

Problem Set #1

The road to wisdom? Well, it's plain and simple to express.
Err and err again, but less and less and less.

Instructions: Prove or refute each of the statements below.

0. Show that the (suspicious!) approach from Lecture #1 leads to the conclusion (conjecture?) that $y^2 = x^3 - 5$ has no solutions in $\mathbf{Z}$.

Definition (adjoining an element): If R is a subring¹ of a ring S and $\alpha \in S$, we define

$$\begin{aligned} R[\alpha] &= \{\text{all finite sums } a_0 + a_1\alpha + \cdots + a_n\alpha^n : \text{each } a_i \in R\} \\ &= \{f(\alpha) : f(x) \in R[x]\}. \end{aligned}$$

1. Let D be a nonzero integer.
 - a) $\mathbf{Q}[\sqrt{D}]$ is a field²,
 - b) If $D = \square$, then $\mathbf{Q}[\sqrt{D}] = \mathbf{Q}$. Otherwise, every element of $\mathbf{Q}[\sqrt{D}]$ has one and only one representation in the form $a + b\sqrt{D}$ with $a, b \in \mathbf{Q}$.

Definition: A quadratic field is a field of the form $\mathbf{Q}[\sqrt{D}]$, where $D \in \mathbf{Z}$, $D \neq \square$.

2. Let D_1, D_2 be nonzero rational integers. Then

$$\mathbf{Q}[\sqrt{D_1}] = \mathbf{Q}[\sqrt{D_2}] \iff D_1/D_2 \in (\mathbf{Q}^\times)^2.$$

3. Every quadratic field has the form $\mathbf{Q}[\sqrt{D}]$ for a unique squarefree integer $D \neq 1$. (Recall that $D \in \mathbf{Z}$ is squarefree if D is not divisible by the square of any integer larger than 1.)

Definition: Let $\mathbf{Q}[\sqrt{D}]$ be a quadratic field, where D is assumed squarefree. If $D \equiv 2, 3 \pmod{4}$, we let

$$\mathcal{O}_D = \{a + b\sqrt{D} : a, b \in \mathbf{Z}\}.$$

¹In this course, unless otherwise stated, rings are always assumed commutative and to contain a multiplicative identity

1. Subrings are required to share their multiplicative identity with the ambient ring.

²To make sense of the notation " $\mathbf{Q}[\sqrt{D}]$ " the way we have defined it, we need $\sqrt{D}$ to be a well-defined element of some ring containing $\mathbf{Q}$. There are various ways of doing this. We proceed naively, viewing $\sqrt{D}$ as one of the two complex square roots of D . For definiteness, when D is positive, you can take $\sqrt{D}$ to be the positive real square root. When D is negative, choose the square root with positive imaginary part.

If $D \equiv 1 \pmod{4}$, we let

$$\mathcal{O}_D = \left\{ \frac{1}{2}(a + b\sqrt{D}) : a, b \in \mathbf{Z}, a \equiv b \pmod{2} \right\}.$$

(Why don't we consider $D \equiv 0 \pmod{4}$?)

4. Let $D \in \mathbf{Z}$ be squarefree, $D \neq 1$. Then $\mathcal{O}_D$ is a ring. In fact, $\mathcal{O}_D = \mathbf{Z}[\sqrt{D}]$ when $D \equiv 2, 3 \pmod{4}$, while $\mathcal{O}_D = \mathbf{Z}[\frac{1+\sqrt{D}}{2}]$ when $D \equiv 1 \pmod{4}$.

5. Let $\mathbf{Q}[\sqrt{D}]$ be a quadratic field, with D squarefree. Then for $\alpha \in \mathbf{Q}[\sqrt{D}]$,

$$\alpha \in \mathcal{O}_D \iff \alpha \text{ is a root of a monic quadratic } x^2 + bx + c, \text{ where } b, c \in \mathbf{Z}.$$

6. (harder!) Let $\mathbf{Q}[\sqrt{D}]$ be a quadratic field, with D squarefree. Then for $\alpha \in \mathbf{Q}[\sqrt{D}]$,

$$\alpha \in \mathcal{O}_D \iff \alpha \text{ is a root of some monic polynomial } f(x) \in \mathbf{Z}[x].$$

Suggestions for P5 and P6. We always have that α is a root of $f_\alpha(x) := (x - \alpha)(x - \tilde{\alpha}) \in \mathbf{Q}[x]$, where the tilde denotes conjugation. This easily yields the " $\Rightarrow$ " direction for both P5 and P6. The " $\Leftarrow$ " direction in P5 can be worked out by hand (do it!).

To handle the " $\Leftarrow$ " direction in P6, note that as long as $\alpha \notin \mathbf{Q}$, the polynomial $f_\alpha(x)$ is irreducible as an element of $\mathbf{Q}[x]$. If $f_\alpha(x) \in \mathbf{Z}[x]$, then P5 applies, and $\alpha \in \mathcal{O}_D$. Otherwise, the following two results, familiar from the first-year problem sets, will allow you to prove that α is not the root of any monic polynomial with integer coefficients.

- (i) Fundamental Property of Minimal Polynomials: Let K be a field. Suppose α belongs to a field extension of K and that α is a root of an irreducible polynomial $m(x) \in K[x]$. Whenever $f(x) \in K[x]$ satisfies $f(\alpha) = 0$, we have that $m(x) \mid f(x)$ in $K[x]$.
- (ii) Gauss's Polynomial Lemma: In $\mathbf{Z}[x]$, the content of the product is the product of the contents. (Here the content of a nonzero polynomial in $\mathbf{Z}[x]$ is the greatest common divisor of its coefficients.)

