bmod 31$ and $14^2 = 196 \equiv 10 \bmod 31$, so $13^5 = ((13^2)^2) \cdot 13 \equiv (14)^2 \cdot 13 \equiv 10 \cdot 13 \equiv 6 \bmod 31$, hence $13^{35} - 7 + 5^3 \equiv 6 - 7 + 1 \equiv 0 \bmod 31$, and thus $13^{35} - 7 + 5^3$ is divisible by 31.

5. By the classification theorem for finite abelian groups, the number of isomorphism classes only depends on the number of times a given prime number divides the order. So there are three cases to consider.

Case 1, $p = q = r$. Then we are considering groups of order p^6. Elementary divisors are in bijection with partitions of 6. There are eleven of them: (6), $(5,1)$, $(4,2)$, $(4,1,1)$, $(3,3)$, $(3,2,1)$, $(3,1,1,1)$, $(2,2,2)$, $(2,2,1,1)$, $(2,1,1,1,1)$, $(1,1,1,1,1,1)$. So there are 11 isomorphism classes of abelian group of order p^6.

Case 2, $p = r$, $q \neq p$. Then we are considering groups of order p^4q^2. Elementary divisors for the p-part are in bijection with partitions of 4, of which there are five: (4), $(3,1)$, $(2,2)$, $(2,1,1)$, $(1,1,1,1)$. Elementary divisors for the q-part are in bijection with partitions of 2, of which there are two: (2), $(1,1)$. So there are $10 = 5 \cdot 2$ isomorphism classes of abelian group of order p^4q^2.

Case 3, p, q, r different. Then we are considering groups of order $p^2q^2r^2$. There are $8 = 2 \cdot 2 \cdot 2$ isomorphism classes of abelian group of order $p^2q^2r^2$.

6. Let G be a group of order $245 = 5 \cdot 7^2$. Let F be a Sylow $5-$subgroup and S be a Sylow $7-$subgroup. As $n_5 \equiv 1 \pmod 5$ and $n_5 | 7^2$, we see that $n_5 = 1$, and thus $F \trianglelefteqslant G$. Also $S \trianglelefteqslant G$ since its index is the smallest prime dividing the order of G. By Lagrange's theorem, $F \subset S = \{1\}$, since they have relatively prime orders. Hence by the recognition theorem for direct products, $G \cong F \times S$. Now $F \cong Z_5$, since its order is prime. We previously proved in class that a group of order p^2 is abelian, hence S is either isomorphic to Z_{49} or $Z_7 \times Z_7$. In conclusion, there are two possible isomorphism classes of groups of order 245: $Z_{245} \cong Z_5 \times Z_{49}$ or $Z_{35} \times Z_7 \cong Z_5 \times Z_7 \times Z_7$.

7. By Cauchy's theorem, G has an element of order 7, which generates a subgroup $K \subset G$ of order 7. By Lagrange's theorem, $K \cap H = \{1\}$, since their orders are relatively prime. Hence by the recognition theorem for semi-direct products, $G \cong H \rtimes K$ with respect to a homomorphism $\varphi : K \to \mathrm{Aut}(H)$. As we learned in one of the problem sets, the automorphism group of S_6 has order $2 \cdot 6!$, with the subgroup of inner automorphisms isomorphic to S_6. By Lagrange's theorem, $\mathrm{Aut}(H)$ has no element of order 7, hence φ is the trivial homomorphism. We conclude that $G \cong H \times K \cong S_6 \times Z_7$.

We know that the abelianization of S_7 is isomorphic to Z_2. Since abelianization commutes with direct products, the abelianization of $S_6 \times Z_7$ is isomorphic to $Z_2 \times Z_7$, hence S_7 is not isomorphic to $S_6 \times Z_7$, and hence cannot contain any normal subgroup isomorphic to S_6.

8. By the problem sets, if $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree r, then $\mathbb{F}_p[x]/(f(x))$ is a field of order p^r. Hence we must find irreducible polynomials of degree 3 over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_5$. By the book, we know that a polynomial of degree 3 is irreducible over a field if and only if it has no roots in that field (remember that this is false for polynomials of degree 4 and higher). It's easy to check (by plugging in the elements) that the polynomial $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and $\mathbb{F}_5$ while the polynomial $x^3 + x^2 + x - 1$ is irreducible over $\mathbb{F}_3$.

