Marcus, Ch. 2
Selected Problems

Andrew Tindall

June 12, 2020

Problem 8. (a) Let $\omega = e^{2\pi ip}$, p an odd prime. Show that $\mathbb{Q}[\omega]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$. Express $\sqrt{-3}$ and $\sqrt{-5}$ as polynomials in the appropriate ω.

Proof. It is hinted for the first half of this problem that we want to use the fact, proven in Marcus, ch. 2, that $\operatorname{disc}(\omega) = \pm p^{p-2}$, with $+$ holding iff $p \equiv 1 \pmod 4$. Another useful fact is that

$$\operatorname{disc}(\omega) = \prod_{1 \le r < s \le n} (\omega^r - \omega^s)^2.$$

We also note that p is assumed to be an odd prime: therefore, $p-3$ is even and nonnegative: let $k = (p-3)/2$, so that $p^{p-2} = p(p^k)^2$. Putting all of these facts together, we have

$$\left(\prod_{1 \le r < s \le n} (\omega^r - \omega^s) \right)^2 = \pm p(p^k)^2.$$

So, it must be true that

$$\left(\frac{\prod_{1 \le r < s \le n} (\omega^r - \omega^s)}{p^k} \right)^2 = \pm p,$$

So indeed the field $\mathbb{Q}[\omega]$ must contain $\sqrt{\pm p}$, with $+$ holding if and only if $p \equiv 1$ (mod 4).

Since this proof is constructive, we can use it to get a formula for $\sqrt{\pm p}$ in any given cyclotomic field. However, the term $\prod_{1 \le r < s \le n} (\omega^r - \omega^s)$ grows quickly with the degree of the given cyclotomic field. For example, for ω_3 a primitive 3rd root of unity, it is a polynomial of degree 8 in ω_3, before reducing to a quadratic polynomial. However, using $\omega_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, it is not too hard to find

$$\begin{aligned} \omega_3 - \omega_3^2 &= \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) \\ &= \sqrt{3}i \\ &= \sqrt{-3} \end{aligned}$$

In the case of ω_5 a primitive root of unity, it is not as easy to find a polynomial formula for $\sqrt{5}$ in terms of ω_5. For example, one primitive 5th root of unity is

$$\omega_5 = \frac{\sqrt{5}-1}{4} + \frac{\sqrt{10+2\sqrt{5}}}{4}i$$

Instead, we will use the formula derived above. First, we can simplify $\prod_{1\le r<s\le 5}(\omega_5^r - \omega_5^s)$:

$$\prod_{1\le r<s\le 5}(\omega_5^r - \omega_5^s) = \prod_{1\le r<s\le 5}\omega_5^r(1-\omega_5^{s-r}).$$

There are 4 terms where r is equal to 1, 3 where it is equal to 2, 2 where it is 3, and 1 where it is 4. So, we can factor out $\omega_5^{4+3\cdot 2+2\cdot 3+4} = \omega_5^{20}$, which is equal to 1, leaving us with

$$\prod_{1\le r<s\le 5}(1-\omega_5^{s-r}).$$

There are 4 ways to choose $1 \le r < s \le 5$ such that $r - s = 1$, 3 ways to choose them such that $r - s = 2$, and so on. So, we can rewrite this as

$$\prod_{1\le r<s\le 5}(1-\omega_5^{s-r}) = (1-\omega_5)^4(1-\omega_5^2)^3(1-\omega_5^3)^2(1-\omega_5^4).$$

Here, we can rewrite

$$\begin{aligned}(1-\omega_5^4) &= (1-\omega_5^2)(1+\omega_5^2),\\ (1-\omega_5^3) &= (1-\omega_5)(1+\omega_5+\omega_5^2), \text{ and}\\ (1-\omega_5^2) &= (1-\omega_5)(1+\omega_5).\end{aligned}$$

So, we end up with

$$(1-\omega_5)^4(1-\omega_5^2)^3(1-\omega_5^3)^2(1-\omega_5^4) = (1-\omega_5)^7(1+\omega_5)^2(1+\omega_5+\omega_5^2)(1+\omega_5^2)$$

□

(b) Show that the 8th cyclotomic field contains $\sqrt{2}$.

This is not hard to see if we take the primitive 8th root of unity ω_8 to be

$$\omega_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i.$$

From this, we see that

$$\begin{aligned}\omega_8 + \omega_8^7 &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\\ &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\\ &= \sqrt{2}.\end{aligned}$$

(c) Show that every quadratic field is contained in a cyclotomic field: in fact, $\mathbb{Q}[\sqrt{m}]$ is contained in the dth cyclotomic field, where $d = \operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}])$.

