

# MA10209 Algebra 1A

Sheet 7 Problems and Solutions v3: GCS

25-xi-11

The course website is <http://people.bath.ac.uk/masgcs/diary.html>

*Hand in work to your tutor by 13:00, Monday Nov 21.*

1. A polynomial  $\sum_{i=0}^n a_i X^i$  is *monic* if  $a_n = 1$ . We will work in  $\mathbb{R}[X]$ , the ring of polynomials in  $X$  with coefficients in  $\mathbb{R}$ . In each case, is the given statement true or false?

(a) The zero polynomial is monic.

**Solution** This is false, because the zero polynomial does not have a leading term.

(b) The sum of two monic polynomials is monic.

**Solution** This is false, because  $X + X = 2X$ .

(c) The difference of two monic polynomials is monic.

**Solution** This is false, because  $(X^2 + 2X) - X^2 = 2X$ .

(d) The product of two monic polynomials is monic.

**Solution** This is correct, because if  $f, g \in \mathbb{R}[X]$  and  $f \neq 0 \neq g$ , then the leading term of  $fg$  is the product of the leading terms of  $f$  and  $g$ .

(e) Every polynomial is a product of a non-zero real number and a monic polynomial.

**Solution** This is incorrect, because the zero polynomial cannot be so expressed.

2. Work in  $\mathbb{Q}[X]$ . Divide  $X^5 + 4X + 1$  by  $X^2 + 1$  to leave a remainder of smallest possible degree. Expressed more formally, find polynomials  $q, r \in \mathbb{Q}[X]$  with  $\deg r < 2$  such that  $X^5 + 4X + 1 = q \cdot (X^2 + 1) + r$ .

**Solution** I will show how to do this by ‘long-division’ on a board, but I am not prepared to typeset that! Here is a version which is easier to insert in this document: Notice that  $X^5 + 4X + 1 - X^3(X^2 + 1) = -X^3 + 4X + 1$ . Also  $-X^3 + 4X + 1 = -X(X^2 + 1) + 5X + 1$ . Therefore

$$X^5 + 4X + 1 = X^3(X^2 + 1) - X(X^2 + 1) + 5X + 1$$

so

$$X^5 + 4X + 1 = (X^3 - X)(X^2 + 1) + 5X + 1$$

as required.

3. Let  $R$  be a ring. A polynomial  $f \in R[X]$  of positive degree is called *irreducible* if whenever  $g, h \in R[X]$  are such that  $f = gh$ , then either  $g$  or  $h$  has degree 0 (i.e. is a non-zero constant). Let  $f_1 = X^2 - 2$  and  $f_2 = X^2 + 2$ .

(a) Is either  $f_1$  or  $f_2$  irreducible, viewed as an element of  $\mathbb{Q}[X]$ ?

**Solution** If either were reducible, it would have two linear factors (i.e. two factors of degree 1). No linear polynomial with rational coefficients has  $\sqrt{2}$  as a root, since  $\sqrt{2}$  is irrational. Thus  $X^2 - 2$  has no non-trivial factorization in  $\mathbb{Q}[X]$ . Also  $X^2 + 2$  has no real roots, so it can have no linear factor with coefficients in  $\mathbb{Q}$ .

(b) Is either  $f_1$  or  $f_2$  irreducible, viewed as an element of  $\mathbb{R}[X]$ ?

**Solution**  $f_1 = (X - \sqrt{2})(X + \sqrt{2})$  is reducible in  $\mathbb{R}[X]$ . However  $X^2 + 2$  has no real root, and so cannot have a linear factor with coefficients in  $\mathbb{R}$ .

(c) Is either  $f_1$  or  $f_2$  irreducible, viewed as an element of  $\mathbb{C}[X]$ ?

**Solution** Neither is irreducible, for  $f_1 = (X - \sqrt{2})(X + \sqrt{2})$  and  $f_2 = (X - i\sqrt{2})(X + i\sqrt{2})$ .

