

**Problem Set 11th and the last. Due Thursday December 3.**

- (1) Prove that  $\mathbb{Q}[x]/(x^2 - 2x - 1)$  is a ring isomorphic to  $\mathbb{Q}[\sqrt{2}]$ . (*Hint:* Use a root of  $x^2 - 2x - 1$  to construct a homomorphism from  $\mathbb{Q}[x]$  to  $\mathbb{Q}[\sqrt{2}]$ , and then apply the first isomorphism theorem).

**Solution.** First of all, the roots of the polynomial are  $1 \pm \sqrt{2}$ . Now let  $\phi$  be the homomorphism from  $\mathbb{Q}[x]$  to  $\mathbb{Q}[\sqrt{2}]$  defined by  $\phi(f) = f(1 + \sqrt{2})$ . (We proved in Lecture that any such “evaluation map” is a homomorphism). Let’s prove that it is surjective. Let  $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ . We need to find  $f \in \mathbb{Q}[x]$  such that  $f(1 + \sqrt{2}) = a + b\sqrt{2}$ . Consider the polynomial  $f(x) = bx + (a - b)$ . It is in  $\mathbb{Q}[x]$  because  $a, b \in \mathbb{Q}$ . Then  $f(1 + \sqrt{2}) = b(1 + \sqrt{2}) + (a - b) = a + b\sqrt{2}$ .

Now we need to prove that the kernel of  $\phi$  is the ideal generated by  $(x^2 - 2x - 1)$  (let us denote it by  $I$ ). If we proved that, then we could use the Isomorphism theorem to arrive at the conclusion of the problem.

It is very easy to see that  $\text{Ker}\phi \supset I$ : if  $f \in I$ , then  $f(x) = (x^2 - 2x - 1)g(x)$ , so  $f(1 + \sqrt{2}) = 0g(1 + \sqrt{2}) = 0$ , so  $f \in \text{Ker}\phi$ . The only difficult part is to show that  $\text{Ker}\phi \subset I$ . The easiest way is to say that clearly  $\text{Ker}\phi$  does not contain any polynomials of degree 1 (if  $a(1 + \sqrt{2}) + b = 0$ , then  $a$  and  $b$  cannot both be rational). We know that  $\text{Ker}\phi$  is an ideal (Section 6.2). Therefore,  $x^2 - 2x - 1$  is a polynomial of the smallest degree contained in the ideal  $\text{Ker}\phi$ , so it must be a generator of that ideal. Proved!

**An alternative way:** if  $\phi(f) = 0$ , then  $f(1 + \sqrt{2}) = 0$ . Now all we need, is to prove somehow that this implies that  $f(1 - \sqrt{2}) = 0$  also (then  $f$  would have to be divisible by the product of these two linear factors, that is, by our polynomial  $x^2 - 2x - 1$ , and we would be done). So, the last remaining problem sounds like this: *let  $f(x)$  be a polynomial with rational coefficients. Given that  $1 + \sqrt{2}$  is a root of  $f(x)$ , prove that  $1 - \sqrt{2}$  is also a root of  $f(x)$ .* Here’s the most elegant solution I know of.

Consider the automorphism (that is, isomorphism to itself)  $\sigma$  of  $\mathbb{Q}[\sqrt{2}]$  defined by  $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ . Then  $\sigma(x) = x$  if and only if  $x \in \mathbb{Q}$ . Let  $g(x)$  be the polynomial  $\sigma(f(x))$ . Then since  $1 + \sqrt{2}$  is a root of  $f$ , the number  $1 - \sqrt{2}$  is a root of  $g$ . On the other hand, since the coefficients of  $f$  are rational,  $g$  is in fact the same polynomial as  $f$ ! Therefore, both  $1 + \sqrt{2}$  and  $1 - \sqrt{2}$  are roots of  $f$ .

- (2) Let  $\omega \in \mathbb{C}$  be a root of the polynomial  $x^5 - 3x + 6$ . Prove that the subring  $R$  of  $\mathbb{C}$  defined by

$$R = \{a_0 + a_1\omega + \dots + a_4\omega^4 \mid a_i \in \mathbb{Q}, i = 0, \dots, 4\}$$

is a field (you do not need to prove that  $R$  is a ring).

