Math 113, Introduction to Abstract Algebra (Kedlaya, fall 2002)
Final exam, Wednesday, December 11, 8–11 AM, 101 Moffitt

This test is closed-book. No calculators, notes or other aids are permitted. There are nine problems (not ten as on the sample exam), and the maximum number of points is 200 (not 250 as on the sample exam).

Please write all answers on the exam sheets; do not use a blue book. I have included one extra page for answers in case you run out of room on a problem (or you may use the back of the page if you prefer), and another extra page for scratch work.

Overall course grades will be posted to BearFacts early next week. Consult the course web page for information about obtaining your final exam grade.

Your name:

Your SID:

Problem 1. Give a one-sentence answer to each of the following questions. (5 points each)

(a) Define a subgroup of a group G.

(b) Give a formula for the number of clements of the alternating group A_n.

(c) Define the product of the groups G and H. (You need to specify the elements of the product, and explain what the group operation is.)

(d) Give a formula for the product of the polynomials $f = f_0 + f_1x + f_2x^2 + \cdots$ and $g = g_0 + g_1x + g_2x^2 + \cdots$. (More precisely, you should give a formula for the coefficient of x^k in fg in terms of the f_i and g_j.)

(e) Give an example of a prime ideal of a ring which is not maximal. (You do not need to provide any further justification.)

(f) Given a nonzero polynomial f over a field F, explain how to construct a field containing F in which f has a root.

Problem 2. Mark each of the following sentences true or false. (Please be clear about which answer goes with each question!) (2 points each)

(a) Any subset S of a group G which is closed under multiplication and contains the identity is a subgroup of G.

(b) Two permutations of $\{1, \ldots, n\}$ are disjoint if and only if they commute.

(c) The product of two cyclic groups is abelian.

(d) Every prime power which divides the order of a finite group G is the order of some subgroup of G.

(e) If $\phi : G \to G'$ is a homomorphism, then $G/\ker(\phi)$ is isomorphic to a subgroup of G'.

(f) Every nonzero element of the ring $\mathbb{Z}_n$ is either a unit or a zero divisor.

(g) The set of elements of a commutative ring which do not have multiplicative inverses is always an ideal.

(h) If p is prime, there is no integer $n < p - 1$ such that $a^n \equiv 1 \pmod{p}$ for all a not divisible by p.

(i) Every prime ideal of a commutative ring with unity is maximal.

(j) For any prime p, $\mathbb{Z}_p[x]/\langle x^2 + 1\rangle$ is a finite field of order p^2.

Problem 3. Let σ and τ denote the permutations of S_7 given by

$$\sigma = (1,5,2,4,3)(6,7), \qquad \tau = (1,6)(2,3,4,5,7).$$

(a) Compute $\sigma\tau$ and $\tau\sigma$. (5 points)

(b) Write σ as a product of transpositions. (5 points)

(c) Find a permutation ρ such that $\rho\sigma\rho^{-1} = \tau$. (5 points)

Problem 4. Let G be the group $\mathbb{Z}_{12} \times \mathbb{Z}_{14} \times \mathbb{Z}_{21}$.

(a) List the elements of a Sylow 2-subgroup of G. (Hint: first figure out how many elements it should have.) (5 points)

(b) Explain why the Sylow theorems guarantee that G has a unique Sylow 2-subgroup. (5 points)

(c) Write G as a product of cyclic groups of prime power order. (5 points)

Problem 5.

(a) Compute 3^{1000} (mod 35). (5 points)

(b) Determine the structure of the group $\mathbb{Z}_{35}^*$ (that is, describe it as a product of cyclic groups of prime power order). (5 points)

(c) How many $a \in \mathbb{Z}_{35}^*$ are there such that $a^2 = 1$? Explain your answer. (5 points)

Problem 6.

(a) Find all integers x such that $x^3 + x^2 - 2x$ is divisible by 24. (10 points)

(b) Find all integers x such that $85x + 10$ is divisible by 30. (5 points)

Problem 7.

(a) Find a nonzero polynomial f over $\mathbb{Q}$, having degree 4 and leading coefficient 1, that has $\sqrt{2} - 2\sqrt{3}$ as a root. (5 points)

(b) Write $x^6 - x^5$ as $q(x)f(x) + r(x)$, where f is the polynomial you found in (a) and $\deg(r) < 4$. (5 points)

(c) Let F be the subfield of $\mathbb{R}$ consisting of elements of the form $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Explain why $\sqrt{2} - 2\sqrt{3}$ does not belong to F. (Hint: it is enough to show that F does not contain a square root of 3.) (5 points)

(d) Find the minimal polynomial of $\sqrt{2} - 2\sqrt{3}$ over F. (5 points)

Problem 8. Define the polynomials $f, g \in \mathbb{Z}_3[x]$ by $f(x) = x^3 + x^2 + x + 2$ and $g(x) = x^3 + 2x + 1$.

(a) Show that f and g are irreducible. (5 points)

(b) Show that there is no isomorphism $\phi : \mathbb{Z}_3[x]/\langle f(x)\rangle \to \mathbb{Z}_3[x]/\langle g(x)\rangle$ such that $\phi(x + \langle f(x)\rangle) = x + \langle g(x)\rangle$. (Hint: evaluate f at $x + \langle g(x)\rangle$.) (5 points)

(c) Find ~~a root of f in $\mathbb{Z}_3[x]/\langle g(x)$~~$\rangle$. (10 points)

Prove that $x^2 + \langle g(x))$ is a root of f.

Problem 9. Give careful proofs of the following statements. An extra page has been provided for your answers in case you need it. (10 points each)

(a) Any nonempty subset H of a group G such that $gh^{-1} \in H$ for any $g, h \in H$ is a subgroup of G.

(b) The symmetric group S_7 has no subgroup of order 15, even though 15 divides the order of S_7. (Hint: we proved in class that every group of order 15 is cyclic.)

(c) There exist infinitely many subgroups H of $\mathbb{Z} \times \mathbb{Z}$ such that $(\mathbb{Z} \times \mathbb{Z})/H$ is isomorphic to $\mathbb{Z}$. (Hint: consider the subgroups generated by $(1, n)$. Make sure to show that the subgroups are all distinct, and that each one has the right quotient.)

(d) For any integers l, m, n, there exists a polynomial P over $\mathbb{Q}$ with $P(l) = 1, P(m) = 2, P(n) = 3$. (Hint: it might be easier to first make a polynomial with $P(l) = 1, P(m) = 0, P(n) = 0$.)

(e) If F is a field of characteristic p (for p a prime number), the set of roots of the polynomial $x^{p^2} + x^p + x$ forms a subgroup of the additive group of F. (Hint: recall that for any $a, b \in F$, $(a + b)^p = a^p + b^p$.)