MATHEMATICS
University of Gothenburg and Chalmers University of Technology
Examination in algebra: MMG 500 and MVE 150, 2023-03-17.
No books, written notes or any other aids are allowed.
Telephone: 031-41 46 70, 031-772 3580 ; e-mail: salberg@chalmers.se

1) There exists a group G of order 8 with six elements of order 4.

a) Show that G is not isomorphic to the symmetry group of a square. 2p

b) Show that G cannot be abelian. (Hint: Use a theorem in Durbin's book.) 3p

2) Consider the problem of painting the squares of a 8×8 chessboard red or blue. Suppose that we view two paintings as indistinguishable if one of them can be obtained from the other by rotating the chessboard on the table. Show that there are exactly $2^{62}+2^{30}+2^{15}$ such indistinguishable paintings. 4p

3) Let R be a commutative ring, I and J be two ideals of R and $I+J$ be the set of all sums $i+j$ where $i \in I$ and $j \in J$. Show that $I+J$ is an ideal of R. 4p

(Do not forget to verify *all* conditions that a subset of a ring must satisfy to be an ideal.)

4) Write x^7-x as a product of irreducible monic polynomials in $\mathbf{Z}_3[x]$. 4p

(Hint : A solution does not require much computation.)

5) Let S be a set and ~ an equivalence relation on S. Show that the set of equivalence classes of ~ forms a partition of S. 4p

6) Let K be a field and $K[x]$ be the ring of all polynomials over K. Show that all ideals of $K[x]$ are principal ideals. 4p

You may use all theorems in Durbin's book to solve the first four problems, but it is important that you motivate your claims.

MATHEMATICS
University of Gothenburg and Chalmers University of Technology
Examination in algebra: MMG 500 and MVE 150, 2023-06-07.
No books, written notes or any other aids are allowed.
Telephone: 031-41 46 70, 031-772 3580 ; e-mail: salberg@chalmers.se

1) Let α and β be two rational numbers and A be the set of all linear combinations $m\alpha+n\beta$ with integer cofficients m and n.

a) Show that A is a subgroup of the additive group $\mathbf{Q}$. 2p

b) Prove that A is cyclic. 3p

2) Let G be a group acting transitively on a set S such that the stabiliser $G_t=\{e\}$ for some $t\in S$. Prove that $G_s=\{e\}$ for all $s\in S$. 4p

3) Let $\varphi: R\to S$ be a ring homomorphism and J be an ideal of S. Show that the inverse image $I=\varphi^{-1}(J)=\{r\in R : \varphi(r)\in J\}$ is an ideal of R. 4p

4) Construct a field extension of $\mathbf{Z}_3$ with 27 elements. 4p
(It is not enough to refer to general existence results on fields with p^n elements.)

5) Let G be a group and H be a subgroup of G. Let $\sim$ be the relation on G where $a\sim b$ if and only if $ab^{-1}\in H$.

a) Prove that $\sim$ is an equivalence relation. 2p

b) Prove that the right cosets of H in G form a partition of G and that $o(H)$ divides $o(G)$ if G is finite. 3p

(You may use general results on equivalence relations on sets without proofs.)

6) Show that a polynomial of degree $n\geq 1$ over a field F has at most n zeros in F. 3p

You may use the theorems in Durbin's book to solve the first four problems, but it is important that you motivate your claims.

MATHEMATICS
University of Gothenburg and Chalmers University of Technology
Examination in algebra: MMG 500 and MVE 150, 2023-08-14.
No books, written notes or any other aids are allowed.
Telephone: 031-41 46 70, 031-772 3580 ; e-mail: salberg@chalmers.se

1) Let F be a field with the property :

(*) If $c, d \in F$ and $c^2 + d^2 = 0$, then $c = 0$ and $d = 0$.