Note that 3 divides all the coefficients of  $x^5 - 3x + 6$  except for the leading coefficient 1, and  $3^2$  does not divide its constant term. Then this polynomial is irreducible in  $\mathbb{Q}[x]$  by Eisenstein’s Criterion (to prove it is one of the extra credit problems). Then  $F = \mathbb{Q}[x]/\langle x^5 - 3x + 6 \rangle$  is a field. Let us prove that this field  $F$  is isomorphic to  $R$ . Let us denote the ideal  $\langle x^5 - 3x + 6 \rangle$  in  $\mathbb{Q}[x]$  by  $I$ . Let us define a homomorphism  $\phi : \mathbb{Q}[x] \rightarrow R$  by the following method: for  $f \in \mathbb{Q}[x]$ , to define  $\phi(f)$ , we write  $f(x) = (x^5 - 3x + 6)g(x) + r(x)$  (where  $r(x)$  is a polynomial of degree at most 4

– the remainder of  $f(x)$  modulo  $x^5 - 3x + 6$ ). Then we define  $\phi(f)$  by the formula  $\phi(f) = r(\omega) \in R$ . We have shown in lecture that such a map is a homomorphism of rings. Clearly,  $\phi$  is surjective: for every  $a_0 + \cdots + a_4\omega^4$ , we have  $\phi(a_0 + \cdots + a_4x^4) = a_0 + \cdots + a_4\omega^4$ . The kernel of  $\phi$  is exactly the ideal that consists of polynomials such that  $r(\omega) = 0$ . We want to show that if  $a_0 + \cdots + a_4\omega^4 = 0$ , then  $a_0 = a_1 = \cdots = a_4 = 0$ . If we prove this, we'll get that  $\text{Ker}(\phi) = I$ , and then by the Isomorphism theorem,  $R \simeq F = \mathbb{Q}[x]/\langle x^5 - 3x + 6 \rangle$ , and we'll be done.

So, it remains to prove that  $\omega$  cannot be a root of a nonzero polynomial of degree 4. Note that it is a very similar problem to what we had to do in Problem 1. Suppose  $g \in \mathbb{Q}[x]$ , and  $g(\omega) = 0$ . Let us divide  $x^5 - 3x + 6$  by  $g(x)$ :

$$x^5 - 3x + 6 = g(x)q_1(x) + r_1(x),$$

where  $r_1(x)$  is the remainder, so that  $\deg(r_1) \leq 3$ . Note that  $r_1(x) \neq 0$ , since  $x^5 - 3x + 6$  is irreducible in  $\mathbb{Q}[x]$ . Since  $\omega$  is a root of  $x^5 - 3x + 6$ , and we assumed that it is a root of  $g$  as well, we get  $r_1(\omega) = 0$ . Now, let us divide  $x^5 - 3x + 6$  by  $r_1(x)$  with remainder:  $x^5 - 3x + 6 = r_1(x)q_2(x) + r_2(x)$ , with  $r_2(x) \neq 0$ , and  $\deg r_2(x) \leq 2$ . Again, we get  $r_2(\omega) = 0$ . Then divide  $x^5 - 3x + 6$  by  $r_2(x)$ ; again we get a remainder, of degree at most 1, which again has to be a nonzero polynomial with root  $\omega$ . Then we'll have that  $\omega$  is a root of a polynomial of degree 1, but then  $\omega \in \mathbb{Q}$ , which is a contradiction, and the proof is complete.

**comment:** Note that we have just proved here that if any complex number  $\omega$  is a root of an irreducible polynomial in  $\mathbb{Q}[x]$  of degree  $k$ , then it cannot be a root of any polynomial in  $\mathbb{Q}[x]$  of degree less than  $k$ .

- (3) (from last year's final exam). Factor the following elements of a ring  $R$  into irreducible elements of  $R$ . Explain why the factors you give are irreducible.
- (a) 15, an element of  $R = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ .

**Solution.**

$$15 = 5 \cdot 3 = 5 \cdot (1 + \sqrt{-2})(1 - \sqrt{-2}).$$

Now, let us prove that 5 and  $1 \pm \sqrt{-2}$  are irreducible. Recall the norm function:  $N(a + b\sqrt{-2}) = a^2 + 2b^2$ . Recall that  $N(z_1z_2) = N(z_1)N(z_2)$ . Then if 5 had been reducible, that is, if  $5 = z_1z_2$ , then  $N(5) = (a_1^2 + 2b_1^2)(a_2^2 + 2b_2^2)$  for some  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ . We have,  $N(5) = 25$ . The only way to factor 25 as a product of two integers is  $25 = 5 \cdot 5$  (of course, we also have  $25 \cdot 1$ , but if  $N(z) = 1$ , then  $z = \pm 1$ , and we are done). So, we have  $a_1^2 + 2b_1^2 = a_2^2 + 2b_2^2 = 5$ , where  $a_i, b_i \in \mathbb{Z}$ . It is easy to see that this is impossible.

Irreducibility of  $1 + \sqrt{-2}$  and  $1 - \sqrt{-2}$  is proved similarly.