4. Suppose that  $\zeta \in \mathbb{C}$ . By considering  $\zeta + \bar{\zeta}$  and  $\zeta\bar{\zeta}$ , prove that there is  $f \in \mathbb{R}[X]$  of degree 2 such that  $f(\zeta) = 0$  (i.e.  $\zeta$  is a root of  $f$ ).

**Solution**  $\zeta + \bar{\zeta} = \zeta + \bar{\zeta} = s \in \mathbb{R}$  and  $\zeta\bar{\zeta} = \zeta\bar{\zeta} = p \in \mathbb{R}$ . Therefore  $\zeta$  is a root of  $X^2 - sX + p$  which can be written  $(X - \zeta)(X - \bar{\zeta})$ .

5. The *Fundamental Theorem of Algebra* states that if  $f \in \mathbb{C}[X]$  and  $\deg f > 0$ , then there is  $\alpha \in \mathbb{C}$  such that  $f(\alpha) = 0$ . A proof of this result is beyond the scope of this course, but assume it for the purposes of this question. The remainder theorem (to be proved in lectures on Monday Nov 14) may be helpful in parts of the following problems.

(a) Prove that every irreducible polynomial in  $\mathbb{C}[X]$  has degree 1.

**Solution** Suppose that  $f \in \mathbb{C}[X]$  has degree at least 1. By the Fundamental Theorem of Algebra  $f$  has a root  $\alpha \in \mathbb{C}$ . Now divide  $f$  by  $X - \alpha$  as best you can. There are polynomials  $q, r$  with the degree of  $r$  at most 0 so that  $f = q(X - \alpha) + r$  with  $r$  a constant. Evaluating at  $\alpha$  we see that  $f(\alpha) = 0 = 0 + r$  so  $r = 0$ . If  $f$  is irreducible, this forces  $q$  to be a non-zero constant and so  $\deg f = 1$ .

(b) Prove that every irreducible polynomial in  $\mathbb{R}[X]$  has degree at most 2.

**Solution** Suppose that  $f \in \mathbb{R}[X]$  is irreducible in  $\mathbb{R}[X]$ . By the Fundamental Theorem of Algebra  $f$  has a root  $\alpha \in \mathbb{C}$ . If  $\alpha \in \mathbb{R}$ , we divide  $f$  by  $X - \alpha$  with remainder a constant  $r$  as in the previous part. Once again  $r = 0$  for the same reason, and  $f$  has degree 1. If  $\alpha \notin \mathbb{R}$ , then let  $m = (X - \alpha)(X - \bar{\alpha}) \in \mathbb{R}[X]$ . There must be polynomials  $q, r \in \mathbb{R}[X]$  with  $f = qm + r$  and  $r$  of degree at most 1. Evaluating at  $\alpha$  we find that  $\alpha$  is a root of  $r$ . Thus  $r$  cannot have degree 1, else it would have  $\alpha$  as a root and  $\alpha$  would be real. Therefore  $r$  is constant and, as before  $r = 0$ . Now  $f = qm$  is irreducible so  $q$  must be a non-zero real number and  $\deg f = 2$ .

(c) Suppose that  $f \in \mathbb{C}[X]$  has degree  $n \geq 1$ . Prove that  $f$  has at most  $n$  roots in  $\mathbb{C}$ .

**Solution** We use induction on  $n = \deg f$ . If  $n = 1$ , then the result holds. Next suppose that  $n > 1$ . By the Fundamental Theorem of Algebra, there is  $\beta \in \mathbb{C}$  such that  $f(\beta) = 0$ . There are polynomials  $q, r \in \mathbb{C}[X]$  with  $r$  a constant such that  $f = q(X - \beta) + r$  and evaluating at 0, we find that  $r = 0$ . Now  $\deg f = \deg q + 1$  and  $q$  has at most  $n - 1$  complex roots by induction. Any root of  $f$  must either be  $\beta$  or a root of  $q$ . Therefore  $f$  has at most  $n$  roots in  $\mathbb{C}$ .

