

# MAT 311: Number Theory

## Spring 2008

### Solutions to HW7

1. Find  $f, g \in \mathbb{Z}[x]$  such that  $\gcd(f, g) = 1$  in  $\mathbb{Z}[x]$  but  $\gcd(f(m), g(m)) > 1$  in  $\mathbb{Z}$  for infinitely many  $m \in \mathbb{Z}$ .  
Let  $f(x) = x^2 + 1, g(x) = x^2 - 1$ .  $\gcd(f, g) = 1$  simple because  $f$  is irreducible over  $\mathbb{Z}$ . However,  $\gcd(f(m), g(m)) \geq 2$  for odd integers  $m$ , because in that case both  $f(m)$  and  $g(m)$  are even.  $\square$
2. Find the minimal polynomials of  $7, \sqrt[3]{7}, (1 + \sqrt[3]{7})/2, 1 + \sqrt{2} + \sqrt{3}$ . Which of those are algebraic integers?  
The minimal polynomials of those numbers are  $x - 7, x^3 - 7, x^3 - (3/2)x^2 + (3/4)x - 1, x^4 - 4x^3 - 4x^2 + 16x - 8$ , respectively. All except the second one are algebraic integers.  $\square$
3. If an algebraic number  $\alpha$  has degree  $n$ , show that  $-\alpha, \alpha^{-1}, \alpha - 1$  have degree  $n$ , too.  
Let  $f(x)$  be the minimal polynomial of  $\alpha$ . Then  $f(-1)^n f(-x), x^n f(x^{-1}), f(x + 1)$  are minimal polynomials of those numbers, respectively. Obviously they are monic and of degree  $n$ . They are irreducible, because otherwise, by reversing the argument we could construct a polynomial of smaller degree for which  $\alpha$  would be the root, contradiction.  $\square$
4. Let  $\alpha = \alpha_1 + a l_2 i$  be an algebraic number. Is it true that  $\alpha_1, \alpha_2$  are algebraic numbers? algebraic integers?  
Note that  $\alpha_1 = 1/2 \cdot (\alpha + \bar{\alpha})$ . Since  $\alpha$  is algebraic, so is  $\bar{\alpha}$ . Since algebraic numbers are closed under addition and subtraction,  $\alpha_1$  is algebraic, too. Since  $\alpha_2 = (\alpha - \alpha_1)/i$  and  $i, \alpha, \alpha_1$  are all algebraic, so is  $\alpha_2$ . However,  $\alpha_1, a l_2$  are not necessarily algebraic *integer*: Let  $\alpha_1 = 1/2, \alpha_2 = \sqrt{3}/2$ . Then  $\alpha$  is an algebraic integer, because it is the cubed-root-of-unity, i.e.  $\alpha^3 - 1 = 0$ , so it is a root of an integral polynomial (we don't have to find the minimal polynomial; as long as it satisfies an integral polynomial, it must be an algebraic integer, that is, the minimal polynomial must automatically be integral). However,  $1/2$  is not an algebraic integer. It's minimal polynomial  $x - 1/2$  is not integral!  $\square$
5. Show that there is an algebraic non-integer  $\alpha$ , with integral norm  $N(\alpha)$ .  
We can take  $\alpha = (3 + 4i)/5$ .  $N(\alpha) = \alpha\bar{\alpha} = 1$  but  $\alpha$  is not an algebraic integer, because its minimal polynomial (over  $\mathbb{Q}$ ) is not integral.
6. If a polynomial  $f \in \mathbb{Z}[x]$  factors into a product  $gh$  in  $\mathbb{Q}[x]$ , prove that there is a factoring  $g_1, h_1$  in  $\mathbb{Z}[x]$ .  
Choose positive integers  $a, b$  such that  $ag, bh$  have integral coefficients and are still primitive (for instance they can be the gcd of the denominators of coefficients of the corresponding polynomial, up to a  $\pm$  sign). Then  $abgh = abf$  is then primitive by the original Gauss' Lemma being a product of two primitive (integral) polynomials. On the other hand  $abf$  has to be equal to  $f$ , because they are both primitive and  $ab > 0$ . Thus,  $ab$  must be 1. Thus  $f = (ag)(bh)$  is the required primitive factoring of  $f$ .  $\square$