392 Homework 1 solutions

Exercises 3.2: 1, 2, 3(a)(b)(c),4,6(b)(c)(d),7, 16.

1. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$ is a monic polynomial of degree n with roots $c_1, \ldots, c_n$. Prove that the sum of the roots is $-a_{n-1}$ and the product is $(-1)^n a_0$.

   Proof. We can factorize

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - c_1)(x - c_2)\ldots(x - c_n).$$

   Let us compute the constant term when you expand the right hand side. It is $(-1)^n c_1 c_2 \ldots c_n$. Hence,

$$a_0 = (-1)^n c_1 c_2 \ldots c_n$$

   i.e. the product of the roots is $(-1)^n a_0$. Similarly, let us compute the x^{n-1}-coefficient on the right hand side. It is $-c_1 - c_2 - \cdots - c_n$. So the sum of the roots is $-a_{n-1}$.

2(a) Prove that $\mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[\sqrt{2} + i]$ but $\mathbb{Q}[\sqrt{2}i] \subsetneq \mathbb{Q}[\sqrt{2}, i]$.

   Proof. Since $\sqrt{2}i$ and $\sqrt{2} + i$ are both contained in $\mathbb{Q}[\sqrt{2}, i]$, we have that $\mathbb{Q}[\sqrt{2} + i], \mathbb{Q}[\sqrt{2}i] \subseteq \mathbb{Q}[\sqrt{2}, i]$.

   To show that $\mathbb{Q}[\sqrt{2}, i] = \mathbb{Q}[\sqrt{2} + i]$ it remains to see that $\sqrt{2}$ and i are both contained in $\mathbb{Q}[\sqrt{2} + i]$. Well, we have

$$(\sqrt{2} + i)^3 = -\sqrt{2} + 5i$$

   Hence $\mathbb{Q}[\sqrt{2} + i]$ contains $-\sqrt{2} + 5i + \sqrt{2} + i = 6i$. Hence it contains i, hence it contains $\sqrt{2}$, so they are equal.

   To show that $\mathbb{Q}[\sqrt{2}, i] \supsetneq \mathbb{Q}[\sqrt{2}i]$, we need to show that $i \notin \mathbb{Q}[\sqrt{2}i]$. Well if you have a polynomial in $\sqrt{2}i$ you can only get elements like

$$a_0 + a_1\sqrt{2}i$$

   since the degree 2 or higher terms can be rewritten in terms of the lower ones. Clearly, i is not of this form.

2(b) Prove that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ but $\mathbb{Q}[\sqrt{6}] \subsetneq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

   The argument is very similar. The two main steps.

   Show that $\sqrt{2} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. For that, look at

$$(\sqrt{2} + \sqrt{3})^3 = 9\sqrt{3} + 11\sqrt{2}.$$

   Subtracting $9(\sqrt{2} + \sqrt{3})$ we get $2\sqrt{2}$, hence $\sqrt{2}$ is there.

   Show that $\sqrt{2} \notin \mathbb{Q}[\sqrt{6}]$. But in the latter you only have things of the form $a_0 + a_1\sqrt{6}$ – and such a thing never squares to 2.

2(c) Prove that $\mathbb{Q}[\sqrt[3]{2} + i] = \mathbb{Q}[\sqrt[3]{2}, i]$. What about $\mathbb{Q}[\sqrt[3]{2}i] \subseteq \mathbb{Q}[\sqrt[3]{2}, i]$?

   This one is rather nasty – I'll go over it in class.

3 Find splitting fields of the following polynomials in $\mathbb{Q}[x]$:

   (a) $x^6 + 1$. *The roots are $e^{\pm\pi i/6}, e^{\pm 3\pi i/6}, e^{\pm 5\pi i/6}$. So we just need to adjoin $e^{\pi i/6}$: once we have that we can build the other ones by* *taking powers. Now*

$$e^{\pi i/6} = \cos(\pi/6) + i\sin(\pi/6) = \sqrt{3}/2 + i/2.$$

So the answer is:

$$\mathbb{Q}[e^{\pi i/6}] = \mathbb{Q}[\sqrt{3}, i] = \mathbb{Q}[\sqrt{3} + i]$$

(any of those answers is acceptable).