By the problem sets, we know that if $\mathbb{F}_{p^r}$ is a field of order p^r, then $\mathbb{F}_{p^r}^\times$ is a cyclic group of order $p^r - 1$. In particular, by the structure theory of subgroups of cyclic groups, for every divisor of $p^r - 1$ there is an element of that order. So $\mathbb{F}_8^\times$ has elements of order 1 and 7; $\mathbb{F}_{27}^\times$ has elements of order 1, 2, 13, and 26; and $\mathbb{F}_{125}^\times$ has elements of order 1, 2, 4, 31, 62, and 124.

9. To prove that R is a subring, we need to verify that it is closed under addition, which is obvious, and under multiplication:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + bd & ad + bc \\ bc + ad & bd + ac \end{pmatrix}$$

In fact, R also contains the identity of $M_2(\mathbb{R})$, and the commutativity is apparent from the formula for the product. We can see from the product:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

that R is not an integral domain. Calculating the square of an element:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}^2 = \begin{pmatrix} a^2 + b^2 & 2ab \\ 2ab & a^2 + b^2 \end{pmatrix}$$

we see that to find an idempotent, we must simultaneously solve the equations $a^2 + b^2 = a$ and $2ab = b$ in $\mathbb{R}$. If $b = 0$, then the second is solved, and the first yields $a = 0$ of 1. If $b \neq 0$, then (since $\mathbb{R}$ is a field) we can cancel b from the second equation to get $a = 1/2$, from which the first equation yields $b = \pm 1/2$. Hence the idempotents are:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}$$

To study nilpotent elements, we need to compute powers, and it is most natural to consider eigenvalues. The characteristic polynomial of an element of R is $x^2 - 2ax + a^2 - b^2 = (x - (a - b))(x - (a + b))$. So the eigenvalues are $a \pm b$. Any nilpotent matrix must have all its eigenvalues nilpotent (indeed, if λ is an eigenvalue of A then λ^k is an eigenvalue to A^k, and the zero matrix has all zero eigenvalues), and since we are over a field, all eigenvalues must zero. However, the only way for both $a \pm b = 0$, is that $a = b = 0$, so there are no nonzero nilpotent elements.

Now we consider the map $\varphi : R \to \mathbb{R}$. It is clearly additive; to check that it is multiplicative, we use the above formula for the product, verifying that $(a - b)(c - d) = (ac + bd) - (ad + bc)$. It also preserves identities, so φ is a homomorphism of rings with 1. The kernel consists of all matrices of the form:

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

The map $\ker(\varphi) \to \mathbb{R}$ taking such a matrix to a is clearly a group homomorphism between additive groups (it is not a ring homomorphism, however). Considering scalar multiples of the identity, we see that φ is surjective, hence by the first isomorphism theorem, $R/\ker(\varphi) \cong \mathbb{R}$. In particular, $\ker(\varphi)$ is a maximal ideal, hence by a theorem from class (since we are in a commutative ring), is also a prime ideal.

10. As R is a subring of the $\mathbb{Q}$-quaternions, which is a division ring, we know that a quaternion $x = a + bi + cj + dk$ is invertible if and only if $N(x) = x\overline{x} = a^2 + b^2 + c^2 + d^2$ is a unit in $\mathbb{Z}$, and then the inverse is $\overline{x}/N(x)$. Since $\mathbb{Z}^\times = \{\pm 1\}$, we are left to solve $a^2 + b^2 + c^2 + d^2 = \pm 1$. Since a sum of squares can only be positive, only $a^2 + b^2 + c^2 + d^2 = 1$ is possible, and then the only solutions are (a, b, c, d) of the form $(\pm 1, 0, 0, 0)$, $(0, \pm 1, 0, 0)$, $(0, 0, \pm 1, 0)$, or $(0, 0, 0, \pm 1)$. Hence $R^\times = \{\pm 1, \pm i, \pm j, \pm k\}$ is isomorphic to the quaternion group of order 8.

11. By a problem set exercise, a unit in $R[x]$ must have unit constant term and all other coefficients nilpotent. In $\mathbb{Z}/4\mathbb{Z}$, the only nonzero nilpotent is 2. Hence for each $n \geq 0$, the element $1 + 2x^n \in \mathbb{Z}/4\mathbb{Z}[x]$ will be a unit (in fact, it's its own inverse).

