MAS220, Semester 1 Problems.

September 6, 2017

1. We define a binary operation $\odot$ on the set $\mathbb{Z}$ of integers by $a \odot b := a+b+1$, $\forall a, b \in \mathbb{Z}$. Prove that $(\mathbb{Z}, \odot)$ is an abelian group. [Beware: the identity element will not be 0.] Can you find an isomorphism between this and a more familiar group? [Hint: the identity of one group has to map to the identity of the other group. This may help you to find the right bijection before you check it is an isomorphism.]

2. Let $\mathbb{R}^\times := \mathbb{R}\backslash\{0\}$. Why does $a \odot b := ab + a + b$ not define a binary operation on $\mathbb{R}^\times$?

3. Let $\mathbb{R}^\times := \mathbb{R}\backslash\{0\}$. Let $P := \{r \in \mathbb{R} : r > 0\}$ and $N := \{r \in \mathbb{R} : r < 0\}$.

   (a) What word describes the relation between the set $G := \{P, N\}$ and the set $\mathbb{R}^\times$? (G is a ____ of $\mathbb{R}^\times$.)

   (b) Define a group operation ("multiplication") on G in as natural a way as possible, by writing down its Cayley table. [What do P and N stand for?] Which element is the identity? What rule is your table expressing?

   (c) Find a subgroup H of $\mathbb{R}^\times$ (with the usual multiplication operation) such that G is the set of cosets of H in $\mathbb{R}^\times$.

   (d) Find another subgroup K of $\mathbb{R}^\times$ such that K is isomorphic to G. Is K a subset of G?

4. Let W be the set of all words listed in the Oxford English Dictionary.

   (a) Let R be the relation on W defined by $w_1 R w_2 \iff w_1$ and w_2 start with the same letter. Is R an equivalence relation? If so, how many equivalence classes are there?

   (b) Let S be the relation on W defined by $w_1 S w_2 \iff w_1$ and w_2 share at least one letter in common. Is S an equivalence relation? Prove your assertion.

5. Let W be the set of all words listed in the Oxford English Dictionary. Let A be the alphabet (whose elements will be presented in lower case) and let S be the set of all subsets of A.

(a) What is the cardinality (size) of S? Is $\{a, \{b\}\} \in S$?

(b) Let $\ell : W \to S$ be the function that sends a word to the set of all the letters occurring in that word. What is ℓ(function)? Is ℓ injective? Justify your answer. Give two completely different proofs that ℓ is not a surjection.

(c) Now we define a binary operation $\odot : W \times W \to W$ by $w_1 \odot w_2 =$ the longest word w such that $\ell(w) \subseteq \ell(w_1) \cup \ell(w_2)$, taking the first in alphabetical order if there is a tie. What do you think gable$\odot$real is? Is $\odot$ commutative? Associative? Is $(W, \odot)$ a group?

6. Let X and Y be two sets, and $f : X \to Y$ a function.

(a) If $B \subseteq Y$, what is meant by $f^{-1}(B)$, and what do we call it, in words?

(b) Let $\mathcal{P}_f := \{f^{-1}(\{y\}) | y \in Y\}$. In the case $X = \{1, 2, 3, 4, 5\}$ and $Y = \{1, 2, 3\}$, with $f(1) = 1, f(2) = 3, f(3) = 2, f(4) = 3, f(5) = 1$, write down $\mathcal{P}_f$. Is $2 \in \mathcal{P}_f$?

(c) Now let X, Y be any sets, and $f : X \to Y$ any function from X to Y. For any $a, b \in X$, define $aRb \iff f(a) = f(b)$. Prove that R is an equivalence relation. Let $\mathcal{Q}_f$ be the associated partition of X. In the example above, what is $\mathcal{Q}_f$? What do you notice? Is it possible to find a different function $g : X \to Y$ such that $\mathcal{P}_g \neq \mathcal{Q}_g$?

7. In the group S_6, if $g = (123456)$, what are g^2, g^3 and g^{-1}? Find an element h such that $gh \neq hg$.

8. Recall that $\mathbb{C}^\times = \mathbb{C} \backslash \{0\}$ is a group under the operation of multiplication. (You may assume this.) Let $H = \{z \in \mathbb{C}^\times : |z| \leq 1\}$. Is H a subgroup of $\mathbb{C}^\times$?

9. Let G be a group. Show that if $g^2 = e,\ \forall g \in G$, then G is abelian. [Hint: consider a^2, b^2 and $(ab)^2$.]

10. * Let $U := \{z \in \mathbb{C} : |z| = 1\}$.

(a) Prove that U is a subgroup of the multiplicative group $\mathbb{C}^\times$.

(b) There is an isomorphism of groups $f : \mathrm{SO}_2 \to U$. Write down a formula for $f(\mathrm{rot}_\theta)$.