(b) $(x^2 - 3)(x^3 + 1)$. *We need to adjoin* $\sqrt{3}$ *and* $e^{\pi i/3}$. *Since* $e^{\pi i/3} = 1/2 + i\sqrt{3}/2$, *the answer is the same as in (a)! Namely,*

$$\mathbb{Q}[\sqrt{3} + i].$$

(c) $x^4 - 9$. *The roots are* $\pm\sqrt{3}, \pm\sqrt{3}i$. *So we need to adjoint* $\sqrt{3}$ *and* i *– the answer is the same as (a) and (b)!*

4. Which of the following is a ring, a field or neither?

(a) $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$. *Neither: it is not closed under multiply since* $\sqrt[3]{2} \times \sqrt[3]{2} = \sqrt[3]{4}$ *is not in this set.*

(b) $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$. *This is a field, since it is* $\mathbb{Q}[\sqrt[3]{2}]$ *and* $\sqrt[3]{2}$ *is a root of a polynomial in* $\mathbb{Q}[x]$ *(namely,* $x^3 - 2$*).*

(c) $\{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}$. *Not a ring since* $\sqrt{6} = \sqrt{2}\sqrt{3}$ *is not in there. On the other hand*

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}$$

is a field!

6 Suppose $f(\alpha) = 0$. Find the multiplicative inverse of $\beta \in \mathbb{Q}[\alpha]$:

(b) $f(x) = x^3 + x^2 - 2x - 1$, $\beta = \alpha + 1$.

Take $f(x)$ *and* $p(x) = x + 1$. *Lets compute the GCD using the Euclidean algorithm.*

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

So the GCD is 1, *in fact* $1 = (x^3 + x^2 - 2x - 1) - (x + 1)(x^2 - 2)$. *Now set* $x = \alpha$. *We get that* $1 = -\beta(\alpha^2 - 2)$. *Hence,* $\beta^{-1} = 2 - \alpha^2$.

(c) $f(x) = x^3 + x^2 + 2x + 1$, $\beta = \alpha^2 + 1$.

Take $f(x)$ *and* $p(x) = x^2 + 1$. *Compute the GCD.*

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

Then,

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

So the GCD is 1. *Now write*

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

Plug in $x = \alpha$ *to get*

$$1 = (\alpha^2 + 1) + \alpha(\alpha^2 + 1)(\alpha + 1).$$

Hence,

$$1 = \beta(1 + \alpha^2 + \alpha).$$

Hence $\beta^{-1} = \alpha^2 + \alpha + 1$.

(d) $f(x) = x^3 - 2, \beta = \alpha + 1$.

Take $f(x) = x^3 - 2$ *and* $p(x) = x + 1$ *and apply the Euclidean algorithm.*

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

So $3 = (x+1)(x^2-x+1)-(x^3-2)$. *Set* $x = \alpha$ *to get* $3 = \beta(\alpha^2-\alpha+1)$. *Hence,* $\beta^{-1} = \frac{1}{3}(\alpha^2 - \alpha + 1)$.

7. Let $f(x) \in \mathbb{R}[x]$. (a) Prove that complex roots come in conjugate pairs.

   (b) Prove the only irreducible polynomials in $\mathbb{R}[x]$ are linear or quadratics of the form $ax^2 + bx + c$ with $b^2 - 4ac < 0$.

   (a) Suppose $z \in \mathbb{Z}$ *is a complex root of* f, *i.e.* $f(z) = 0$. *Then,* $\overline{f(z)} = f(\overline{z}) = 0$ *so* $\overline{z}$ *is also a root.*

   (b) Take an irreducible polynomial $f(x) \in \mathbb{R}[x]$ *that is not linear. Then* $f(x)$ *has no real roots. So its complex roots are all in pairs by (a). So when we factor it into linear factors over* $\mathbb{C}$ *(which we can do by FTA) it factors like*

   $$f(x) = (x - \alpha_1)(x - \overline{\alpha_1}) \ldots (x - \alpha_r)(x - \overline{\alpha_r}).$$

   But now look at each conjugate pair:

   $$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}.$$

   This is a real polynomial! So you can collect the conjugate pairs together to get $f(x)$ *factored into a product of real quadratics. Since* $f(x)$ *was irreducible, that means that actually* $f(x)$ *is a quadratic. Now the only real quadratics without real roots are the ones of the form* $ax^2 + bx + c$ *with* $b^2 - 4ac < 0$.

16. NO. In fact $\mathbb{Q}[\pi]$ is isomorphic to $\mathbb{Q}[x]$ since π is transcendental. For instance π itself is not invertible in this ring.