(d) Suppose that  $f \in \mathbb{R}[X]$  has degree  $n \geq 1$ . Prove that  $f$  has at most  $n$  roots in  $\mathbb{R}$ .

**Solution** By part (c),  $f$  has at most  $n$  roots in  $\mathbb{C}$ , so it certainly has at most  $n$  roots in  $\mathbb{R} \subseteq \mathbb{C}$ .

6. Suppose that  $R$  is a ring. Show that  $R$  is an integral domain if, and only if,  $R[X]$  is an integral domain.

**Solution** The constants form a copy of  $R$ . Therefore if  $R[X]$  is an integral domain, then  $R$  is an integral domain too. Conversely, suppose that  $R$  is an integral domain and  $f, g$  are non-zero polynomials in  $R[X]$ . Let the leading term of  $f$  be  $aX^m$  and the leading term of  $g$  be  $bX^n$ . Then the leading term of  $fg$  is  $abX^{m+n}$  because  $ab \neq 0$  (since  $R$  is an integral domain). Therefore  $fg \neq 0$ .

7. A polynomial  $f \in \mathbb{Z}[X]$  is called *primitive* if the gcd of its coefficients is 1. Prove that the product of two primitive polynomials is primitive. *This is due to Gauss. You might approach*

the proof like this. Suppose, for contradiction, that a prime number  $p$  is a common divisor of the coefficients of the product of two primitive polynomials. Now interpret this fact in  $\mathbb{Z}_p[X]$  and become concerned.

**Solution** Use the hint and the previous problem. Since  $p$  is prime,  $\mathbb{Z}_p$  is a field and therefore certainly an integral domain. By Problem 6,  $\mathbb{Z}_p[X]$  is an integral domain. Suppose that  $f$  and  $g$  are primitive, and for contradiction, that there is a prime number  $p$  which divides every coefficient of  $fg$ . By reducing all coefficients modulo  $p$ , we can interpret the product in  $\mathbb{Z}_p[X]$ , where the product of the polynomials is 0. Therefore either  $f$  or  $g$  is 0 when viewed in  $\mathbb{Z}_p[X]$ , and viewed in  $\mathbb{Z}[X]$  this means either that  $p$  divides every coefficient of  $f$ , or that  $p$  divides every coefficient of  $g$ . This contradicts the primitivity of  $f$  and  $g$ .

8. Suppose that  $f \in \mathbb{Z}[X]$  and  $f \neq 0$ . We define the *content*  $c(f)$  of  $f$  to be the gcd of the coefficients of  $f$ .

- (a) Prove that  $f = c(f)\widehat{f}$  where  $\widehat{f} \in \mathbb{Z}[X]$  and  $\widehat{f}$  is primitive.

**Solution** Suppose that  $f = \sum_i^k a_i X^i$  and  $a_k \neq 0$ . Now for each  $i$ ,  $a_i = c(f)b_i$  where  $b_i$  is an integer. If  $d > 1$  were a natural number dividing each  $b_i$ , then  $c(f)d$  would divide each  $a_i$ , and this would contradict the definition of  $c(f)$  as the gcd of the coefficients  $a_i$ . Therefore the gcd of the  $b_i$  is 1, and  $\sum_i b_i X^i$  is a primitive polynomial.

- (b) Prove that if  $n \in \mathbb{N}$  and  $f \in \mathbb{Z}[X]$  is primitive, then  $c(nf) = n$ .

**Solution** If the gcd of the coefficients of  $nf$  is  $m$ , then  $n$  divides  $m$  so  $m = kn$  for some positive integer  $k$ . Now  $k$  divides each coefficient of  $f$  and so, by primitivity of  $f$ , is 1. Therefore  $c(nf) = n$ .

- (c) Suppose that  $m, n$  are positive integers, and that  $f, g \in \mathbb{Z}[X]$  are primitive polynomials. Suppose that  $mf = ng$ . Prove that  $m = n$  and  $f = g$ .

