Algebra Preliminary Examination

Department of Mathematics, University of Denver

Fall 2014 (5 September 2014)

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 p be an odd prime. An element x of $\mathbb{Z}_p$ is a *square* if there is $y \in \mathbb{Z}_p$ such that $y^2 = x$.

(a) [3 points] Show that there are precisely $(p+1)/2$ squares in $\mathbb{Z}_p$.

(b) [7 points] Let d be a nonzero element of $\mathbb{Z}_p$ that is not a square. Let $\sqrt{d}$ be a symbol, and let $R = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}_p\}$ be equipped with the operations

$$(x + y\sqrt{d}) + (u + v\sqrt{d}) = (x + u) + (y + v)\sqrt{d},$$
$$(x + y\sqrt{d}) * (u + v\sqrt{d}) = (xu + yvd) + (xv + yu)\sqrt{d}.$$

Prove that R is a field of order p^2. Either give all details by calculations, or explain why the details can be skipped.

Problem 1.2: Let R be a commutative ring, and let $S = R[x]$.

(a) [2 points] Show that S has a subring isomorphic to R.

(b) [6 points] Show that S has a quotient ring isomorphic to R.

(c) [2 points] Can an isomorphic copy of $\mathbb{R}$ occur as a subring or quotient ring of $\mathbb{Z}[x]$?

Problem 1.3: A group G is said to be *capable* if it is isomorphic to the inner automorphism group $\mathrm{Inn}(H)$ of some group H.

(a) [4 points] Prove that no capable group of prime order exists.

(b) [6 points] Prove that the symmetric group S_n is capable if and only if $n \neq 2$, giving all details.

Problem 1.4: Let $(G, \cdot)$ be a finite set G with a binary operation $\cdot : G \times G \to G$ such that for each $x \in G$, the mapping $L_x : G \to G$ defined by $L_x(y) = xy$ for all $y \in G$ is a bijection. Suppose $H \subseteq G$ is closed under $\cdot$ and satisfies the following property: $(xh)H = xH$ for every $x \in G$, $h \in H$. Prove that $|H|$ divides $|G|$.
(*Hint*: Recall how Lagrange's Theorem for groups is proved.)

Part 2: Group Theory

Problem 2.1: Prove that the alternating group A_6 has no subgroups of prime index.
(*Hint*: For such a subgroup H, consider the action of A_6 on the left cosets of H.)

Problem 2.2: Prove that every group of order $255 = 3 \cdot 5 \cdot 17$ is abelian.
(*Hint*: Recall that whenever a factor group G/H is abelian, the commutator subgroup G' is contained in H.)

Problem 2.3: Prove that the following two statements are equivalent, that is, if you assume either statement to be true, then the other one is also true. *Do not try to prove either statement!*

(a) Every finite group of odd order is solvable.

(b) Every finite nonabelian simple group has even order.

Problem 2.4: Let G be a finite group and let $\Phi(G)$ denote the Frattini subgroup of G, that is, the intersection of all maximal subgroups of G.

(a) [6 points] Prove that $\Phi(G)$ is precisely the set of all nongenerators of G. (An element $a \in G$ is a nongenerator if, whenever $G = \langle a, S\rangle$ for some $S \subseteq G$, it follows that $G = \langle S\rangle$. Informally, a can be removed from any set of generators of G.)

(b) [4 points] Prove that every Sylow subgroup of $\Phi(G)$ is normal in G. (*Hint*: the Frattini argument might be helpful.)

Part 3: Rings and Fields

Problem 3.1: Give an example of each of the following [1 point each].

(a) An irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$.
(b) A polynomial in $\mathbb{Z}[x]$ that is reducible in $\mathbb{Z}[x]$ but irreducible in $\mathbb{Q}[x]$.
(c) A PID that is not a Euclidean domain.
(d) A UFD that is not a PID.
(e) An integral domain that is not a UFD.
(f) A nontrivial prime ideal of a commutative ring that is not a maximal ideal.
(g) An irreducible element of an integral domain that is not a prime element.
(h) A finite noncommutative ring.
(i) A commutative ring that has exactly one maximal ideal, and is not a field.
(j) A field in which the polynomial $x^3 - 2$ has exactly one root.

Problem 3.2:

(a) [7 points] Show that $(2, x)$ is a maximal ideal but not a principal ideal in $\mathbb{Z}[x]$.
(b) [3 points] Show that if F is a field, $F[x, y]$ is not a PID.

