Algebra Preliminary Examination

Department of Mathematics, University of Denver

Fall 2015 (11 September 2015)

NAME:

INSTRUCTIONS:

- The duration of the exam is 4 hours.
- The exam has three parts, each part consisting of four problems.
- Each problem is worth 10 points.
- All problems from part 1 and the best 6 problems from parts 2 and 3 (combined) will determine your score.
- A score of 70% guarantees a pass.

POINTS:

Problem 1.1	.....	/10
Problem 1.2	.....	/10
Problem 1.3	.....	/10
Problem 1.4	.....	/10
Problem 2.1	.....	/10
Problem 2.2	.....	/10
Problem 2.3	.....	/10
Problem 2.4	.....	/10
Problem 3.1	.....	/10
Problem 3.2	.....	/10
Problem 3.3	.....	/10
Problem 3.4	.....	/10

TOTAL POINTS: PERCENTAGE: PASSED: Yes No

Part 1: Introduction to Abstract Algebra

Problem 1.1: Let S_7 denote the group of permutations of $\{1, 2, 3, 4, 5, 6, 7\}$.

(a) [4 points] What is the maximal order of elements of S_7? Find an element of maximal order, and determine how many conjugacy classes of such elements there are.

(b) [4 points] How many conjugacy classes of elements of order 6 does S_7 contain? Give a representative for each conjugacy class of elements of order 6.

(c) [2 points] Give a smallest generating set for S_7.

Problem 1.2: Let R be a commutative ring with unit, and let I, J be ideals of R.

(a) [3 points] Show that $R/I \times R/J$ is a ring with coordinate-wise addition and multiplication, and the map $\phi : R \to R/I \times R/J$ given by $r \mapsto (r + I, r + J)$ is a ring homomorphism.

(b) [5 points] We call I, J *comaximal* if $I + J = R$. Equivalently, $x + y = 1$ for some $x \in I$ and $y \in J$. Show that ϕ is surjective if and only if I, J are comaximal.

(c) [2 points] Show that if I, J are comaximal, $R/(I \cap J) \cong R/I \times R/J$.

Problem 1.3: Let S be a finite semigroup such that there exists a and b in S with $aS = S$ and $Sb = S$. Prove that S is a group. [Recall that a semigroup is a set endowed with an associative binary operation.]

Problem 1.4: Define the *infinite dihedral group* D_∞ to be the group of symmetries of the line of integers. More precisely, D_∞ consists of all bijections $f : \mathbb{Z} \to \mathbb{Z}$ such that $|f(n) - f(n + 1)| = 1$ for all $n \in \mathbb{Z}$, under composition.

(a) [3 points] Show that every element of D_∞ is either a shift or the composition of a shift with the inversion map $\sigma(n) = -n$.

(b) [2 points] Find a two-element generating set for D_∞.

(c) [3 points] Prove that D_∞ is isomorphic to the group generated by the matrices

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}$$

under multiplication.

(d) [2 points] Prove that D_∞ it also isomorphic to the group $\mathbb{Z} \times \{-1, 1\}$ under the operation $(a, b) * (c, d) = (a + bc, bd)$.

Part 2: Group Theory

Problem 2.1: Prove that every group G of order 2015 contains a cyclic normal subgroup H such that G/H is cyclic.

Problem 2.2: Recall that a group G is solvable if there exists an ascending subnormal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

where each G_{i+1}/G_i is abelian. Let G be a group and let N be a normal subgroup of G. Suppose N and G/N are solvable. Prove that G is solvable.

Problem 2.3: Let G be a group and let $N \trianglelefteq G$ be such that $\mathrm{Aut}(N) = \mathrm{Inn}(N)$. Show that every coset of N has a representative in $C_G(N)$, the centralizer of N in G. In other words, show that for every $g \in G$, there exists $a \in C_G(N)$ such that $g \in aN$.

Problem 2.4: Let G be a finite group which is the internal direct product of subgroups H and K (namely that $G = HK$, H and K intersect trivially and every element of H commutes with every element of K). Also, let M be a subgroup of G.

