Selected Problems from Marcus, Number Fields

Sayer Herin

August 17, 2006

I have selected several problems from Marcus' *Number Fields*. Some consist of legwork for theorems and will be designated accordingly. Others are found in the lists of problems at the end of each chapter. Some introduction will be provided before many problems.

Let $\omega = e^{2\pi i/m}$, a primitive m^{th} root of unity. Let us call $\mathbb{Q}[\omega]$ the m^{th} cyclotomic field over $\mathbb{Q}$.

Proposition (page 12). *If m is odd then $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$. Alternatively, the m^{th} cyclotomic field is the same as the $2m^{th}$.*

Proof. Let m be odd, $m > 0$. Let $\omega = e^{2\pi i/2m}$.
Note: $\mathbb{Q}[\omega] \supset \mathbb{Q}[\omega^2]$ since $\omega^2 \in \mathbb{Q}[\omega]$.

$$-\omega = e^{2\pi i}e^{2\pi i/2m} = e^{2\pi i + 2\pi i/2m} = e^{2(m+1)\pi i/2m} = \omega^{m+1} = \omega^{2n} = (\omega^2)^n$$

for some n since m is odd. So $-\omega \in \mathbb{Q}[\omega]$ and $-1 \in \mathbb{Q}$ so $\omega \in \mathbb{Q}[\omega^2]$.
Hence $\mathbb{Q}[\omega] \subset \mathbb{Q}[\omega^2]$ and therefore $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$. □

Exercise 2.5. *Let $f \in \mathbb{Z}/p\mathbb{Z}$ with p prime. Show $f(x^p) = (f(x))^p$.*

Proof. By induction on the number of terms.
1 term:

$$f(x^p) = a(x^p)^m = a(x^{pm}) = a(x^m)^p = 1a(x^m)^p = a^{p-1}a(x^m)^p \overset{1}{=} (ax^m)^p = (f(x))^p$$

(1: Multiplication is commutative in $\mathbb{Z}/p\mathbb{Z}$.)
Assume true for n terms.
$n+1$ terms: Let $f(x) = g(x) + h(x)$ where $g(x)$ has n terms and $h(x)$ has 1 term.

$$f(x^p) = g(x^p) + h(x^p) = (g(x))^p + (h(x))^p \overset{2}{=} (g(x) + h(x))^p = (f(x))^p$$

(2: Since $a^p + b^p = (a+b)^p$ in $\mathbb{Z}/p\mathbb{Z}$.) □

Exercise 2.14. *Show that* $1+\sqrt{2}$ *is a unit in* $\mathbb{Z}[\sqrt{2}]$*, but not a root of* 1*. Use powers of* $1+\sqrt{2}$ *to find infinitely many solutions to the diophantine equation* $a^2-2b^2=\pm 1$*.*

Proof. Note that $(\sqrt{2}+1)(\sqrt{2}-1)=\sqrt{2}^2-1^2=1$. So $1+\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.
To check that it is not a root of 1, remember that $\mathbb{Z}[\sqrt{2}]\subset\mathbb{R}$ and that it is in fact a subring. Now note that $(1+\sqrt{2})^n>(1+\sqrt{2})^{n-1}$ since $(1+\sqrt{2})>1$. This argument shows that all the powers of $1+\sqrt{2}$ are distinct and hence not a root of 1. Also $(1+\sqrt{2})^n*(1-\sqrt{2})^n=(-1)^n$ so $(1+\sqrt{2})^n$ is a unit and since the norm in $\mathbb{Z}[\sqrt{2}]$ is multiplicative, $N((1+\sqrt{2})^n)=|a^2-2b^2|=1$. This gives infinitely many solutions to $a^2-2b^2=\pm 1$ since the powers are distinct. □

Exercise 2.15.

a) Show that $\mathbb{Z}[\sqrt{-5}]$ *contains no element of norm 2 or 3.*

b) Verify that $2*3=(1+\sqrt{-5})(1-\sqrt{-5})=6$ *is an example of non-unique factorization in* $\mathbb{Z}[\sqrt{-5}]$

Proof.

a) By way of contradiction, assume so.
Then $\exists a,b\in\mathbb{Z}$ *s.t.* $\|a+b\sqrt{-5}\|=2$ *or* $=3$. $\|a+b\sqrt{-5}\|=|a^2+5b^2|=2$ *or* $=3$ So, taking this equation mod 5, we are left with $a^2\equiv 2 \pmod 5$ or $a^2\equiv 3 \pmod 5$ since 5b is divisible by 5 and $-2\equiv 3 \pmod 5$. But note, $a^4\equiv 1 \pmod 5$ for $a\neq 0$ so $a^2\equiv\pm 1 \pmod 5$.⇒⇐ □

b) $\|2\|=4$ so if $a|2$ then $\|a\||4\Rightarrow\|a\|=1$ *or* 4 since there are no elements of norm 2. So either a is a unit or $2=au$ where u is a unit. Similarly for 3. But note, $\|1\pm\sqrt{-5}\|=6$ and $4\not|6$ and $9\not|6$. Hence these are two non-unique factorizations of 6. □

