# MAT 150C, Spring 2021
# Solutions to Homework 6

**1.** Suppose that $a$ is not a square in the field $F$. Prove that there is an automorphism $\sigma$ of the field $F[\sqrt{a}]$ such that

$$\sigma(x + y\sqrt{a}) = x - y\sqrt{a} \text{ for all } x, y \in F$$

**Solution 1:** Since $\sigma^2 = \mathrm{id}$, $\sigma$ is a bijection. Let us check that it preserves addition and multiplication: let $z_1 = x_1 + y_1\sqrt{a}, z_2 = x_2 + y_2\sqrt{a}$. Then

$$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)\sqrt{a},\ \sigma(z_1 + z_2) = (x_1 + x_2) - (y_1 + y_2)\sqrt{a},$$
$$\sigma(z_1) + \sigma(z_2) = (x_1 - y_1\sqrt{a}) + (x_2 - y_2\sqrt{a}) = \sigma(z_1 + z_2);$$
$$z_1 z_2 = (x_1x_2 + ay_1y_2) + (x_1y_2 + x_2y_1)\sqrt{a},\ \sigma(z_1z_2) = (x_1x_2 + ay_1y_2) - (x_1y_2 + x_2y_1)\sqrt{a},$$
$$\sigma(z_1)\sigma(z_2) = (x_1 - y_1\sqrt{a})(x_2 - y_2\sqrt{a}) =$$
$$(x_1x_2 + ay_1y_2) - (x_1y_2 + x_2y_1)\sqrt{a} = \sigma(z_1z_2).$$

Therefore

$$\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2),\ \sigma(z_1z_2) = \sigma(z_1)\sigma(z_2)$$

and $\sigma$ is an automorphism.

**Solution 2:** Observe that $F[\sqrt{a}]$ has a basis $1, \sqrt{a}$ over $F$ and the multiplication is completely determined by the equation $\sqrt{a} \cdot \sqrt{a} = a$. Now $\sigma(1) = 1, \sigma(\sqrt{a}) = -\sqrt{a}$, so $\sigma$ is an $F$-linear map which sends a basis to a basis, so it is a bijection. Since $\sigma(\sqrt{a})^2 = (-\sqrt{a})^2 = a = \sigma(a)$, $\sigma$ preserves multiplication and it is an automorphism.

**2.** Suppose that $\sigma(z) = z$ for some $z \in F[\sqrt{a}]$ and $\sigma$ as in Problem 1. Prove that $z$ is an element of $F$.

**Solution:** Let $z = x + y\sqrt{a}$, then $x + y\sqrt{a} = x - y\sqrt{a}$ and $y = 0$ (here we assume that $F$ is not of characteristic 2). Therefore $z = x \in F$.

**3.** Prove that $(2 - \sqrt{3})^n + (2 + \sqrt{3})^n$ is an integer for all $n$. *Hint: use the automorphism $\sigma$ of $\mathbb{Q}[\sqrt{3}]$ from Problems 1 and 2.*

**Solution:** First, we can expand this sum and obtain some expression of the form $A + B\sqrt{3}$ where $A$ and $B$ are some integers. We need to prove that $B = 0$. Indeed, let $\sigma$ be an automorphism of $\mathbb{Q}[\sqrt{3}]$ as above, then

$$\sigma(2 - \sqrt{3}) = 2 + \sqrt{3},\ \sigma(2 + \sqrt{3}) = 2 - \sqrt{3},$$
$$\sigma\left((2 - \sqrt{3})^n\right) = (2 + \sqrt{3})^n,\ \sigma\left((2 + \sqrt{3})^n\right) = (2 - \sqrt{3})^n,$$

so $\sigma(A + B\sqrt{3}) = A + B\sqrt{3}$ and $B = 0$ by problem 2.

**4.** Prove that the distance between $(2 + \sqrt{3})^n$ and the nearest integer becomes arbitrary small for $n \to \infty$.

**Solution:** By problem 3 we have $(2 - \sqrt{3})^n + (2 + \sqrt{3})^n = A_n$ is an integer (depending on $n$). On the other hand, $0 < 2 - \sqrt{3} < 1$, so $(2 - \sqrt{3})^n$ becomes arbitrary small as $n$ approaches 0. Therefore $(2 + \sqrt{3})^n$ becomes arbitrary close to $A_n$.