(a) [3 points] Show by example that M does not have to have the form H_1K_1 for some $H_1 \leq H$, $K_1 \leq K$.
(b) [7 points] Now suppose $|H|$ and $|K|$ are relatively prime. Show that M is the internal direct product of some H_1 and K_1, where $H_1 \leq H$ and $K_1 \leq K$.

Part 3: Rings and Fields

Problem 3.1: Give an example of five of the following, or explain why no such example exists. [2 points each]

(a) An irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$.
(b) A ring with exactly 2 invertible elements, which is not a field.
(c) A polynomial in $\mathbb{Z}[x]$ that is irreducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{Q}[x]$.
(d) A polynomial in $\mathbb{Z}[x]$ that is reducible in $\mathbb{Z}[x]$ but irreducible in $\mathbb{Q}[x]$.
(e) A UFD that is not Noetherian.
(f) A finite non-commutative ring which has a nontrivial 2-sided ideal.
(g) A polynomial of degree 4 whose Galois group is the Klein 4-group.
(h) A field in which the polynomial $x^7 - 2$ has exactly one root.

Problem 3.2: Let R be an integral domain.

(a) [6 points] If R is a PID, show that if $I \subseteq R$ is any nonzero ideal, there are only finitely many ideals of R containing I.
(b) [4 points] If R is Noetherian (but not necessarily a PID), is it still true that given a nonzero ideal $I \subseteq R$, there are only finitely many ideals of R containing I? Justify your answer by giving either a proof or a counterexample.

Problem 3.3: Let $f(x) \in \mathbb{Q}[x]$ be a cubic polynomial whose Galois group is cyclic of order 3. Show that all roots of $f(x)$ are real.

Problem 3.4: Let $\alpha = \sqrt{5 + 2\sqrt{5}}$

(a) [2 points] Find a monic polynomial $f(x)$ of degree 4 over $\mathbb{Z}$ having α as a root.
(b) [3 points] Show that $f(x)$ is irreducible, and find the remaining roots of $f(x)$.
(c) [5 points] Show that the splitting field K of f over $\mathbb{Q}$ satisfies $[K : \mathbb{Q}] = 4$, and determine the Galois group $G = \mathrm{Aut}(K/\mathbb{Q})$.

Solutions

Problem 1.1:

(a) The maximal order is 12. A product of a 3-cycle and a 4-cycle such as (1 2 3)(4 5 6 7) has order 12, and there is only one such conjugacy class.

(b) There are three such conjugacy classes: the 6-cycles such as (1 2 3 4 5 6), the products of a 2-cycle and a 3-cycle such as (1 2)(3 4 5), and the products of two 2-cycles and a 3-cycle such as (1 2)(3 4)(5 6 7).

(c) S_7 is generated by (1 2 3 4 5 6 7) and (1 2).

Problem 1.2:

(a) Obvious.

(b) Suppose that I, J are comaximal. Fix $x \in I$ and $y \in J$ such that $x + y = 1$. Let $(a + I, b + J)$ be an arbitrary element of $R/I \times R/J$. Note that $ax + ay = a$ and $bx + by = b$. Taking $r = ay + bx$, we have $r + I = ay + I = a + I$ and $r + J = ay + bx + J = bx + J = b + J$, so $\phi(r) = (a + I, b + J)$, and ϕ is surjective. Conversely, if ϕ is surjective, then $\phi(x) = (0 + I, 1 + J)$ for some $x \in R$. Since $x + I = 0 + I$ we have $x \in I$, and since $x + J = 1 + J$, there exists $y \in J$ such that $x + y = 1$.

(c) The kernel of ϕ is clearly $I \cap J$ for any I, J, not necessarily comaximal. So the claim follows from (b).

Problem 1.3 It suffices to show that there is a neutral element 1 as then, because of finiteness, for every x in S there will be an positive integer n such that $x^n = 1$, and x^{n-1} will be the inverse of x. To show that have a neutral element, note that by assumption left multiplication by a is surjective, so it has to also be injective, because of finiteness, hence a permutation on S. So, there is a natural number k such that $a^k x = x$ for all $x \in S$, namely a^k is left neutral. Likewise, b^m is right neutral for some m, and so we have a unique neutral element, by the usual short argument.