(c) Suppose that H is a subgroup of U. Show that if $\mathrm{rot}_\alpha, \mathrm{rot}_\beta \in H$ and if $n\alpha < \beta < (n+1)\alpha$ with $n \in \mathbb{Z}$, then $\mathrm{rot}_{\beta - n\alpha} \in H$. By choosing $\alpha > 0$ as small as possible (call it α_0), prove that if H is finite then H is cyclic, generated by $g := \mathrm{rot}_{\alpha_0}$. Prove that $H \simeq U_n$ (the group of complex n^{th} roots of unity), for some n. What is α_0, in terms of n?

(d) Give an example of an infinite subgroup of U that is proper (i.e. not the whole of U). Give another example of an infinite proper subgroup of U that is either cyclic or non-cyclic (whichever your first example wasn't).

(e) By considering the order of any element, prove that if H is a finite subgroup of $\mathbb{C}^\times$ then $H \subseteq U$. Give an example of an infinite subgroup of $\mathbb{C}^\times$ that is not contained in U.

(f) Let $\mathbb{Z}/n\mathbb{Z}$ be the additive group of integers mod n. Does $\mathbb{C}^\times$ have any subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$? If so, write it down. Does $\mathbb{C}^\times$ have a subgroup isomorphic to the direct product $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$? Does O_2 have such a subgroup?

11. In A_4, let V_4 be the subset $\{\text{id.}, (12)(34), (13)(24), (14)(23)\}$, and let K be the subset $\{\text{id.}, (123), (132)\}$.

(a) Construct multiplication tables for V_4 and K, and show that they are subgroups of A_4.

(b) How many left cosets of K in A_4 are there? Take any two such cosets, different from each other and from K, and multiply them together in some order. (You are not expected to do this for all pairs of cosets, just for one.) Is the result another coset?

(c) How many left cosets of V_4 in A_4 are there? Take two such cosets, different from each other and from V_4, and multiply them together. Is the result another coset?

(d) Calculate the cosets $(124)K$ and $K(124)$. Write down all the left cosets of V_4 in A_4, listing all the elements in each coset, and not repeating any coset. Do the same for right cosets. In other words, partition A_4 into left cosets of V_4 and also into right cosets of V_4. What do you notice?

12. Let G be a group. For any $a, b \in G$ we define the *commutator* $[a, b] := aba^{-1}b^{-1}$. An element of G is said to be a commutator if it is of the form $[a, b]$ for some $a, b \in G$.

(a) Prove that $[a, b] = e$ if and only if a and b commute with each other.

(b) Prove that if c is a commutator then so is c^{-1}.

(c) Let H be the subset of G comprising all finite products of commutators, i.e. $h \in H$ if and only if there exists a $k \geq 0$ and commutators $c_1, \ldots, c_k$ such that $h = c_1 c_2 \cdot \ldots \cdot c_k$. (By convention, $h = e$ if $k = 0$.) Prove that H is a subgroup of G. [This is called the commutator subgroup, or derived subgroup, denoted $[G, G]$ or G'.]

(d) Recall that SO_2 is the subgroup of rotations in O_2. Using the relations $\mathrm{ref}_\alpha \mathrm{rot}_\beta = \mathrm{ref}_{\alpha-\beta}$ and $\mathrm{ref}_\alpha \mathrm{ref}_\beta = \mathrm{rot}_{\alpha-\beta}$, prove that every element of SO_2 is a commutator in O_2.

13. (a) Let G be a group, and suppose that some $g \in G$ is a commutator, i.e. $g = [a, b] := aba^{-1}b^{-1}$ for some $a, b \in G$. Prove that for any $h \in G$, hgh^{-1} is also a commutator.

(b) In S_4, confirm that $(12)(34) = [(13)(24)](34)[(13)(24)]^{-1}(34)^{-1}$ and that $(123) = (23)(123)(23)^{-1}(123)^{-1}$

(c) List the elements of A_4. Prove that they are all commutators in S_4. Which (if any) of them are commutators in A_4, i.e. of the form $[a, b]$ for $a, b \in A_4$ (not just in S_4)?

(d) Prove that for any $n \geq 3$, A_n is contained in the commutator subgroup (see # 12) of S_n. What about $n = 1$ and $n = 2$?

14. (a) Let G be a finite group. Prove that any element $g \in G$ has finite order.

(b) Prove that if G is a finite group, and if $g_1, g_2 \in G$ are conjugate to each other, then g_1 and g_2 have the same order.

(c) Prove that in S_3, any two elements of the same order are conjugate. Is the same true in S_4?

15. Let G be a group, and let $\theta : G \to G$ be the map such that $\theta(g) = g^{-1}$ for all $g \in G$. Is θ an isomorphism from G to itself?

16. Let G be a group, and $h \in G$ any fixed element. Let $\theta_h : G \to G$ be the map such that $\theta_h(g) = hgh^{-1}$ for all $g \in G$.

(a) Show that θ_h is a group isomorphism from G to itself (i.e. an *automorphism* of G). [Hint: To prove it is a bijection, you might like to produce the inverse function.]