Problem 3.3: Let R be a unital, commutative ring, and let $M_n(R)$ denote the ring of $n \times n$ matrices with coefficients in R.

(a) [4 points] Prove that $M_n(I)$ is an ideal of $M_n(R)$ whenever I is an ideal of R.
(b) [4 points] Prove that every ideal of $M_n(R)$ has this form.
(c) [2 points] Prove that if F is a field, $M_n(F)$ is simple.

Problem 3.4: Consider the polynomial $f(x) = x^4 - 2x^2 - 1$ over $\mathbb{Q}$.

(a) [2 points] Show that $f(x)$ is irreducible over $\mathbb{Q}$.
(b) [4 points] Find the roots of $f(x)$ and determine the splitting field K of $f(x)$.
(c) [4 points] Show that $[K : \mathbb{Q}] = 8$.

Solutions

Problem 1.1: (i) Consider the squaring map $x \mapsto x^2$. Since $x^2 = y^2$ iff $(x+y)(x-y) = 0$ iff $x = y$ or $x = -y$, the squaring map is 2-to-1 on $\mathbb{Z}_p^*$. Of course, 0 is a square, so we get $(p-1)/2 + 1 = (p+1)/2$ squares.

(ii) Everything is routine. For the multiplicative inverse of $x + y\sqrt{d}$: If $y = 0$, we are back in $\mathbb{Z}_p$ and we merely need $x \neq 0$. If $y \neq 0$, then $x + y\sqrt{d}$ has an inverse iff $x^2 - y^2 d \neq 0$, which is equivalent to $d \neq (x/y)^2$, which is satisfied thanks to the assumption that d is not a square.

Problem 1.2: (i) The mapping $R \to S[x]$, $r \mapsto r$ is an embedding.

(ii) The mapping $S \to R$, $\sum_i f_i x^i \mapsto f_0$ is a homomorphism whose image is R and whose kernel is the ideal (x). Hence $R \cong S/(x)$.

(iii) This is not possible since $\mathbb{R}$ is uncountable, while $\mathbb{Z}[x] = \mathbb{Z} \cup (\mathbb{Z} + x\mathbb{Z}) \cup (\mathbb{Z} + x\mathbb{Z} + x^2\mathbb{Z}) \cup \cdots$ is countable, being a countable union of countable sets.

Problem 1.3 (i) Recall that $\mathrm{Inn}(H) \cong H/Z(H)$. Suppose that G is of prime order and capable, $G \cong H/Z(H)$. Then $H/Z(H)$ is cyclic, hence H is abelian, hence $H/Z(H) = 1$, a contradiction.

(ii) The group $S_1 = S_1/Z(S_1)$ is capable. The group S_2 is not capable by (i). Suppose that $n > 2$. We claim that $Z(S_n) = 1$. Let $1 \neq \pi \in S_n$. If π has $(abc\dots)$ in its cycle decomposition, the calculation of $\pi * (ab)$, $(ab) * \pi$ takes place within the cycle $(abc\dots)$, and we have $(abc\dots) * (ab) \neq (ab) * (abc\dots)$, so $\pi * (ab) \neq (ab) * \pi$ and $\pi \notin Z(S_n)$. Suppose that π is a product of 2-cycles. If $(ab)(cd)$ is in the decompotision of π, check that $(ab)(cd) * (ac) \neq (ac) * (ab)(cd)$. If π is a transposition (ab), then $n > 2$ gives us $c \notin \{a, b\}$ and then $\pi * (ac) \neq (ac) * \pi$.

We have proved that $Z(S_n) = 1$. Thus $S_n \cong S_n/Z(S_n)$ is capable.

Problem 1.4 It suffices to prove that if $xH \cap yH \neq \emptyset$ then $xH = yH$: then we have a partition of G into cosets xH, and all such cosets have the same cardinality as H because all left translations L_x are bijections. Thus suppose that $z \in xH \cap yH$. Then $z = xh_1 = yh_2$ for some $h_i \in H$. Therefore $xH = (xh_1)H = (yh_2)H = yH$, as desired.

Problem 2.1: Let H be a subgroup of A_6 of prime index p. The action of A_6 on left cosets of H induces a homomorphism $\phi : A_6 \to S_p$. Since A_6 is simple, the kernel of ϕ must be trivial. Thus A_6 embeds in S_p and so $|A_6|$ divides $|S_p|$, that is, 360 divides $p!$. This cannot happen for $p = 2, 3, 5$, the only possibilities.