(a) Show that $x^2 + 1$ is irreducible in $F[x]$. 2p

(b) Which of the fields $\mathbf{Z}_3$, $\mathbf{Z}_5$ satisfy (*) ? 2p

2) Let G and H be finite groups with $(|G|, |H|) = 1$. Show that if $\phi : G \to H$ is a homomorphism, then $\phi(g) = e_H$ for all $g \in G$. (Here e_H is the neutral element of H.) 4p

3) How many elements of order 12 are there in S_7 ? 4p

4) Let $\phi : \mathbf{Z}[x] \to \mathbf{Z}[x]$ be a ring automorphism of the polynomial ring $\mathbf{Z}[x]$.

a) Show that $\phi(m)=m$ for all $m \in \mathbf{Z}$. 2p

b) Show that $\phi(x)=x+n$ or $-x+n$ for some $n \in \mathbf{Z}$. 3p

5) Formulate and prove the fundamental homomorphism theorem for groups. 4p

6) Show that any finite integral domain is a field. 4p

You may use the theorems in Durbin's book to solve the first four problems, but it is important that you motivate your claims.

Solutions to the algebra exam 2023-03-17

1a) The rotations by 90° or 270° are the only symmetries of order 4 of a square. Hence G cannot be isomorphic to the square group as they do not have the same number elements of order 4.

1b) If G were abelian, then it would be isomorphic to one of the additive groups $\mathbf{Z}_8$, $\mathbf{Z}_4\times \mathbf{Z}_2$ or $\mathbf{Z}_2\times \mathbf{Z}_2\times \mathbf{Z}_2$ by the fundamental theorem for finite abelian groups. But none of these groups contain more than four elements of order 4. Hence G cannot be abelian.

2) Let g_0, g_1, g_2 resp. g_3 be the rotations by 0°, 90° , 180° or 270° and e_i be the number of orbits under the action of $< g_i>$ on the set of the 64 squares. Then $e_0=64$, $e_2=32$ and $e_1=e_3=16$ as each orbit consists of $o(g_i)$ elements. The number $\Psi(g_i)$ of g_i-invariant 2-colourings of the squares are therefore $\Psi(g_0)=2^{64}$, $\Psi(g_2)= 2^{32}$ and $\Psi(g_1)= \Psi(g_3)=2^{16}$, which by Burnside's lemma gives $(\Psi(g_0)+\Psi(g_1)+ \Psi(g_2)+\Psi(g_3))/4 =2^{62}+2^{30}+2^{15}$ inequivalent paintings.

3) Clearly, $I+J\neq\varnothing$. Let $i+j$ and $i´+j´$ be elements of $I+J$ with i and $i´$ in I and j and $j´$ in J. Then $(i+j) +(i´+j´)= (i+i´)+ (j+j´)$ and $–(i+j) =(–i)+(–j)$ are also elements of $I+J$ as I and J are additive subgrups of R. We have, thererefore, by the subgroup criterion that $I+J$ is an additive subgrup of R. To prove the ideal condition, suppose that $r\in R$ and $i+j\in I+J$ with $i\in I$ and $j\in J$. Then $ri\in I$ and $rj\in J$ as I and J are ideals. Hence $r(i+j)= ri+rj\in \in I+J$, thereby completing the proof that $I+J$ is an ideal.

4) $x^7–x=x(x^6– 1)=x(x^3+1)(x^3–1)$ by the conjugate rule. We have also by the factor theorem that x^3+1 is divisible by $x+1$ as $(–1)^3+1=0$ and that $x^3–1$ is divisible by $x–1$ as $1^3–1=0$. On applying long division or the formula for the sum of a geometric series we get further that $x^3+1=(x+1)(x^2– x+1)$ and $x^3–1=(x–1)(x^2+ x+1)$. Hence $x^7–x=x(x+1)(x^2–x+1)(x–1)(x^2+x+1)$ in $\mathbf{Z}[x]$ and $x^7–x=x(x+1)(x^2+2x+1)(x–1)(x^2–2x+1)= x(x+1)^3(x–1)^3$ in $\mathbf{Z}_3[x]$.

5) See the proof of theorem 9.1 in Reid's book

6) See the proof of theorem 40.3 in Reid's book

Solutions to Eexamination in algebra: MMG 500 and MVE 150, 2023-06-017.