(b) If $G = O_2$ and $h = \mathrm{rot}_\phi$, what are $\theta_h(\mathrm{rot}_\alpha)$ and $\theta_h(\mathrm{ref}_\beta)$?

(c) If $G = O_2$ and $h = \mathrm{ref}_\phi$, what are $\theta_h(\mathrm{rot}_\alpha)$ and $\theta_h(\mathrm{ref}_\beta)$?

(d) If $G = Q = \{\pm 1, \pm i, \pm j, \pm k\}$, the quaternion group, work out $\theta_{-1}(g)$ for each $g \in Q$, and work out $\theta_i(g)$ for each $g \in G$. How many different automorphisms of Q do we get by considering θ_h for all possible $h \in Q$?

(e) Find another automorphism of Q that is not of the form θ_h for any $h \in Q$.

17. (a) Let G be a group, and $H \leq G$ a subgroup. Prove that if $g \in G$ is fixed, then $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup of G.

(b) Suppose that G acts on a set X. Recall that for any $x \in X$, the stabiliser of x, $\mathrm{stab}(x) := \{g \in G : g * x = x\}$. Using **GA1** and **GA2**, prove that for any $x \in X$, $\mathrm{stab}(x)$ is a subgroup of G.

(c) Prove that if $x \in X$ and $h \in G$ then $\mathrm{stab}(h * x) = h\,\mathrm{stab}(x)h^{-1}$. [Hint: it suffices to show that $h\,\mathrm{stab}(x)h^{-1} \subseteq \mathrm{stab}(h * x)$ and that $h^{-1}\,\mathrm{stab}(h * x)h \subseteq \mathrm{stab}(x)$. (Why?) Alternatively, show that $g \in \mathrm{stab}(h * x) \iff h^{-1}gh \in \mathrm{stab}(x)$.]

(d) Consider the natural action of O_2 on $\mathbb{R}^2$ (just applying rotations and reflections to vectors in the plane). Letting $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, what is $\mathrm{stab}(x)$ (it should have only two elements)? Using 16(b), find

$h\,\mathrm{stab}(x)h^{-1}$ when $h = \mathrm{rot}_\phi$. According to (c), this should be the same as $\mathrm{stab}(h * x)$. Can you see this directly by looking at $h * x$? Repeat with $h = \mathrm{ref}_\phi$, using 16(c).

18. (a) List all the elements σ of the alternating group A_4, in the first column of a table. In the next column, put $\sigma(1\ 2\ 3)\sigma^{-1}$, and in the next put $\sigma(1\ 3\ 2)\sigma^{-1}$.

    (b) Exhibit the conjugacy classes of A_4. Hence find all the normal subgroups of A_4.

19. (a) Let G be a group, and X a set on which G acts. Prove that $\theta : g\,\mathrm{stab}(x) \mapsto g * x$ gives a bijection between the set $G/\mathrm{stab}(x)$ of left cosets of $\mathrm{stab}(x)$ in G, and the orbit $\mathrm{orb}(x) = \{g*x : g \in G\}$. Deduce that if G is finite then $|\mathrm{orb}(x)| = \frac{|G|}{|\mathrm{stab}(x)|}$.

    (b) Let G be a finite group, and $x \in G$. Define the conjugacy class $\mathrm{conj}_G(x)$ and the centraliser $\mathrm{cent}_G(x)$. What is the relationship between $|G|$, $|\mathrm{cent}_G(x)|$ and $|\mathrm{conj}_G(x)|$, and why?

    (c) Let $G = S_5$. Determine $|G|$, $|\mathrm{conj}_G((123))|$, and therefore $|\mathrm{cent}_G((123))|$. By finding enough elements, in $\mathrm{cent}_G((123))$, list them all.

20. Let $G = O_2$.

    (a) Find $\mathrm{cent}_G(\mathrm{id.})$ and $\mathrm{conj}_G(\mathrm{id.})$.

    (b) Find $\mathrm{cent}_G(\mathrm{rot}_\alpha)$ and $\mathrm{conj}_G(\mathrm{rot}_\alpha)$, when $\mathrm{rot}_\alpha) \neq \mathrm{id.}$.

    (c) Find $\mathrm{cent}_G(\mathrm{ref}_\beta)$ and $\mathrm{conj}_G(\mathrm{ref}_\beta)$.

    (d) What is the centre $Z(G)$? Is $G/Z(G) \simeq \mathrm{SO}_2$?

21. (a) Let G be a group. Define the centre $Z(G)$ of G, and prove that it is a subgroup of G (using SG1,SG2,SG3 as an alternative to the proof in the lecture).

    (b) Prove that $Z(G)$ is in fact a normal subgroup of G, and that $g \in Z(G)$ if and only if $\mathrm{conj}_G(g) = \{g\}$.

    (c) Show that $Z(S_n) = \{\mathrm{id.}\}$ except for one value of n. What is it?