**Solution**  $m = c(mf) = c(ng) = n$  by part (b). Therefore  $f = g$ .

- (d) Prove that if  $f, g \in \mathbb{Z}[X]$  and  $f \neq 0 \neq g$ , then  $c(fg) = c(f)c(g)$ .

**Solution** Let  $f = c(f)\widehat{f}$ ,  $g = c(g)\widehat{g}$  and  $fg = c(fg)\widehat{fg}$  where  $\widehat{f}, \widehat{g}$  and  $\widehat{fg}$  are primitive. Now  $f = c(f)\widehat{f}$  and  $g = c(g)\widehat{g}$  so  $c(fg)\widehat{fg} = fg = c(f)c(g)\widehat{f}\widehat{g}$ . Now  $\widehat{f}\widehat{g}$  is primitive by Problem 7, and so  $c(fg) = c(f)c(g)$  by part (c) of this Problem.

- (e) *Harder, use previous parts cleverly.* Suppose that  $f \in \mathbb{Z}[X]$ . Prove that  $f$  is irreducible in  $\mathbb{Z}[X]$  if, and only if,  $f$  is irreducible in  $\mathbb{Q}[X]$ .

**Solution** One way round this is trivial. If  $f \in \mathbb{Z}[X]$  is irreducible in  $\mathbb{Q}[X]$ , then certainly it is irreducible in  $\mathbb{Z}[X]$ . Next let us assume that  $f \in \mathbb{Z}[X]$  is irreducible in  $\mathbb{Z}[X]$  but (for contradiction) that  $f$  is reducible in  $\mathbb{Q}[X]$ . Therefore there are  $g, h \in \mathbb{Q}[x]$ , both of degree smaller than that of  $f$ , with  $f = gh$ . Choose natural numbers  $m, n$  so that  $mg, nh \in \mathbb{Z}[X]$ . Now  $mnf = mg \cdot hf$  so  $mnc(f) = c(mg)c(nf)$ . Therefore  $c(f) = c(mg)c(nf)/(mn)$  is a positive integer. Let  $mg = c(mg)g_1$  and  $nh = c(nh)h_1$  so  $g_1, h_1 \in \mathbb{Z}[X]$  are primitive. now  $f = mg \cdot nh = c(f)g_1 \cdot h_1$ . Now the polynomials  $c(f)g_1$  and  $h_1$  have, respectively, the same degrees as  $g$  and  $h$ , because they are obtained from  $g$  and  $h$  by multiplying by non-zero rational numbers. This contradicts the irreducibility of  $f$  in  $\mathbb{Z}[X]$ .

9. Suppose that  $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$  and that there is a prime  $p$  such that  $p$  does not divide  $a_0$ , but  $p$  divides  $a_i$  for  $1 \leq i \leq n$  but  $p^2$  does not divide  $a_n$ . Prove that  $f$  is irreducible in  $\mathbb{Q}[X]$ . Use Problem 8(e), and worry about what happens in  $\mathbb{Z}_p[X]$ .

**Solution** Suppose, for contradiction, that  $f$  is reducible in  $\mathbb{Q}[X]$ . By Problem 8(e),  $f = gh$  where  $g, h \in \mathbb{Z}[X]$  and each of  $g$  and  $h$  has smaller degree than  $f$ . Now interpret this in  $\mathbb{Z}_p[X]$ . Here  $f$  is a non-zero constant polynomial, so by degree considerations ( $\mathbb{Z}_p$  is an integral domain), both  $g$  and  $h$  must be constants when viewed in  $\mathbb{Z}_p[X]$ . Up in  $\mathbb{Z}[X]$ , this forces the coefficients of the leading terms of  $g$  and  $h$  to be multiples of  $p$ , and so  $a_n$  must be