1) Let α and β be two rational numbers and A be the set of all linear combinations $m\alpha+n\beta$ with integer cofficients m and n.
a) Show that A is a subgroup of the additive group $\mathbf{Q}$.
b) Prove that A is cyclic.
Solution : a). Clearly $A\neq\emptyset$. Further, if $k\alpha+l\beta$ and $m\alpha+n\beta\in A$, then $(k\alpha+l\beta)+(m\alpha+n\beta)=(k+m)\alpha+(l+n)\beta$ and $-(m\alpha+n\beta)=(-m)\alpha+(-n)\beta$ are also in A. Hence A is a subgroup of $\mathbf{Q}$ by the subgroup criterion.

b) Let q be a positive integer such that $q\alpha\in\mathbf{Z}$ and $q\beta\in\mathbf{Z}$. Then $\alpha=a/q$ and $\beta=b/q$ for some integers a and b. Let d=GCD(a,b) with d=0 if a=b=0 and $\delta=d/q$. Then $m\alpha+n\beta=(ma/d+nb/d)\delta\in<\delta>$ for all $m,n\in\mathbf{Z}$ as ma/d, $nb/d\in\mathbf{Z}$. Hence $A\subseteq<\delta>$. There exists also by Euclid's algorithm $m,n\in\mathbf{Z}$ with $ma+nb=d$. Therefore, $k\delta=kd/q=k(ma+nb)/q=km\alpha+kn\beta\in A$ for all $k\in\mathbf{Z}$ such that $<\delta>\subseteq A$ and $A=<\delta>$.

2) Let G be a group acting transitively on a set S such that the stabiliser $G_t=\{e\}$ for some $t\in S$. Prove that $G_s=\{e\}$ for all $s\in S$.
Solution : Let $s\in S$ and $g\in G_s$. As G acts transitively on S, there exists $h\in G$ with $\pi_h(t)=s$ such that $\pi_{h^{-1}gh}(t)=\pi_{h^{-1}}(\pi_g(\pi_h(t)))=\pi_{h^{-1}}(\pi_g(s))=\pi_{h^{-1}}(s)=\pi_h^{-1}(s)=t$. Hence, $h^{-1}gh\in G_t$ such that $h^{-1}gh=e$ by hypothesis. But then $g=(hh^{-1})g(hh^{-1})=h(h^{-1}gh)h^{-1}=heh^{-1}=e$, as was to be proved.

3) Let φ: $R\to S$ be a ring homomorphism and J be an ideal of S. Show that the inverse image $I=\varphi^{-1}(J)=\{r\in R : \varphi(r)\in J\}$ is an ideal of R.
Solution : As φ is additive, we have that $\varphi(0)=0$ and $\varphi(a+b)=\varphi(a)+\varphi(b)=0$ and $\varphi(-a)=-\varphi(a)=0$ for $a,b\in I$. Hence I is an additive subgroup of R by the subgroup criterion. Moreover, if $r\in R$ and $i\in I$, then $\varphi(ri)=\varphi(r)\,\varphi(i)=0$ and $\varphi(ir)=\varphi(i)\,\varphi(r)=0$, thereby proving that I is an ideal.

4)) Construct a field extension of $\mathbf{Z}_3$ with 27 elements.
Solution : If K is a field and $p(x)\in K[x]$ is of degree $d\geq 0$, then every coset in $K[x]/(p(x))$ has a unique representative $a_0+a_1x+\ldots+a_{d-1}x^{d-1}$ with $a_0,a_1,\ldots,a_{d-1}$ in K. There are thus 3^d elements in $K[x]/(p(x))$ for $K=\mathbf{Z}_3$ and 27 elements if $p(x)=x(x+1)(x-1)+1\in\mathbf{Z}_3[x]$. We also

note that none of the linear polynomials x, x+1 or x-1 can be a factor of $p(x)$ in $\mathbf{Z}_3[x]$ as we get the remainder 1 in all cases. Hence $p(x)= x^3–x+1$ is irreducible in $\mathbf{Z}_3[x]$ and $K[x]/(p(x))$ a field by a theorem in Durbin´s book, as desired.