    (d) Suppose that $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathrm{GL}_2(\mathbb{R}))$. Using the fact that g commutes with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, show that $b = c$ and $a = d$. Show further that g is of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, with $a \neq 0$. Write down an isomorphism $\theta : \mathbb{R}^\times \to Z(\mathrm{GL}_2(\mathbb{R}))$.

22. Suppose that G is a group of order 39 with centre $Z(G) = \{e\}$.

    (a) What are the possible sizes of conjugacy classes in G? How many of each size must there be?

(b) Let $h \in G$ be an element of order 13, and let $H = \langle h \rangle$ be the cyclic subgroup generated by h. Show that $H \leq \mathrm{cent}_G(h)$. What must be the size of $\mathrm{conj}_G(h)$?

(c) Prove that H must be a normal subgroup of G, and that there aren't any others apart from $\{e\}$ and G.

(d) Do you think that such a group G actually exists?

23. (a) Prove that if G is a finite group, with a subgroup H, then the left cosets of H in G partition G. Deduce that $|H|$ divides $|G|$.

(b) Prove that if G is a cyclic group of order n, and if $d \mid n$, then G has a subgroup of order d.

(c) Prove that if G is a finite group, with a subgroup H such that $|G|/|H| = 2$, then $H \lhd G$. [Hint: consider H and $G \backslash H$ as cosets.]

(d) Give an example of a group of order 12 with no subgroup of order 6.

24. Recall from # 12 the derived (commutator) subgroup G' of a group G.

(a) Prove that G' is a normal subgroup of G, and that G/G' is abelian.

(b) Prove also that if N is a normal subgroup of G and G/N is abelian, then $G' \subseteq N$. [Thus G/G' is the maximal abelian quotient of G. It is called the abelianisation of G.]

(c) Prove that if $G = O_2$ then $G' = \mathrm{SO}_2$. What is the abelianisation of G?

(d) Prove that if $G = S_n$ with $n \geq 2$ then $G' = A_n$. What is the abelianisation of G? (Recall Q 13.)

25. Let $\theta : G \to H$ be a homomorphism of groups.

(a) Describe $\ker(\theta)$ as $\theta^{-1}(S)$, for an appropriately chosen subset S of H.

(b) Show that if $\theta(a) = b$ then $\theta^{-1}(\{b\}) = a \ker(\theta)$.

26. Let G be a group, and $n \geq 1$ a natural number. We define $\theta_n : G \to G$ by $\theta_n(g) = g^n, \ \forall g \in G$.

(a) Prove that if G is abelian then θ_n is a group homomorphism.

(b) If $G = \mathbb{C}^\times$, what are $\ker(\theta_4)$ and $\mathrm{im}(\theta_4)$. What does the First Isomorphism Theorem tell you? What is $\theta_4^{-1}(\{4\})$?

(c) Prove that if θ_2 is a homomorphism then G is abelian.

(d) Give an example of a non-abelian group G for which θ_6 is still a homomorphism.

(e) By counting the elements in the kernel, show that θ_5 could not possibly be a homomorphism of S_5.

27. Let

$$p_1 = (x_1 + x_2)(x_3 + x_4)$$
$$p_2 = (x_1 + x_3)(x_2 + x_4)$$
$$p_3 = (x_1 + x_4)(x_2 + x_3).$$

The symmetric group S_4 acts on these polynomials by permuting the variables, that is, for $\alpha \in S_4$

$$\alpha * (x_i + x_j)(x_k + x_l) = (x_{\alpha(i)} + x_{\alpha(j)})(x_{\alpha(k)} + x_{\alpha(l)}).$$

Let's get some feeling for what this means.

(a) The element (2 3) acts on each polynomial by switching 2 and 3, so in effect x_2 becomes x_3 and x_3 becomes x_2. Write down the result of doing this to the polynomial

$$(x_1 + x_2)(x_3 + x_4).$$

(b) What you have just done is apply the element (2 3) to the polynomial p_1. Which of p_1, p_2, p_3 was the result?

(c) Now apply (2 3) to p_2 and to p_3 and see which polynomial results in each case.

(d) This means that the element (2 3) has *permuted* the polynomials $\{p_1, p_2, p_3\}$. So we have produced a permutation in S_3. Which one?

(e) Now try it for the element (1 2)(3 4). What happens if you apply this to each of p_1, p_2, p_3?

(f) So, what permutation of S_3 have you produced from (1 2)(3 4)?

(g) Find all the permutations in S_4 that leave p_1 fixed. *This is the* ***stabiliser*** of p_1.

(h) Find also the stabilisers of p_2 and of p_3, and all the permutations that fix all of p_1, p_2, p_3 simultaneously.

(i) The above method gives a homomorphism $f : S_4 \to S_3$. What is its kernel?

(j) What does the First Isomorphism Theorem tell us about this situation?

28. Prove that in any ring R, $0.x = 0$, and $(-1).x = -x$, for all $x \in R$, and also that $(-x).y = -(xy)$, $\forall x, y \in R$.