- (b)  $x^3 + 1$ , an element of  $\mathbb{F}_7[x]$ . First, let us look for roots of this polynomial in  $F_7$ . We quickly note that  $(-1)^3 + 1 = 0$ , so  $-1 = 6 \in F_7$  is a root (I'll use the notation “-1” rather than “6”). Then by Bezout's theorem,  $x^3 + 1 = (x + 1)g(x)$ . You can either perform long division to find  $g(x)$ , or use elementary algebraic identities (that works over any field), or look for more roots. I'll use the elementary identity:

$$x^3 + 1 = (x + 1)(x^2 - x + 1).$$

Now, let us look for roots of  $x^2 - x + 1$ . Try 0, 1, 2, 3, and get that 3 is a root:  $3^2 - 3 + 1 = 7 = 0$  in  $\mathbb{F}_7$ . Then  $x^2 - x + 1 = (x - 3)h(x)$ . The last step is to find the degree 1 polynomial  $h(x)$ . Again, either by long division (of course, remembering that all the operations happen in  $\mathbb{F}_7$ ), or keep looking for a root:  $h(x)$  is guaranteed to have a root, after all, since it has degree 1). I'll keep looking for a root: get that 5 is a root of  $x^2 - x + 1$ . Finally,

$$x^3 + 1 = (x + 1)(x - 3)(x - 5)$$

in  $\mathbb{F}_7[x]$ . These factors are irreducible since all polynomials of degree 1 over a field are irreducible.

(4) Section 4.10: Problem 26.

**Part (i):** All monic irreducible polynomials of degree 2 have the form:  $x^2 + ax + b$ , with  $a, b \in \mathbb{F}_3$ . For a polynomial of degree 2, “irreducible” is equivalent to “has no roots”. Then  $b \neq 0$ , since 0 cannot be a root. Then, consider the cases  $b = 1$  and  $b = 2$ . If  $b = 1$ , we get  $1^2 + a + 1 \neq 0$ , and  $2^2 + 2a + 1 \neq 0$ . Then  $a \neq 1$ ,  $a \neq 2$ ;  $a = 0$  works, and we get a polynomial  $x^2 + 1$ . Similarly, if  $b = 2$ , then  $a = 1, 2$  work, and  $a = 0$  doesn't.

**Part (ii):** This is pure logic: if  $f$  is reducible, then  $f = gh$  for some  $g, h \in \mathbb{F}_3[x]$ , and  $\deg(g), \deg(h) \neq 0$ . Then degrees of  $g, h$  can be between 1 and 4. If one of them has degree 1, then it means that  $f$  has a root. Thus, degrees of  $g$  and  $h$  have to be at least two, and  $\deg(g) + \deg(h) = \deg(f) = 5$ ; then one of these degrees is 2.

**Part (iii):** Let  $f = x^5 - x + 1$ . The most common mistake: to check that  $f$  has no roots, and conclude that then it is irreducible. This is a mistake, because for a polynomial of degree higher than 4, no roots does not mean irreducible. To check that  $f$  is irreducible, you need to check that it has no roots in  $\mathbb{F}_3$ , and *also* that it is not divisible by any of the polynomials from Part (i). Then by Part (ii) you'll be able to conclude that it is irreducible. I'm skipping the actual check (done by long division, unfortunately).

In short, suppose we checked that  $f$  is irreducible. Then we know from lecture that  $\mathbb{F}_3[x]/\langle f \rangle$  is a field, and it has  $3^{\deg(f)} = 3^5 = 243$  elements (you can refer to this fact).

Let  $I = \langle f \rangle$  – an ideal in  $\mathbb{F}_3[x]$ . Finally, we need to compute the inverse of  $\alpha = [x] = x + I$  in this field. Recall that we proved in lecture that  $\alpha$  is an element of  $L = \mathbb{F}_{3^5}$  that is a root of  $f(x)$ : indeed, if we plug in  $\alpha = x + I$  into  $f(x)$ , we get:

$$f(\alpha) = (x + I)^5 - (x + I) + 1 = x^5 - x + 1 + I = 0 + I,$$

(the last equality is by definition of the ideal  $I$ ), and this means that in the quotient ring  $\mathbb{F}_3/I$ ,  $f(\alpha) = 0$ . Now, all elements of our field  $L = \mathbb{F}_3/I$  have the form  $a_0 + \dots + a_4x^4 + I$ , where  $a_0, \dots, a_4 \in \mathbb{F}_3$ . So, we need to find  $a_0, \dots, a_4$  such that

$$(a_0 + \dots + a_4x^4 + I)(x + I) = 1 + I.$$

This means, we need

$$(a_0 + \dots + a_4x^4)x - 1 \in I.$$

The polynomial  $(a_0 + \cdots + a_4x^4)x - 1$  has degree 5, so it is in  $I$  iff it is a constant multiple of  $x^5 - x + 1$ . We get:

$$-1 + a_0x + a_1x^2 + \cdots + a_4x^5 = c(x^5 - x + 1).$$

Then  $c = -1$  (compare the constant terms), and we get:  $a_0 = 1, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = -1$ .