Proof. *incomplete* □

Problem 11. (a) Suppose all roots of a monic polynomial $f \in \mathbb{Q}[x]$ have absolute value 1. Show that the coefficient of x^r has absolute value $\leq \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.

Proof. Since all roots of f must exist in $\mathbb{C}$, in $\mathbb{C}[x]$ we can write f as

$$f(x) = \prod_{1 \leq i \leq n} (x - \alpha_i),$$

Where α_i are the roots of f in $\mathbb{C}$. The coefficients of f can be calculated from the α_is: by Vieta's formulas, the coefficient a_r of x^r in a monic polynomial with roots $\alpha_1, \ldots, \alpha_n$ is

$$a_r = (-1)^r \sum_{1 \leq i_1 < i_2 < \cdots < i_r < n} \left(\prod_{j=1}^{r} \alpha_{i_j} \right)$$

Since all terms $-1, \alpha_1, \ldots, \alpha_i$ in this expression have absolute value 1 in $\mathbb{C}$, we see that

$$\begin{aligned} |a_r| &= \left| (-1)^r \sum_{1 \leq i_1 < i_2 < \cdots < i_r < n} \left(\prod_{j=1}^{r} \alpha_{i_j} \right) \right| \\ &\leq \sum_{1 \leq i_1 < i_2 < \cdots < i_r} \left| \prod_{j=1}^{r} \alpha_{i_j} \right| \\ &= \sum_{1 \leq i_1 < i_2 < \cdots < i_r} 1 \\ &= \binom{n}{r} \end{aligned}$$

□

(b) Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1.

Proof. An algebraic integer α of degree n, all of whose conjugates have absolute value 1, has an irreducible polynomial of the kind discussed in part (a); since all the roots of f in $\mathbb{C}$ have absolute value 1, the coefficients of f must have absolute value $\leq \binom{n}{r}$. However, since the coefficients of f all lie in $\mathbb{Z}$, there are only $2\binom{n}{r} + 1$ possibilities for each coefficient a_r of f:

$$-\binom{n}{r}, -\binom{n}{r} + 1, \ldots, -1, 0, 1, \ldots, \binom{n}{r} - 1, \binom{n}{r}$$

Therefore, there are only

$$\prod_{1\le r\le n}\left(2\binom{n}{r}+1\right)$$

possible minimal polynomials. Since only n algebraic integers $\alpha_1,\dots,\alpha_n$ can share the same minimal polynomial f, there can be no more than

$$n\prod_{1\le r\le n}\left(2\binom{n}{r}+1\right)$$

algebraic integers of degree n, all of whose conjugates have absolute value 1. □

(c) Show that α (as in (b)) must be a root of 1. (Show that its powers are restricted to a finite set.)

Proof. Let α be an algebraic integer of degree n, all of whose conjugates have absolute value 1. If α_i is a conjugate of α, then α_i^k is a conjugate of α^k, for any $k \ge 1$ - this shows that each algebraic integer in the sequence $\alpha, \alpha^2, \alpha^3, \dots$ has absolute value 1, and also each of its conjugates has absolute value 1, since

$$\left|\alpha^k\right| = |\alpha|^k = 1, \text{ and}$$

$$\left|\alpha_i^k\right| = |\alpha_i|^k = 1.$$

But as we have seen, the set of all algebraic integers whose conjugates all have absolute value 1 is finite. As a subset of this set, the set $\{\alpha, \alpha^2, \alpha^3, \dots\}$ is also finite: $\alpha^j = \alpha^k$ for some $j \ne k$ - assume WLOG that $j < k$. Then $\alpha^j(1-\alpha^{k-j}) = 0$, showing that α is a $(k-j)$th root of unity. □

Problem 12. Now we can prove Kummer's lemma on units in the pth cyclotomic field, as stated before exercise 26, chapter 1: Let $\omega = e^{2\pi i/p}$, p an odd prime, and suppose u is a unit in $\mathbb{Z}[\omega]$.

(a) Show that $u/\overline{u}$ is a root of 1. (Use 11(c)) above and observe that complex conjugation is a member of the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$.) Conclude that $u/\overline{u} = \pm\omega^k$ for some k.

Proof. Because u is a unit in $\mathbb{Z}[\omega]$, so is $\overline{u}$, and so $u/\overline{u}$ is a well-defined member of $\mathbb{Z}[\omega]$. We know already that $|u/\overline{u}| = 1$, as this holds for every number. What we want to show is that this holds for each conjugate $\sigma_i(u/\overline{u})$ of $u/\overline{u}$, for each embedding of $\mathbb{Q}[\omega]$ in $\mathbb{C}$.