29. A *Boolean ring* (named after George Boole, born in Lincoln, 1815) is a ring R such that $x^2 = x$ for all $x \in R$. In the following, show your reasoning carefully, referring to axioms or to things you have already proved.

(a) By squaring $x + y$, prove that $yx = -xy$ for all $x, y \in R$.

(b) By choosing y carefully in (a), deduce that $x = -x,\ \forall x \in R$. Now substituting xy for x, deduce that R is a commutative ring.

(c) We define a unary operation $' : R \to R$ by $x' := 1 + x$ ($\forall x \in R$), and binary operations $\wedge, \vee : R \times R \to R$ by $x \wedge y := xy$ (so not really a new operation) and $x \vee y := x + y + xy$. Prove that

i. $(x')' = x\ \forall x \in R$ [Hint: consider (b) with $x = 1$];

ii. $(x \vee y) \vee z = x \vee (y \vee z)\ \forall x, y, z \in R$;

iii. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\ \forall x, y, z \in R$;

iv. $(x \wedge y)' = (x') \vee (y')\ \forall x, y, z \in R$.

Does this remind you of anything?

(d) Prove that $x + y = (x \vee y) \wedge (x \wedge y)'$, for all $x, y \in R$.

30. (a) Prove that if R is a commutative ring and $a, b \in R$ then $a^2 - b^2 = (a - b)(a + b)$, saying which axioms, earlier results or conditions you are using at each step.

(b) In the matrix ring $M_2(\mathbb{R})$, find two elements A, B such that $A^2 - B^2 \neq (A - B)(A + B)$, calculating both sides to check.

(c) In Hamilton's quaternion ring $\mathbb{H}$, find two elements a, b such that $a^2 - b^2 \neq (a - b)(a + b)$, calculating both sides to check.

(d) In the Weyl algebra, how do we know that $P^2 - Q^2 \neq (P - Q)(P + Q)$ (where $PQ - QP = 1$)?

31. In the Weyl algebra, is there an easy way to see that P is not a unit?

32. Let R be a Boolean ring (see earlier exercise). If $0, 1$ and $a \in R$ are all distinct, show that $S := \{0, 1, a, 1 + a\}$ is a 4-element subring of R, writing down the addition and multiplication tables and justifying each entry.

33. (Messy) Using quaternions, rotate the vector $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ through an angle $\pi/3$ about the axis $\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}$.

34. Let $R = \{a + b\epsilon : a, b \in \mathbb{R}\}$, a commutative ring with the multiplication rule $\epsilon^2 = 0$. Note that the subset of elements such that $b = 0$ forms a subring isomorphic to $\mathbb{R}$, which I shall henceforth refer to as "$\mathbb{R}$".

(a) Calculate $(1 + \epsilon)(3 - 2\epsilon)$.

(b) Show that $(a + b\epsilon)(a - b\epsilon) \in \mathbb{R}$. Hence show that if $a \neq 0$ then $a + b\epsilon$ is invertible, and calculate $(3 - 2\epsilon)^{-1}$.

(c) Show that for any $b \in \mathbb{R}$, $b\epsilon$ is not a unit in R. Hence describe exactly the group U of units in R.

(d) Calculate $(2+\epsilon)^8$. Find all the elements of finite order in U.

(e) Let $F = a + b\epsilon$ and $G = c + d\epsilon$. Calculate FG, G^{-1} and FG^{-1}. Do the answers remind you of anything? If not, relabel $a = u, b = u'$, $c = v, d = v'$, and try again.

35. * Let $\mathbb{H}$ be Hamilton's quaternion ring, and let L be the subset $\{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$.

(a) Prove that L is a subring of $\mathbb{H}$.

(b) For $\alpha \in \mathbb{H}$, let $N(\alpha) = \alpha\overline{\alpha}$, where for $\alpha = a + bi + cj + dk$ (with $a, b, c, d \in \mathbb{R}$) we put $\overline{\alpha} := a - bi - cj - dk$. What is $N(\alpha)$, in terms of a, b, c, d? Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$, for all $\alpha, \beta \in \mathbb{H}$.

(c) Prove that if $\alpha\beta = 1$, with $\alpha, \beta \in L$, then $N(\alpha) = 1$. Hence show that the group Q of units in L has order 8. What is j^{-1}?

(d) Let H be the subset $\{\frac{1}{2}(a + bi + cj + dk) : a, b, c, d \in \mathbb{Z},$ all odd or all even$\}$. Show that H is a subring of $\mathbb{H}$.

(e) Let $U(H)$ be the unit group of H. Show that Q is a subgroup of $U(H)$, and that $U(H)$ is a subgroup of $\mathrm{SU}(2) := \{\alpha \in \mathbb{H} : N(\alpha) = 1\}$.

(f) Show that $\alpha := \frac{1}{2}(1 - i - j - k)$ belongs to $U(H)$, and that $U(H)$ has order 24. (If you can't do that yet, just keep going.)

(g) Calculate α^2 and α^3. What is α^{-1}?