**Answer:**  $\gamma = 1 - \alpha^4$ . Check that it works:

$$\alpha(1 - \alpha^4) = \alpha - \alpha^5.$$

Recall that  $\alpha$  is a root of  $x^5 - x + 1$ . Then  $\alpha^5 - \alpha + 1 = 0$ , so  $\alpha - \alpha^5 = 1$ , and our  $\gamma$  is correct.

**Another solution:** In fact, there is an alternative way of writing this solution, without the quotient ring: our field  $L = \mathbb{F}_{243}$  consists of elements of the form  $a_0 + a_1\alpha + \cdots + a_4\alpha^4$ , where  $a_i \in \mathbb{F}_3$ . Then we have to solve for the  $a_0, \dots, a_4$ , such that

$$(a_0 + a_1\alpha + \cdots + a_4\alpha^4)\alpha = 1.$$

Remember that  $\alpha^5 - \alpha + 1 = 0$ , so every time we see  $\alpha^5$ , replace it with  $1 - \alpha$ . We get:

$$(a_0 + a_1\alpha + \cdots + a_4\alpha^4)\alpha = 1.$$

$$a_0\alpha + a_1\alpha^2 + \cdots + a_4\alpha^5 = 1.$$

$$a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 + a_4(1 - \alpha) = 1.$$

$$(-a_4 - 1) + (a_0 + a_4)\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 = 0.$$

We have proved in Problem 2 that if  $\alpha$  is a root of degree 5 *irreducible* polynomial, then it cannot also be a root of a degree 4 polynomial, so we get:  $a_4 - 1 = 0, a_0 - a_4 = 0, a_1 = a_2 = a_3 = 0$ , so  $\gamma = -\alpha^4 - 1$ , as before.

(5) Section 3.6: Problem 31.

The answer is no: a Euclidean ring has to be a unique factorization domain. I will show an element that has more than one factorization into irreducibles. Consider the element  $4 = 2^2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ . Using the norm function  $N(a + b\sqrt{-3}) = a^2 + 3b^2$ , we can prove that 2 is irreducible, and also  $1 \pm \sqrt{-3}$  are irreducible (very similar to problem 3(a) above). Then we have an element with two irreducible factorizations, which proves that our ring is not Euclidean.

(6) Section 3.6: problem 33. If a number  $z \in \mathbb{Z}[i]$  has the property that  $N(z)$  is a prime number in  $\mathbb{Z}$ , then  $z$  is prime: since  $\mathbb{Z}[i]$  is a PID, an element  $z$  is prime iff  $z$  is irreducible; and if  $N(z)$  is a prime in  $\mathbb{Z}$ , then  $z$  has to be irreducible, since if  $z = z_1z_2$ , then  $N(z) = N(z_1)N(z_2)$ . (see also Proposition 3.5.11 on p. 132; it says the same thing).

The hard part is to prove the converse: that if  $z$  is a prime element in  $\mathbb{Z}[i]$  with nonzero imaginary part, then  $N(z)$  is a prime number. The other hard part is figuring out which *real* numbers are prime in  $\mathbb{Z}[i]$ . This is done in Corollary 3.5.14 and Lemma 3.5.18. You don't have to know any of this for the exam, but I'll sketch the proof.

Suppose  $z = a + bi$  with  $a, b \neq 0$  is a prime element in  $\mathbb{Z}[i]$ . WE want to show that  $N(z) = a^2 + b^2$  is a prime in  $\mathbb{Z}$ . If  $N(z)$  is not a prime, then it has prime factorization in  $\mathbb{Z}$ :  $N(z) = p_1 \dots p_m$ . Note that  $z \mid N(z)$  (since

$N(z) = z\bar{z}$ . Then, since  $z$  is a prime, we have:  $p_i = zw$  for some  $i$ , and for some  $w \in \mathbb{Z}[i]$ . Then  $p_i = \bar{p}_i = \bar{z}\bar{w}$ . So, we have:  $N(z) = z\bar{z}$ , and then  $N(z) \mid p_i^2$ . This proves that either  $N(z) = p_i$  or  $N(z) = p_i^2$ . If  $N(z) = p_i$ , we are done. If  $N(z) = p_i^2$ , then  $a = 0$  or  $b = 0$  – a contradiction with our assumption.