Since complex conjugation is a member of the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$, we know it also corresponds to an embedding σ_j of $\mathbb{Q}[\omega]$ in $\mathbb{C}$. It is shown in Marcus, Ch. 2, that the Galois group of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_p^*$. In particular, it is commutative, so $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$. So, we have

$$\begin{aligned}
\sigma_i(u/\overline{u}) &= \sigma_i(u/\sigma_j(u)) \\
&= \sigma_i(u)/\sigma_i(\sigma_j(u)) \\
&= \sigma_i(u)/\sigma_j(\sigma_i(u)) \\
&= \sigma_i(u)/\overline{\sigma_i(u)}
\end{aligned}$$

So, every conjugate of $u/\overline{u}$ also has absolute value 1, and it fulfills the hypothesis of problem 11. As we showed there, this implies that it is a root of unity. The only roots of unity in $\mathbb{Q}[\omega]$ are the pth roots of unity, and these are exactly $\pm\omega^k$ for $1 \le k \le p$. □

(b) Show that the + sign holds: Assuming $u/\overline{u} = -\omega^k$, we have $u^p = -\overline{u^p}$; whow that this implies that u^p is divisible by p in $\mathbb{Z}[\omega]$. But this is impossible since u^p is a unit.

Proof. Assume we did have $u/\overline{u} = -\omega^k$: then $u = -\overline{u}\omega^k$, and

$$\begin{aligned}
u^p &= (-\overline{u}\omega^k)^p \\
&= (-1)^p\overline{u}^p\omega^{pk} \\
&= -(\overline{u}^p)
\end{aligned}$$

Incomplete - why does this imply that $p \mid u^p$? □

Problem 13. Show that 1 and -1 are the only units in the ring $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$, m squarefree, $m < 0$, $m \neq -1, -3$. What if $m = -1$ or -3?

Proof. Let us first split into cases for the value of m modulo 4. If $m \equiv 0$ or 3 (mod 4), then $\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ is equal to □

Problem 14. Show that $1+\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$, but not a root of 1. Use the powers of $1+\sqrt{2}$ to generate infinitely many solutions to the diophantine equation $a^2 - 2b^2 = \pm 1$.

Proof. We see that the element $-\overline{(1+\sqrt{2})} = -1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is an inverse to $1+\sqrt{2}$:

$$\begin{aligned}
(1+\sqrt{2})(-1+\sqrt{2}) &= -1 + (\sqrt{2})^2 \\
&= -1 + 2 \\
&= 1
\end{aligned}$$

However, it is not a root of unity, as its absolute value, $1+\sqrt{2}$, is greater than 1 - any root of unity must be of absolute value 1 in $\mathbb{C}$.

Therefore, we see that the numbers $\alpha_1, \alpha_2, \ldots$, where $\alpha_i = (1+\sqrt{2})^i$, form an infinite set, and also that they are all units. Also, because $\alpha_1^{-1} = -\overline{\alpha_1}$, we have

$$\alpha_i^{-1} = (-1)^i\overline{\alpha_i}.$$

If we write $\alpha_i = a_i + b_i\sqrt{2}$ for some $a_i, b_i \in \mathbb{Z}$, we have

$$\begin{aligned} a_i^2 - 2b_i^2 &= (a_i + b_i\sqrt{2})(a_i - b_i\sqrt{2}) \\ &= (-1)^n \alpha_i \alpha_i^{-1} &= \pm 1, \end{aligned}$$

With $+$ holding iff $i = 0 \pmod 2$. So, there are an infinite number of solutions to both Diophantine equations $a - 2b^2 = 1$ and $a - 2b^2 = -1$. □

Problem 15. (a) Show that $\mathbb{Z}[\sqrt{-5}]$ contains no element whose norm is 2 or 3.

Proof. Let $\alpha = a + b\sqrt{-5}$ be an arbitrary element of $\mathbb{Z}[\sqrt{-5}]$, and write $N(\alpha)$ for $N^{\mathbb{Q}[\sqrt{-5}]}$. Then $N(\alpha)$ is equal to

$$\begin{aligned} \alpha \cdot \overline{\alpha} &= (a + b\sqrt{-5})(a - b\sqrt{-5}) \\ &= (a^2 + 5b^2). \end{aligned}$$

Therefore $N(\alpha) \pmod 5$ is equal to a^2. The quadratic residues modulo 5 are 0, 1 and 4, so there is no way that $N(\alpha) \equiv 2$ or $3 \pmod 5$. So, $N(\alpha) \neq 2$ or 3. □

(b) Verify that $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is an example of non-unique factorization in the number ring $\mathbb{Z}[\sqrt{-5}]$.