Problem 2.2: Let G be such a group. Then n_{17} divides 15 and is congruent to 1 mod 17, so $n_{17} = 1$. Thus G has a normal subgroup N of order 17. If $n_3 > 1$, then G has 85 subgroups of order 3, hence 170 elements of order 3, since the intersection of distinct subgroups of order 3 is trivial. Similarly, if $n_5 > 1$, then G has 51 subgroups of order 5, hence 204 elements of order 5. We cannot have both of these things occurring since $170 + 204 > 255$. Thus G has a normal subgroup K of order 3 or of order 5. Now $|G/N| = 15$, so G/N is an abelian group since 3 does not divide $5 - 1 = 4$. Also, $|G/K| = 3 \cdot 17$ or $5 \cdot 17$. In either case, G/K is abelian since neither 3 nor 5 divides $17 - 1 = 16$. Since both G/N and G/K are abelian

groups, we must have that G is contained in both N and K. But $N \cap K = \{1\}$. Thus $G = \{1\}$, that is, G is abelian.

Problem 2.3: (a) $\Longrightarrow$ (b): If G is a finite simple group of odd order, then by (a), G is both solvable and simple, hence abelian.

(b) $\Longrightarrow$ (a): Let G be a group of odd order.

Proof 1: Any composition factor of G is a simple group and also has odd order by Lagrange's theorem. By (b), such a composition factor must be abelian, hence cyclic of prime order. Since every composition factor is cyclic of prime order, G is solvable.

Proof 2: Assume G is a minimal counterexample. If N is a nontrivial proper normal subgroup of G, then since both N and G/N have odd order, each is solvable by the minimality of G. But then G is solvable, a contradiction. Therefore G has no nontrivial proper normal subgroups, that is, G is simple. By (b), G must be abelian, another contradiction.

Problem 2.4: (a) Suppose a is a nongenerator and suppose $M < G$ is a maximal subgroup. If $a \notin M$, then $\langle a, M\rangle = G$, and so $M = \langle M\rangle = G$. Thus every nongenerator is contained in every maximal subgroup, that is, $\Phi(G)$ is contained in the intersection of all maximal subgroups. Conversely, suppose a in that intersection, and suppose $G = \langle a, S\rangle$ for some $S \subseteq G$. If $\langle S\rangle \neq G$, then $\langle S\rangle \leq M < G$ for some maximal subgroup M. But $a \in M$, so $\langle a, S\rangle \leq M$, a contradiction.

(b) Suppose P is a Sylow p-subgroup of $\Phi(G)$. Since $\Phi(G)$ is normal in G, $G = \Phi(G)N_G(P)$ by the Frattini Argument. But $\Phi(G)$ consists of nongenerators of G, so $G = N_G(P)$.

Problem 3.1:

(a) $x^3 + 2x^2 + 1$.
(b) $2x$.
(c) $\mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-19}}{2}$.
(d) $F[x, y]$ for any field F.
(e) $R = \mathbb{Z}[\sqrt{-5}]$. Then $2 \cdot 3 = 6 = (1 - \sqrt{-5})(1 + \sqrt{5})$, which are distinct factorizations into irreducibles.
(f) $(x) \subset \mathbb{Z}[x]$.
(g) Take $R = \mathbb{Z}[\sqrt{-5}]$. The element 3 is irreducible in R but not prime since $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$, but 3 does not divide $2 \pm \sqrt{-5}$.
(h) The unit quaternions.
(i) The localization of $\mathbb{Z}$ at the prime ideal (2). This consists of all rational numbers $\frac{p}{q}$ where q is not divisible by 2.
(j) $\mathbb{Q}[\xi]$ where ξ is the positive real cube root of 2.

Problem 3.2:

(a) Clearly $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$, which is a field, so $(2, x)$ is maximal. Suppose that $(2, x) = (f(x))$ for some $f(x) \in \mathbb{Z}[x]$. Since $2 \in (f(x))$, we have $2 = p(x)f(x)$ for some $p(x) \in \mathbb{Z}[x]$. Since $\mathbb{Z}$ is an integral domain, we have $\deg(p(x)f(x)) = \deg(p(x)) + \deg(f(x)) = 0$, so both $p(x)$ and $f(x)$ lie in $\mathbb{Z}$. Since 2 is prime, both $p(x)$ and $f(x)$ are either ± 1 or ± 2, and since $(2, x)$ is a proper ideal (check this!), $f(x) = \pm 2$. But $x \in (f(x)) = (2)$, which is impossible since any multiple of 2 is a polynomial with even coefficients.