(h) By calculating, and comparing, the cosets αQ and $Q\alpha$, prove that Q is a normal subgroup of $U(H)$. What is the quotient group $U(H)/Q$ isomorphic to?

(i) Let $\phi : \mathrm{SU}(2) \to \mathrm{SO}_3$ be the group homomorphism taking a quaternion of norm 1 to its associated rotation, where SO_3 is the group of all rotations about the origin in $\mathbb{R}^3$. Restricting ϕ to the subgroup $U(H)$ of $\mathrm{SU}(2)$, we may view it as a group homomorphism $\phi : U(H) \to \mathrm{SO}_3$. By writing each in the form $\cos(\theta/2) + \sin(\theta/2)(u_x i + u_y j + u_z k)$, for some unit vector $u_x\mathbf{i} + u_y\mathbf{j} + u_z\mathbf{k}$, find the angle and axis of rotation for each of i, j, k, α. What about $-i$?

(j) What is the kernel of $\phi : U(H) \to \mathrm{SO}_3$, and how big is the image subgroup $\phi(U(H))$ of SO_3? Can you see how it might be the group of rotations of a regular tetrahedron (with the origin at the centre of mass)? What other group do you guess it might be isomorphic to?

36. Let R be a commutative ring, and $R[x]$ the polynomial ring.

(a) If $a(x) = a_0 + a_1x + \cdots + a_nx^n$ and $b(x) = b_0 + b_1x + \cdots + b_mx^m$ are arbitrary elements of $R[x]$, and if c_r, d_r are the coefficients of x^r in $a(x) + b(x)$ and $a(x)b(x)$, respectively, write down formulas for c_r and d_r in terms of the a_i and b_i.

(b) Prove that if R is a subring of S (both commutative rings) then $R[x]$ is a subring of $S[x]$.

(c) If $\phi : R \to S$ is a homomorphism of commutative rings, and if we define $\tilde{\phi} : R[x] \to S[x]$ by $\tilde{\phi}(a(x)) := \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$, prove that $\tilde{\phi}$ is a ring homomorphism.

37. Let R be a non-commutative ring, and $R[x]$ the set $\{a_0 + a_1x + \cdots + a_nx^n : n \in \mathbb{N}_0, \text{ all } a_i \in R\}$. If we define binary operations of "addition" and "multiplication" on $R[x]$ using the same formulas as when R is commutative, it is easy to show that $R[x]$ is still a ring. (We are simply starting with R and throwing in a new element x that commutes with every element of R. Think about the process of multiplying out two polynomials–the coefficients in the second one have to move from the right to the left of the powers of x in the first one.) If b is some fixed element of R, we define the evaluation map $\mathrm{ev}_b : R[x] \to R$ by $\mathrm{ev}_b(a(x)) = a_0 + a_1b + \cdots + a_nb^n$, for all $a(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. In other words $\mathrm{ev}_b(a(x)) = a(b)$. If $R = \mathbb{H}$, Hamilton's quaternion ring, give examples of choices of b for which ev_b is:

(a) a ring homomorphism;

(b) not a ring homomorphism.

38. Let R be a ring, and $M_2(R)$ the 2-by-2 matrix ring over R. If we define $f : M_2(R) \to M_2(R)$ by $f(A) := A^t$ (the transpose), prove that f is a bijection. Is it a ring isomorphism?

39. Let $R = \{a + b\epsilon : a, b \in \mathbb{R}\}$, with the multiplication rule $\epsilon^2 = 0$, as in Q34. Is R an integral domain? Describe R as the quotient of the polynomial ring $\mathbb{R}[x]$ by some ideal. Equivalently (linked by the First Isomorphism Theorem), give a natural homomorphism $\theta : \mathbb{R}[x] \to R$ (where might x land?), and identify its kernel.

40. Let $R = M_2(\mathbb{R})$, the 2-by-2 matrix ring over $\mathbb{R}$.

(a) Give an example to prove that R is not commutative.

(b) Let J be any (two-sided) ideal in R. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J$, calculate the products

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

By calculating two more similar products, prove that if $J \neq \{0\}$ then there exists some element in J with precisely one non-zero entry. Why may we take this entry to be 1?

(c) Using multiplication on the left and right by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, show that if $J \neq \{0\}$ then

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

all belong to J, hence that $J = R$. In conclusion, the only ideals of R are $\{0\}$ and R.

41. (a) Show that $(x+1)(x+2)(x+3) = x^3 - x$ in $(\mathbb{Z}/6\mathbb{Z})[x]$ (where $\overline{a}$ is denoted a for convenience).
    (b) What are the roots of $(x+1)(x+2)(x+3)$ in $\mathbb{R}$?
    (c) What are the roots of $x^3 - x$ in $\mathbb{R}$?
    (d) What are the roots of $(x+1)(x+2)(x+3)$ in $\mathbb{Z}/6\mathbb{Z}$?