Exercise 2.27. *Let G and H be two free abelian groups of rank n in K, with $H \subset G$.*

a) Show that G/H is finite.

b) Show that G has a generating set $\beta_1, \ldots, \beta_n$ such that (for appropriate integers d_i) $d_1\beta_1, \ldots, d_n\beta_n$ is a generating set of H.

c) Show that $disc(H) = |G/H|^2 disc(G)$.

d) Show that if $\alpha_1, \ldots, \alpha_n \in R = \mathbb{A} \bigcap K$ then they form an integral basis for R iff $disc(\alpha_1, \ldots, \alpha_n) = disc(R)$.

e) Show that if $\alpha_1, \ldots, \alpha_n \in R = \mathbb{A} \bigcap K$ and $disc(\alpha_1, \ldots, \alpha_n)$ is square free then the α_i form an integral basis for R

Proof.

a) Without loss of generality, $G = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ since they are isomorphic. Since $H \leq G$ then $H = k_1\mathbb{Z} \oplus k_2\mathbb{Z} \oplus \cdots \oplus k_n\mathbb{Z}$ with $k_i \in \mathbb{Z}\backslash\{0\}$, since H restricted to each coordinate must be a subgroup of $\mathbb{Z}$ and it is of rank n. Hence,

$$G/H = \frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}{k_1\mathbb{Z} \oplus k_2\mathbb{Z} \oplus \cdots \oplus k_n\mathbb{Z}} \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \mathbb{Z}/k_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_n\mathbb{Z}$$

So, since k_i is never 0, then G/H is a finite abelian group which is isomorphic to a direct sum of at most n cyclic groups. □

b) Further, if $\beta_1, \ldots, \beta_n \in K$ generate G then $k_1\beta_1, \ldots, k_n\beta_n$ generate H since they do under the canonical isomorphism into $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. □

c) From b), $\beta_1, \ldots, \beta_n$ is a basis for G and $k_1\beta_1, \ldots, k_n\beta_n$ is a basis for H. Also,

$$\begin{pmatrix} k_1\beta_1 \\ k_2\beta_2 \\ \vdots \\ k_n\beta_n \end{pmatrix} = \begin{pmatrix} k_1 & 0 & \cdots & 0 \\ 0 & k_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & k_n \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

Note that $disc(\alpha_1, \ldots, \alpha_k) = |\sigma_i(\alpha_j)|^2$ (the square of the determinant of the matrix). Also, since $H \subset G$ of equal rank, then an embedding of one corresponds to an embedding of the other (by multiplication or division). So by applying σ_i to each of the n equations, we

arrive at the equation $[\sigma_j(k_i\beta_i)] = M[\sigma_j(\beta_i)]$ where M is the previous diagonal matrix. So, now, by taking determinants and squaring, we see that $disc(k_1\beta_1, \ldots, k_n\beta_n) = |M|^2 disc(\beta_1, \ldots, \beta_n)$ so we have $disc(H) = |G/H|^2 disc(G)$. (Since the determinant of a diagonal matrix is the product of the diagonal elements.) □

d) Note: Integral basis implies equality of discriminants by Theorem 11.

So, we must prove the converse. The α_i are linearly dependent iff their discriminant (in R) is 0 (Theorem 7). So, we can assume that they generate a free abelian group of rank n. Call this H. $\alpha_i \in R \Rightarrow H \subset R$. Now, by c) we see that $|R/H| = 1$ and hence $H = R$. □

e) Similarly to d), we see that the α_i form a basis for a subgroup H with equal rank to R. Then $disc(H) = |R/H|^2 disc(R)$ and since $|R/H|$ is an integer, then it must be 1. So they are equal. □

Exercise 3.2. *Prove that a finite integral domain is a field; in fact show that for each $\alpha \neq 0$ we have $\alpha^n = 1$ and hence $\alpha^{n-1} = \alpha^{-1}$.*

Proof. Let K be a finite integral domain, $\alpha \in K, \alpha \neq 0$. Then $\exists k, l \in \mathbb{N}, k \neq l$ *s.t.* $\alpha^k = \alpha^l$ since K is finite. Assume without loss of generality that $k > l$. So, $\alpha^k = \alpha^{k-l+l} = \alpha^{k-l}\alpha^l = \alpha^l$. Hence $\alpha^{k-l} = 1$ by cancelation. Also, $\alpha^{k-l-1} = \alpha^{-1}$. □

Exercise 3.7. *Show that if I and J are ideals in a commutative ring s.t. $1 \in I + J$, then $1 \in I^m + J^n$ $\forall m, n \in \mathbb{N}$.*

Proof. Note: $1 = \alpha + \beta$ with $\alpha \in I, \beta \in J$.
Let $k = m + n$. Then:

$$1 = 1^k = (\alpha + \beta)^k = \sum_{i=0}^{k} \binom{k}{i} \alpha^i \beta^{k-i}$$

and each term is in either I^m or in J^n. Since if $i \leq m$ then $k - i \geq n$ so $\alpha^i \beta^{k-i} \in J^n$. Similarly if $i > m$ then $\alpha^i \beta^{k-i} \in I^m$. □