5) See Durbun´s book

6) See Durbun´s book

Solutions to exam in algebra MMG 500/MVE 150 2023-08-14

1a) x^2+1 cannot have a zero a in F as $a^2 + 1^2 = 0$ would imply that $a = 1 = 0$. But then x^2+1 must be irreducible in $F[x]$ as any linear factor in $F[x]$ would give rise to zero in F.

b) We have for $c,d \in \mathbf{Z}_3$ that c^2, $d^2 \in \{[0], [1]\}$ such that $c^2 + d^2 = [0]$ only when $c^2 = d^2 = [0]$. Hence (*) holds in $\mathbf{Z}_3$. But $\mathbf{Z}_5$ will not satisfy (*) as $c^2 + d^2 = [0]$ in $\mathbf{Z}_5$ for $(c, d) = ([1], [2])$.

2) Let $g \in G$ and $h = \phi(g)$. Then $g^{|G|} = e_G$ and $h^{|H|} = e_H$ by a corollary of Lagrange's theorem. We have therefore also that $h^{|G|} = \phi(g^{|G|}) = \phi(e_G) = e_H$. But we know from Euclid's algorithm that there exists integers k, l with $k|G| + l|H| = (|G|,|H|) = 1$. Hence $h = h^{k|G|+l|H|} = h^{k|G|}h^{l|H|} = (h^{|G|})^k(h^{|H|})^l = (e_H)^k(e_H)^l = e_H$, as was to be proved.

Alternative solution : Let $K = \ker \phi$ and $H_0 = \text{im } \phi$. Then G/K and H_0 are isomorphic by the fundamental homomorphism theorem. By Lagrange's theorem we have also that $o(G/K) = o(G)/o(K)$ divides $|G|$ and that $o(H_0)$ divides $|H|$. Therefore, $o(G/K) = o(H_0)$ divides $(|G|,|H|) = 1$ such that $K = G$, as asserted.

3) The order of a permutation in S_n is the LCM of the lengths of its cycles. A permutation of order 12 in S_7 must therefore consist of one 3-cycle and one 4-cycle.

There are $7!/3!4! = 35$ partitions of $\{1,2,3,4,5,6,7\}$ into two subsets of three and four elements and $(k\text{-}1)!$ k-cycles for each k-subset of $\{1,2,3,4,5,6,7\}$. There are therefore $35 \times 2! \times 3! = 420$ elements of order twelve in S_7.

4a) Let $g \in \mathbf{Z}[x]$. Then $g = \phi(f)$ for some $f \in \mathbf{Z}[x]$ and $\phi(1)g = \phi(1)\phi(f) = \phi(1 \times f) = \phi(f) = g$. Hence $\phi(1) = 1$ as $\phi(1)g = g$ for all $g \in \mathbf{Z}[x]$. We see also by induction that $\phi(n) = n$ for all $n \in \mathbf{N}$ as $\phi(n) = n \Rightarrow \phi(n+1) = \phi(n) + \phi(1) = n+1$. So $\phi(m-n) = \phi(m) - \phi(n) = m-n$ for all $m, n \in \mathbf{N}$, thereby proving the assertion.

b) We first note that $h = \phi(x)$ is of positive degree by a) and the injectivity of ϕ. Now let $p(x) = a_k x^k + a_{k-1}x^{k-1} + \dots + a_1 x + a_0$ be an arbitrary polynomial in $\mathbf{Z}[x]$ with $a_k \neq 0$. Then $\phi(p(x)) = \phi(a_k)\phi(x^k) + \dots + \phi(a_1)\phi(x) + \phi(a_0) = a_k f^k + \dots + a_1 f + a_0$ is of degree $k\deg f$ as $\deg a_i f^i = i$ for all $i \geq 1$ with $a_i \neq 0$. If $p(x) \in \mathbf{Z}[x]$ is the polynomial with $\phi(p(x)) = x$, we see thus that $k = \deg f = 1$. But then $a_1\phi(x) = \phi(a_1 x) = \phi(a_1 x + a_0) - \phi(a_0) = x - a_0$, which implies that $a_1 = \pm 1$ and $\phi(x) = \pm(x - a_0)$.

5) See Durbin's book pp.114-115.

6) See Durbin's book page 129.