42. Show that $(1+3x)$ is a unit in $(\mathbb{Z}/9\mathbb{Z})[x]$. [Hint: seek a multiplicative inverse of the form $a + bx$.]

43. (deleted)

44. Let R be an integral domain. Prove that the polynomial ring $R[x]$ is also an integral domain.

45. (a) Let R be a finite integral domain. Given a fixed non-zero element $a \in R$, and elements $b_1, b_2 \in R$, prove that if $b_1 \neq b_2$ then $ab_1 \neq ab_2$. [Hint: consider the difference.] Hence prove that R must be a field.
    (b) Give an example of a finite field, and also an example of a finite commutative ring that is not an integral domain.
    (c) Give an example of an infinite integral domain that is not a field, and another one that is a field.

46. List all the associates of 5 in $\mathbb{Z}$, and of $5+4i$ in $\mathbb{Z}[i]$. For each associate a of $5+4i$ in $\mathbb{Z}[i]$, find $b \in \mathbb{Z}[i]$ such that $ab = 1+9i$. What do you notice about the bs?

47. (a) Find non-zero elements $a, b \in \mathbb{Z}/4\mathbb{Z}$ such that $ab = 0$, hence showing that $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.
    (b) Find non-zero elements $\alpha, \beta \in \mathbb{Z}[i]/2\mathbb{Z}[i]$ such that $\alpha\beta = 0$, hence showing that $\mathbb{Z}[i]/2\mathbb{Z}[i]$ is not an integral domain. (Again, you might try $\beta = \alpha$.)
    (c) Show that $\mathbb{Z}[i]/2\mathbb{Z}[i] = \{[0], [1], [i], [1+i]\}$, so also has 4 elements. Is it isomorphic to $\mathbb{Z}/4\mathbb{Z}$? [Hint: consider these two rings just as additive groups, forgetting about multiplication.] Is it isomorphic, as a ring, to the 4-element Boolean ring $S = \{0, 1, a, 1+a\}$ appearing in Q32?

48. Let F be any field, and for $f(x), g(x) \in F[x]$, with $g(x) \neq 0$, consider $f(x) = q(x)g(x) + r(x)$, with $r = 0$ or $\deg(r) < \deg(g)$.

(a) Prove that if $g(x) = x - a$, with $a \in F$, then $r(x) = f(a)$. Deduce that if $f(a) = 0$ then $(x - a) \mid f(x)$. What do you call this theorem?

(b) If $f(x) \in \mathbb{R}[x]$, let $r_1(x)$ be the remainder when $f(x)$ is divided by $(x^2 + 1)$ in $\mathbb{R}[x]$, and let $r_2(x)$ be the remainder when $f(x)$ is divided by $(x - i)$ in $\mathbb{C}[x]$. What is the relationship between $r_1(x)$ and $r_2(x)$? Illustrate your answer with the example $f(x) = x^3 + 1$.

49. Find the group of units of $\mathbb{Z}/9\mathbb{Z}$, and show that it is cyclic.

50. Why is $\mathbb{Z}/59\mathbb{Z}$ a field? Given this, we call it $\mathbb{F}_{59}$. Find the inverse of the element $[16]$ (or, in different notation, the inverse of $\overline{16}$) in the group $\mathbb{F}_{59}^{\times}$.

51. Prove that $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field. Find the multiplicative inverse of the element $[1 + x]$ in this field.

52. (a) Give examples of non-zero $a(x), b(x) \in \mathbb{Z}[x]$ such that there exist $q(x), r(x) \in \mathbb{Z}[x]$, with $r(x) = 0$ or $\deg(r) < \deg(b)$, such that $a(x) = q(x)b(x) + r(x)$.

(b) Give examples of non-zero $a(x), b(x) \in \mathbb{Z}[x]$ such that there do not exist $q(x), r(x) \in \mathbb{Z}[x]$, with $r(x) = 0$ or $\deg(r) < \deg(b)$, such that $a(x) = q(x)b(x) + r(x)$.

53. Consider the map $\theta : \mathbb{C}[x] \to \mathbb{C}[x]$ defined by $\theta(a(x)) := \overline{a_0} + \overline{a_1}x + \cdots \overline{a_n}x^n$, for every $a(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$, where, for any $\alpha \in \mathbb{C}$, $\overline{\alpha}$ is its complex conjugate.

(a) Prove that θ is a ring isomorphism.

(b) Let $S := \{f \in \mathbb{C}[x] : \theta(f) = f\}$. Prove that S is a subring of $\mathbb{C}[x]$. Which subring is it?

(c) From now on, given $f \in \mathbb{C}[x]$, it is convenient to let $\overline{f}$ denote $\theta(f)$. Suppose $f \in \mathbb{C}[x]$ and $g \in \mathbb{R}[x]$. Prove that if $f \mid g$ in $\mathbb{C}[x]$ then also $\overline{f} \mid g$ in $\mathbb{C}[x]$. Illustrate your answer with the example $g(x) = x^3 + 1$.