Problem 1.4

(a) Let $f \in D_\infty$ and let $n = f(0)$. Then $f(1) = n + 1$ or $f(1) = n - 1$. In the first case, $f(k) = n + k$ by induction for all $k > 0$, and $f(-1) = n - 1$, so again by induction $f(k) = n + k$ for all $k \in \mathbb{Z}$. Therefore f is a shift by n. In the second case, the same argument shows that $f(k) = n - k$ for all $k \in \mathbb{Z}$, so f has the desired form.

(b) D_∞ is generated by the inversion map $\sigma(n) = -n$ and the shift by one $\tau(n) = n + 1$. Note that they satisfy the conditions $\sigma^2 = 1$ and $\tau\sigma\tau\sigma = 1$.

(c) Set

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

And note that $T = AB$ and $S = AT^{-1}$, and also that $A = ST$ and $B = A^{-1}T$, so the sets $\{A, B\}$ and $\{T, S\}$ generate the same subgroup. Also, we can check that $S^2 = I$ and that $TSTS = I$.

(d) Note that $\mathbb{Z} \times \{-1, 1\}$ is generated as a group by $(0, -1)$ and $(1, 1)$. Define a map $\mathbb{Z} \times \{-1, 1\} \to D_\infty$ by $(0, -1) \mapsto \sigma$ and $(1, 1) \mapsto \tau$. This is easily seen to be an isomorphism.

Problem 2.1:

We have $2015 = 5 * 13 * 31$. The number of Sylow 31-subgroups divides $5 * 13 = 65$ and is congruent to 1 modulo 31, thus it is equal to 1. So there is a unique normal subgroup H of order 31 in G, necessarily cyclic. The group G/H has order $5 * 13 = 65$, so it suffices to prove that every group K of order 65 is cyclic. In K, both the Sylow 13-subgroup and the Sylow 5-subgroup are normal (standard counting), they generate K, and they intersect trivially (by Lagrange, say). Hence K is the direct product of Z_5 and Z_{13}. Because $\gcd(5, 13) = 1$, K is cyclic.

Problem 2.2: Recall that G is solvable if and only if $G^{(n)} = 1$ for some n. Here $G^{(0)} = G$, $G^{(1)} = [G, G]$, and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for all $i \geq 1$. Moreover, if $f : G \to H$ is a surjective homomorphism, we have $f(G^{(i)}) = H^{(i)}$ for all i. Suppose that N is a normal subgroup of G, and that N and G/N are both solvable. Then $(G/N)^{(n)} = 1$ for some n. Letting $f : G \to G/N$ be the projection, we have $f(G^{(n)}) = (G/N)^{(n)} = 1$, so that $G^{(n)} \subseteq N$. Since N is solvable, $N^{(m)} = 1$ for some m, so $G^{(n+m)} = 1$.

Problem 2.3: For $g \in G$, define $\gamma_g : G \to G$ by $\gamma_g(x) = gxg^{-1}$. Then the restriction of γ_g to N is an automorphism of N since N is normal in G. Since $\mathrm{Aut}(N) = \mathrm{Inn}(N)$, there is $n \in N$ such that $\gamma_g(m) = \gamma_n(m)$ for every $m \in N$, i.e., $gmg^{-1} = nmn^{-1}$. But then $n^{-1}gmg^{-1}n = m$, so $n^{-1}g \in C_G(N)$. Setting $a = n^{-1}g$, we have $g = na \in Na = aN$, as claimed.

Problem 2.4:

(a) Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, say, and consider $M = \{(a, a) | a \in N\}$.

(b) Set $H_1 = M \cap H$, $K_1 = M \cap K$. For $g \in M$, write $g = hk$ where $h \in H$, $k \in K$. Let r, s be the orders of h, k, respectively. Then $g^r = k^r \in K_1$ and $g^s = h^s \in H_1$. Since r, s are relatively prime, k^r generates $\langle k \rangle$ and h^s generates $\langle h \rangle$. Thus $\langle h \rangle \leq H_1$ and $\langle k \rangle \leq K_1$. In particular, $h \in H_1$, $k \in K_1$. Therefore $M = H_1K_1$ and we already knew $H_1 \cap K_1 = 1$, so we are done.