(b) Let $a \in R$ be an arbitrary irreducible element. By the same argument as Part (a), the ideal $(a, x) \in R[x]$ is not principal.
(c) Let $R = F[x]$, which is an integral domain that is not a field. Since $F[x, y] = R[y]$, this follows from Part (b).

Problem 3.3:

(a) Let $I \subset R$ is an ideal. Clearly the zero matrix lies in $M_n(I)$ since $0 \in I$, and $M_n(I)$ is an abelian group under matrix addition. Given an arbitrary matrix $A = (a_{ij}) \in M_n(R)$ and $B = (b_{ij}) \in M_n(I)$, the kl^{th} entry of AB is $\sum_{i=1}^{n} a_{ki}b_{il}$, which lies in I since I is an ideal of R. Similarly, each entry of BA lies in I, so $M_n(I)$ is a 2-sided ideal of $M_n(R)$. (Note that it's necessary to show $M_n(I)$ is a 2-sided ideal since $M_n(R)$ is noncommutative).
(b) Let $J \subset M_n(R)$ be a 2-sided ideal. If $J = M_n(R)$ or $J = 0$ there is nothing to prove, so assume J is a nontrivial, proper ideal. Define $I \subset R$ to be the set consisting of all $b \in R$ such that b appears as an entry of a matrix $B \in J$.

First, we claim that I is an ideal. If $b = b_{ij}$ for some $B = (b_{ij}) \in J$, we can multiply B on the left by E_{ii} and on the right by E_{jj} to obtain $bE_{ij} \in J$. (Here bE_{ij} is the matrix with b in the ij^{th} slot and all other entries zero). Multiplying on the left by E_{1i} and on the right by E_{j1} we have $bE_{11} \in J$. Since the map $R \to M_n(R)$ sending $r \mapsto rE_{11}$ is a ring homomorphism, it is easy to check that I is an ideal of R.

By definition, $J \subset M_n(I)$. To show that $M_n(I) \subset J$, it suffices to show that for each $b \in I$, $bE_{kl} \in J$ for all $k, l = 1, \ldots, n$. But this is clear from the above discussion. There exists $B = (b_{ij}) \in J$ such that $b = b_{ij}$, so $bE_{ij} \in J$. Multiplying on the left by E_{ki} and on the right by E_{jl}, we get $bE_{kl} \in J$.
(c) This is immediate from Parts (a) and (b) since F has no ideals other that (0) and F.

Problem 3.4:

(a) This follows from Eisenstein's criterion with $p = 2$. Alternatively, by the Rational Roots Theorem, the only possible rational roots are 1 and -1, neither of which works.
(b) The roots of $y^2 - 2y - 1$ are $1 \pm \sqrt{2}$, so the roots of $f(x)$ are

$$\alpha_1 = \sqrt{1+\sqrt{2}}, \qquad \alpha_2 = -\sqrt{1+\sqrt{2}}, \qquad \alpha_3 = \sqrt{1-\sqrt{2}}, \qquad \alpha_4 = -\sqrt{1-\sqrt{2}}.$$

Note that $\mathbb{Q}(\alpha_1)$ does not contain α_3 or α_4 since $\alpha_1 \in \mathbb{R}$, but $\alpha_3, \alpha_4 \notin \mathbb{R}$. So the splitting field K must contain $\mathbb{Q}(\alpha_1, \alpha_3)$. But $\alpha_2, \alpha_4 \in \mathbb{Q}(\alpha_1, \alpha_3)$, so $K = \mathbb{Q}(\alpha_1, \alpha_3)$.
(c) Since $f(x)$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$. Since $\alpha_3 \notin \mathbb{Q}(\alpha_1)$, we have $[K : \mathbb{Q}(\alpha_1)] > 1$. Note that $(\alpha_1)^2 = 1 + \sqrt{2}$, so $\sqrt{2} \in \mathbb{Q}(\alpha_1)$. Since $(\alpha_3)^2 = 1 - \sqrt{2} \in \mathbb{Q}(\alpha_1)$, we see that α_3 satisfies a polynomial of degree 2 over $\mathbb{Q}(\alpha_1)$. Therefore $[K, \mathbb{Q}(\alpha_1)] \leq 2$, so $[K : \mathbb{Q}(\alpha_1)] = 2$. Finally, this implies that

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = (2)(4) = 8.$$