(d) Show that if $g(x) \in \mathbb{R}[x]$, and if $(x - i) \mid g(x)$ in $\mathbb{C}[x]$, then $(x^2 + 1) \mid g(x)$ in $\mathbb{R}[x]$. Be careful to justify your answer.

(e) According to the "Fundamental Theorem of Algebra", if $f(x) \in \mathbb{C}[x]$, with f non-constant, then there exists some $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Assuming this, prove that if $f(x) \in \mathbb{R}[x]$ is irreducible *in* $\mathbb{R}[x]$ then $\deg(f) = 1$ or 2. [Hint: consider $(x - \alpha)$ and $x^2 - (\alpha + \overline{\alpha})x + (\alpha\overline{\alpha})$.]

54. (a) What are the units in the ring $R := \mathbb{Z}[i]/2\mathbb{Z}[i]$ (recall Q47)? Now, for a proper challenge, what are the units in $R[x]$?

(b) Show that $R[x]$ is not a unique factorisation domain, by exhibiting essentially different factorisations of x^2+1 into products of irreducibles.

55. Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$, the field with two elements.

(a) Show that $\mathbb{F}_2$ is a Boolean ring.

(b) Given any set S, let $R = 2^S$ be the set of functions $f : S \to \mathbb{F}_2$. We may define binary operations $+, \cdot : R \times R \to R$ by $(f+g)(x) := f(x) + g(x)$ and $(f \cdot g)(x) := f(x) \cdot g(x)$, for all $f, g \in R$ and $x \in S$. You may assume that with these operations, R becomes a ring. What are the additive and multiplicative identity elements? Why is it a Boolean ring?

(c) Given any subset $A \subseteq S$, we define its *indicator function* $\chi_A \in R$ by

$$\chi_A(x) := \begin{cases} \overline{1} & \text{if } x \in A; \\ \overline{0} & \text{if } x \notin A. \end{cases}$$

Have you seen $\chi_\emptyset$ and χ_S before? What are they?

(d) Now let $S = \{1, 2, 3, 4, 5, 6\}$. What is the cardinality of R in this case?

(e) Letting $A = \{1, 2, 3\}$ and $B = \{2, 3, 4, 5\}$, write down the tables of all values of the functions χ_A and χ_B, i.e. tables with all the $x \in S$ in one column and the corresponding $f(x)$ in the other column, where f is the function in question. Using these tables, write down also tables of values for the functions $\chi_A + \chi_B$, $\chi_A \cdot \chi_B$ and $\chi_A + \chi_B + \chi_A \cdot \chi_B$.

(f) Recall that $f \wedge g := f \cdot g$ and $f \vee g := f + g + f \cdot g$. In the example above, if $\chi_A \wedge \chi_B = \chi_C$ and $\chi_A \vee \chi_B = \chi_D$, how can you describe the subsets C and D of S, in terms of A and B. What has this got to do with what you found in Q 29?

(g) For any $f : S \to \mathbb{F}_2$, in terms of f, how do you describe the subset $E \subseteq S$ such that $f = \chi_E$?

56. Let $F := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, and $R := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Prove that if $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, and $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$, then $a_1 = a_2$ and $b_1 = b_2$. [Hint: what special property of $\sqrt{2}$ did you see in MAS114?]

(b) Prove that F is a subring of $\mathbb{R}$, and that R is a subring of F.

(c) Prove that the map $\theta : F \to F$ given by $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$ is a ring isomorphism, as is its restriction $\theta : R \to R$.

(d) Prove that F is a field, but that R is not a field. Why must R be an integral domain?

(e) If $\alpha = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$, what is $\alpha\,\theta(\alpha)$ in terms of a and b? Find $u \in R$ such that $u\,\theta(u) = 1$. Why is u a unit? What is u, to 3 decimal places.

(f) Prove that for each $n \in \mathbb{Z}$, u^n is a unit. Why are these elements all different? Calculate u^3, in the form $A + B\sqrt{2}$. Is there any unit in R that is not of the form u^n for $n \in \mathbb{Z}$?

(g) Letting $\delta(\alpha) = |\alpha\,\theta(\alpha)|$, show that R is a Euclidean domain.

(h) Why are the elements $2+\sqrt{2}$ and $3+\sqrt{2}$ irreducible in R?

(i) Check that $(2+\sqrt{2})(3+\sqrt{2}) = (4+3\sqrt{2})(-1+2\sqrt{2})$. Why does this not contradict the fact that R is a unique factorisation domain?

(j) Find a ring homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{R}$ whose image is the subring F. [Hint: where do you think x might land?] Find a polynomial $h(x)$ of degree 2, in the kernel of ϕ. By considering remainders upon division by $h(x)$, prove that $\ker(\phi)$ is precisely $\langle h(x) \rangle$, the set of all multiples of $h(x)$. What does the First Isomorphism Theorem tell us now?

(k) Why is $\mathbb{Q}[x]/\langle x^2 - 3 \rangle$ a field? Write down a field isomorphic to this one.