Problem 3.1:

(a) $f(x) = x^3 + 2x + 1$.
(b) $\mathbb{Z}_6$.
(c) Does not exist, by the Gauss lemma.
(d) $f(x) = 2x$.
(e) The polynomial ring $\mathbb{C}[x_1, x_2, \dots]$ on infinitely many variables.
(f) The ring of $n \times n$ matrices over $\mathbb{Z}_m$ for any $n \geq 2$ and $m \geq 4$, with m not prime.
(g) $f(x) = (x^2 - 2)(x^2 - 3)$.
(h) $\mathbb{Q}[\xi]$ where ξ is the positive real seventh root of 2.

Problem 3.2:

(a) Since R is a PID, $I = (a)$ some nonzero $a \in R$. Given an ideal J containing I, we have $J = (b)$ for some $b \in R$, and $I \subseteq J$ means that $b|a$. Recall that R is a UFD, so a has a factorization

$$a = u\pi_1^{r_1} \cdots \pi_n^{r_n},$$

where u is a unit, each π_i is irreducible and uniquely determined up to associates, and each $r_i \geq 1$. In particular, b must be a product of irreducible factors of a, up to associates. So the ideals J containing I are in bijection with factors of a of the form $\pi_1^{s_1} \cdots \pi_n^{s_n}$ with $0 \leq s_i \leq r_i$.

(b) It is not true. Here is a counterexample. Consider the polynomial ring $\mathbb{C}[x, y]$, which is Noetherian by Hilbert's basis theorem, and let $I = (x)$. Let $J_n = (x, y^n)$ for $n \geq 1$. We have $I \subseteq J_n$ for each n but the J_n's are all distinct.

Problem 3.3:

Let $f(x) \in \mathbb{Q}[x]$ be a cubic whose Galois group is cyclic of order 3, so the splitting field E is a degree 3 extension of $\mathbb{Q}$. In particular $f(x)$ is irreducible over $\mathbb{Q}$, since otherwise E would be either $\mathbb{Q}$ or a degree 2 extension. By continuity, $f(x)$ must have at least one real root α, and since $f(x)$ is irreducible, $\mathbb{Q}(\alpha)$ must be a degree 3 extension of $\mathbb{Q}$. Therefore $[E : \mathbb{Q}(\alpha)] = 1$, so $E = \mathbb{Q}(\alpha)$. It follows that the other roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$, and therefore must be real.

Problem 3.4:

(a) $\alpha_1 = \sqrt{5 + 2\sqrt{5}}$ satisfies the polynomial $f(x) = x^4 - 10x^2 + 5$.

(b) By Eisenstein's criterion with $p = 5$, $f(x)$ is irreducible. The remaining roots are

$$\alpha_2 = -\sqrt{5 + 2\sqrt{5}}, \qquad \alpha_3 = \sqrt{5 - 2\sqrt{5}}, \qquad \alpha_4 = -\sqrt{5 - 2\sqrt{5}}.$$

(c) Since $f(x)$ is irreducible, it is the minimal polynomial of α_1 over $\mathbb{Q}$, so $\mathbb{Q}(\alpha_1)$ is a degree 4 extension of $\mathbb{Q}$. Since $\sqrt{5} = \frac{\alpha_1^2 - 5}{2}$ and $\alpha_3 = \frac{\sqrt{5}}{\alpha_1}$, it is immediate that $\mathbb{Q}(\alpha_1)$ contains α_2, α_3, α_4, so $\mathbb{Q}(\alpha_1)$ must be the splitting field of $f(x)$. It follows that $G = \mathrm{Aut}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ has degree 4. So G is either the cyclic group C_4 or the Klein 4-group V_4. But $G \neq V_4$ since $\mathbb{Q}(\alpha_1)$ only has one subfield of degree 2 over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{5})$, but if $G = V_4$, $\mathbb{Q}(\alpha_1)$ would have three such subfields.