12. Since $\mathbb{Z}/36\mathbb{Z}$ is a cyclic group, any group homomorphism is determined by where it sends 1, and the image of 1 must be an element of order dividing 36. Since $\gcd(36, 48) = 12$, a homomorphism $\varphi : \mathbb{Z}/36\mathbb{Z} \to \mathbb{Z}/48\mathbb{Z}$ must send 1 to an element of order dividing 12, which consists of the subgroup of $\mathbb{Z}/48\mathbb{Z}$ generated by $48/12 = 4$. It is straightforward to check that if $G = \langle g \rangle$ is a cyclic group and H is any abelian groups and $\varphi_1, \varphi_2 \in \mathrm{Hom}(G, H)$ satisfy $\varphi_i(g) = a_i \in H$, then the element $\varphi_1 + \varphi_2 \in \mathrm{Hom}(G, H)$ satisfies $(\varphi_1 + \varphi_2)(g) = a_1 + a_2$, and thus we have that $\mathrm{Hom}(G, H)$ is isomorphic to the subgroup $\{\varphi(g) \,|\, \varphi \in \mathrm{Hom}_Z(G, H)\} \subset H$. Hence $\mathrm{Hom}(\mathbb{Z}/36\mathbb{Z}, \mathbb{Z}/48\mathbb{Z})$ is isomorphic to the subgroup of $\mathbb{Z}/48\mathbb{Z}$ generated by 4, which is a cyclic group of order 12.

Similarly, as additive groups, $\mathrm{Hom}(\mathbb{Z}/36\mathbb{Z}, \mathbb{Z}/36\mathbb{Z})$ and $\mathrm{Hom}(\mathbb{Z}/48\mathbb{Z}, \mathbb{Z}/48\mathbb{Z})$ are cyclic of order 36 and 48, respectively. In fact, it is similarly straightforward to prove that if $G = \langle g \rangle$ is a cyclic group then the map $\mathrm{Hom}(G, G) \to G$ defined by $\varphi \mapsto \varphi(g)$ is multiplicative. In conclusion, this defines a ring isomorphism $\mathrm{Hom}(G, G) \cong G$ for any cyclic group G.

13.
- We discussed how Gauss proved that $\mathbb{Z}[i]$ is a Euclidean domain for the standard norm. This is not isomorphic to either $\mathbb{Z}$ (since it has an element of multiplicative order 4) nor to $F[x]$ for any field F (any such F would have to have characteristic zero, which is impossible, since for example $2 = 1 + 1 \in \mathbb{Z}[i]$ is not invertible but it would be in $F[x]$).
- A Euclidean domain is a PID, as proved in class, so the above example works.
- Technically speaking, a Euclidean domain must be an integral domain, so there are plenty of quotients of $\mathbb{Z}$ (e.g., $\mathbb{Z}/4\mathbb{Z}$) or $F[x]$ (e.g., $F[x]/(x^2)$) that are not integral domains. If we ask whether any quotient of $\mathbb{Z}$ or $F[x]$, which is an integral domain, is Euclidean, then the answer is "yes." Indeed, any quotient of $\mathbb{Z}$ is either $\mathbb{Z}$ itself or is $\mathbb{Z}/n\mathbb{Z}$, which is a domain only when it is a field (remember that finite integral domains are fields). Similarly, any quotient of $F[x]$ is either $F[x]$ itself, or is $F[x]/(f(x))$, which, is a domain if and only if $f(x)$ is irreducible if and only if $F[x]/(f(x))$ is a field. Recall that a field is always Euclidean, with respect to the zero norm.

- As above, technically speaking, a PID must be an integral domain, so there are plenty of quotients of $\mathbb{Z}$ of $F[x]$ that are not integral domains. If a particular quotient is an integral domain, then by the lattice isomorphism theorem, it is a PID.
- In class, it was stated that there are only finitely many imaginary quadratic integer rings that are Euclidean, but many more that are PID. For example, $\mathbb{Z}[(1+\sqrt{-19})/2]$ is one.
- As mentioned in class, $F[x, y]$ is a UFD but not a PID.
- Impossible, any Euclidean domain is a PID.

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: asher.auel@yale.edu