Proof.

$$\begin{aligned} (1 + \sqrt{-5})(1 - \sqrt{-5}) &= 1 + 5 \\ &= 6 \\ &= 2 \cdot 3 \end{aligned}$$

However, the elements $1 + \sqrt{-5}$, $1 - \sqrt{-5}$, 2, and 3 are all irreducible in $\mathbb{Z}[\sqrt{-5}]$:

The norm of $1+\sqrt{-5}$ is 6, so if it could be factored as two nonunits $a \cdot b = 1+\sqrt{5}$, then we would have $N(a) \cdot N(b) = N(\alpha) = 6$. Assuming $N(a) \leq N(b)$, we would have either $N(a) = 1$ and $N(b) = 6$, or $N(a) = 2$ and $N(b) = 3$. We have seen that the second is impossible, and we also know that $N(a) = 1$ only if $a = \pm 1$, and we have assumed it is not a unit. So, $1 + \sqrt{-5}$ is irreducible, as is $1 - \sqrt{-5}$ by the same argument.

Similarly, 2 must be irreducible because its norm is 4; if it could be factored into two nonunits a and b, with $N(a) \leq N(b)$, then either $N(a) = N(b) = 2$, which is impossible, or $N(a) = 1$, so it is a unit. Finally, 3 is irreducible, since its norm is 9, and the norms of its nonunit factors would have to be 3 and 3 or 1 and 9, which is also impossible. So, 6 has non-unique factorization into irreducibles in $\mathbb{Z}[\sqrt{-5}]$. □

Problem 21. Let α be an algebraic integer and let f be a monic polynomial over $\mathbb{Z}$ (not necessarily irreducible) such that $f(\alpha) = 0$. Show that $\operatorname{disc}(\alpha)$ divides $N^{\mathbb{Q}[\alpha]} f'(\alpha)$.

Proof. Let g be the minimal polynomial of α. It is a theorem in Marcus, Ch. 2, that $\mathrm{disc}(\alpha) = N^{\mathbb{Q}[\alpha]}(g'(\alpha))$. Because $f(\alpha) = 0$, it must have g as a factor: say $f = gh$, for some polynomial $h \in \mathbb{Z}[x]$. Then $f' = g'h + gh'$, by the product rule. So, calculating:

$$\begin{aligned} N^{\mathbb{Q}[\alpha]}(f'(\alpha)) &= N^{\mathbb{Q}[\alpha]}(g'(\alpha)h(\alpha) + g(\alpha)h'(\alpha)) \\ &= N^{\mathbb{Q}[\alpha]}(g'(\alpha)h(\alpha) + 0) \\ &= N^{\mathbb{Q}[\alpha]}(g'(\alpha))N^{\mathbb{Q}[\alpha]}(h(\alpha)) \\ &= \mathrm{disc}(\alpha) \cdot N^{\mathbb{Q}[\alpha]}(h(\alpha)) \end{aligned}$$

So, we do see that $\mathrm{disc}(\alpha)$ divides $N^{\mathbb{Q}[\alpha]}(f'(\alpha))$. □

Problem 22. Let K be a number field of degree n over $\mathbb{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. We know that $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will show that $d \equiv 0$ or $1 \pmod 4$. Letting $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, we know that d is the square of the determinant $|\sigma_i(\alpha_j)|$. This determinant is a sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P denote the sum of the terms corresponding to even permutations, and let N denote the sum of the terms (without negative signs) corresponding to odd permutations. Thus $d = (P - N)^2 = (P + N)^2 - 4PN$. Complete the proof by showing that $P + N$ and PN are in $\mathbb{Z}$.

In particular we have $\mathrm{disc}(\mathbb{A} \cap K) \equiv O$ or $1 \pmod 4$. This is known as *Stickelberger's criterion.*

Problem 23. Just as with the trace and norm, we can define the relative discriminant disc_K^L of an n-tuple, for any pair of number fields $K \subset L$, $[L : K] = n$.

(a) Generalize Theorems $6 - 8$ and the corollary to Theorem 6.

Proof. ¡++¿ □

(b) Let $K \subset L \subset M$ be number fields, $[L : K] = n$, $[M : L] = m$ and let $[\alpha_1, \ldots, \alpha_n]$ and $[\beta_1, \ldots, \beta_m]$ be bases for L over K adn M over L, respectively. Establish the formula

$$\mathrm{disc}_K^M(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = (\mathrm{disc}_K^L(\alpha_1, \ldots, \alpha_n))^m N_K^L \mathrm{disc}_L^M(\beta_1, \ldots, \beta_m).$$

Proof. ¡++¿ □

(c) Let K and L be number fields satisfying the conditions of Corollary 1, Theorem 12. Show that $(\mathrm{disc} T) = (\ \mathrm{disc} R)^{[L:Q]}(\mathrm{disc}\ S)^{[K:\mathbb{Q}]}$. (This can be used to obtain a formula for $\mathrm{disc}(\omega)$, $\omega = e^{2\pi i/m}$)