a multiple of  $p^2$ , which it is not by hypothesis. This contradiction completes the proof. This result is known as *Eisenstein's criterion*. This has the consequence that if  $p$  is a prime number, then for all natural numbers  $n$ , the polynomial  $pX^n + 1$  is irreducible in  $\mathbb{Q}[X]$ . It is not hard to prove a mirror version of Eisenstein's criterion: if  $f = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$  and that there is a prime  $p$  such that  $p$  does not divide  $a_n$ ,  $p$  divides  $a_i$  for  $0 \leq i < n$  but  $p^2$  does not divide  $a_0$ , then  $f$  is irreducible in  $\mathbb{Q}[X]$ . This has the consequence that if  $p$  is a prime number, then for all natural numbers  $n$ , the polynomial  $X^n + p$  is irreducible in  $\mathbb{Q}[X]$ . To prove the second version, suppose that  $f = gh$  is a factorization of  $f$  which satisfies the mirror condition, into polynomials of degree  $m$  and  $n$ . Then  $X^{m+n}f(1/X) = X^m g(1/X) \cdot X^n h(1/X)$  is a factorization of  $X^{m+n}f(1/X)$  in  $\mathbb{Q}[X]$ . However,  $X^{m+n}f(1/X)$  satisfies Eisenstein's criterion, so this forces  $m = 0$  or  $n = 0$ , so  $f$  is irreducible. In fact people use the term *Eisenstein's criterion* for both results.

10. (Tutor pacifier) Find all  $f \in \mathbb{R}[X]$  such that  $q \in \mathbb{Q}$  if, and only if,  $f(q) \in \mathbb{Q}$ .

**Solution** Not yet! Here is a solution to Problem 10 of Sheet 5. The statements was this. *Let  $S$  be a finite set of positive integers which has the following property: if  $x$  is an element of  $S$ , then so too are all positive divisors of  $x$ . A non-empty subset  $T$  of  $S$  is good if whenever  $x, y \in T$  and  $x < y$ , the ratio  $y/x$  is a power of a prime number. A non-empty subset  $T$  of  $S$  is bad if whenever  $x, y \in T$  and  $x < y$ , the ratio  $y/x$  is not a power of a prime number. A single element set is considered both good and bad (by definition, or by vacuous reasoning, as you please). Let  $k$  be the largest possible size of a good subset of  $S$ . Prove that  $k$  is also the smallest number of pairwise-disjoint bad subsets whose union is  $S$ .*

Here is a solution. First notice that a bad subset of  $S$  contains at most one element from a good one, so a partition of  $S$  into bad subsets has at least as many members as a maximal good subset. Notice further that the elements of a good subset of  $S$  must be among the terms of a geometric sequence whose ratio is a prime: if  $x < y < z$  are elements of a good subset of  $S$ , then  $y = xp^\alpha$  and  $z = yq^\beta = xp^\alpha q^\beta$  for some primes  $p$  and  $q$  and some positive integers  $\alpha$  and  $\beta$ , so  $p = q$  for  $z/x$  to be a prime power. Next, let  $P = \{2, 3, 5, 7, 11, \dots\}$  denote the set of prime numbers, let

$$m = \max\{ \exp_p x \mid x \in S \text{ and } p \in P \},$$

where  $\exp_p$  is the exponent of the prime  $p$  in the prime-power decomposition of  $x$ , and notice that a maximal good subset of  $S$  must be of the form  $\{a, ap, \dots, ap^m\}$  for some prime  $p$  and some positive integer  $a$  which is not divisible by  $p$ . Consequently, a maximal good subset of  $S$  has  $m + 1$  elements, so a partition of  $S$  into bad subsets has at least  $m + 1$  members. Finally, notice by maximality of  $m$  that the sets

$$S_k = \{x \mid x \in S \text{ and } \sum_{p \in P} \exp_p x \equiv k \pmod{m + 1}\}$$

(for  $k = 0, 1, \dots, m$ ) form a partition of  $S$  into  $m + 1$  bad subsets. The conclusion follows.

This was Problem 3 of the *28th Balkan Mathematical Olympiad* held in Romania in 2011. The marking scheme allocated 60% of the points for this question to the cunning 'Finally, notice ...' observation. The UK competed as a guest team. Two British students solved this particular problem, including the outright winner of the competition, James Aaronson of St Paul's School.

<http://www.bmo2011.lbi.ro/index.php?page=results>