SOLUTIONS (CONTINUED FROM CLASS)

5. When we left off, we agreed it was enough to prove the “ $\Leftarrow$ ” direction. That is, if $\alpha \in \mathbf{Q}[\sqrt{D}]$ is a root of a monic quadratic $x^2 + bx + c$, then $\alpha \in \mathcal{O}_D$.

Notice that if $\alpha \in \mathbf{Q}$, then $\alpha \in \mathbf{Z}$ (in fact, the rational root test tells us that every rational root of $x^2 + bx + c$ is an integer dividing c). In that case, it is clear from the definition of $\mathcal{O}_D$ that $\alpha \in \mathcal{O}_D$. So we may suppose $\alpha \notin \mathbf{Q}$. We apply the quadratic formula to see that

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Since $\alpha \notin \mathbf{Q}$, we know $b^2 - 4c \neq \square$.

Since $2\alpha + b = \pm \sqrt{b^2 - 4c} \in \mathbf{Q}[\sqrt{D}]$, the solution to Problem 2 shows that $b^2 - 4c = Dr^2$ for some rational number r . In fact, $r \in \mathbf{Z}$: If a prime p divides the (lowest-terms) denominator of r , then p^2 divides the denominator of r^2 . Since D is squarefree, p can divide D at most once; so Dr^2 would keep a factor of p in the denominator, contradicting that

$$Dr^2 = b^2 - 4c \in \mathbf{Z}. \quad (*)$$

Rewriting,

$$\alpha = \frac{-b \pm r\sqrt{D}}{2}.$$

To finish: It suffices to show that if $D \equiv 2, 3 \pmod{4}$, then b and r are both even, while if $D \equiv 1 \pmod{4}$, then b and r have the same parity.

Suppose first that $D \equiv 2 \pmod{4}$. Reducing the equation in $(*)$ mod 4 shows that $b^2 \equiv 2r^2 \pmod{4}$. Since $2r^2$ and 4 are even, b must be even. But then $b^2 \equiv 0 \pmod{4}$, implying that $2r^2 \equiv 0 \pmod{4}$. This forces r to be even as well, and we're done.

Now suppose that $D \equiv 3 \pmod{4}$. Reducing the equation in $(*)$ mod 4 shows that $3r^2 \equiv b^2 \pmod{4}$. Since 4 is even, b^2 and $3r^2$ have the same parity. Hence, b and r have the same parity. If r is odd, then $r^2 \equiv 1 \pmod{4}$, forcing $b^2 \equiv 3 \pmod{4}$ — which is impossible for integers b . So it must be that r is even, and hence b is even as well.

Finally, suppose $D \equiv 1 \pmod{4}$. In this case, reducing $(*)$ mod 4 gives $r^2 \equiv b^2 \pmod{4}$, which implies that r and b have the same parity.

6. Since the “ $\Rightarrow$ ” direction here is making a weaker claim than the “ $\Rightarrow$ ” direction in P5, we focus on the “ $\Leftarrow$ ” implication.

We suppose $\alpha \in \mathbf{Q}[\sqrt{D}]$ is a root of a monic polynomial $m(x) \in \mathbf{Z}[x]$. We may assume that $\alpha \notin \mathbf{Q}$: otherwise, the rational root test shows that $\alpha \in \mathbf{Z} \subseteq \mathcal{O}_D$, and we're done.

Our strategy will be to show that

$$f(x) := (x - \alpha)(x - \bar{\alpha})$$

has integer coefficients. Once this is known, the “ $\Leftarrow$ ” implication of P5 implies that $\alpha \in \mathcal{O}_D$.

Expanding $f(x)$, one sees that $f(x) \in \mathbf{Q}[x]$. Since $f(x)$ is quadratic but its roots $\alpha, \bar{\alpha} \notin \mathbf{Q}$, we know that $f(x)$ is irreducible over $\mathbf{Q}$. As $m(x)$ and $f(x)$ share the root α , it must be that $f(x)$ divides $m(x)$ in $\mathbf{Q}[x]$ (by the theory of the minimal polynomial). That is,

$$m(x) = f(x)q(x) \quad \text{for some } q(x) \in \mathbf{Q}[x].$$

We now clear denominators: Choose positive integers A, B with $Af(x) \in \mathbf{Z}[x]$ and $Bq(x) \in \mathbf{Z}[x]$. Then

$$ABm(x) = (Af(x))(Bq(x)).$$

Taking the content of both sides and using Gauss's result that the content of a product is the product of the contents,

$$AB = \text{cont}(ABm(x)) = \text{cont}(Af(x)) \cdot \text{cont}(Bq(x)).$$

(The first equality here comes from $m(x)$ being monic.) So if we set

$$C = \text{cont}(Af(x)), \quad C' = \text{cont}(Bq(x)),$$

then $AB = CC'$, and

$$m(x) = \frac{ABm(x)}{CC'} = \left(\frac{A}{C} f(x) \right) \left(\frac{B}{C'} q(x) \right),$$

where both $\frac{A}{C} f(x), \frac{B}{C'} q(x) \in \mathbf{Z}[x]$.

When a product of two polynomials with integer coefficients is monic, both factors have leading coefficient ± 1 . The leading coefficient of $\frac{A}{C} f(x)$ is $\frac{A}{C}$, which is positive. Thus, $\frac{A}{C} = 1$. Hence, $f(x) = \frac{A}{C} f(x) \in \mathbf{Z}[x]$, which is what we wanted to show!