Daniel A. Marcus

Number Fields

Daniel A. Marcus

Number Fields

Springer-Verlag
New York Heidelberg Berlin

Dr. Daniel A. Marcus

Department of Mathematics
The Ohio State University
Columbus, Ohio 43210

AMS Subject Classifications: 12-01, 12Axx, 12Cxx

Library of Congress Cataloging in Publication Data

Marcus, Daniel A 1945–
Number fields

(Universitext)
"This book grew out of the lecture notes of a course at Yale University in the fall semester, 1972"
Bibliography: p
Includes indexes
1 Algebraic number theory 2 Fields, Algebraic. I. Title.
QA247.M346 512'.74 77-21467

Printed in the United States of America

9 8 7 6 5 4 3 2 1

ISBN 0-387-90279-1 Springer-Verlag New York
ISBN 3-540-90279-1 Springer-Verlag Berlin Heidelberg

Foreword

This book grew out of the lecture notes of a course which I gave at Yale University in the Fall semester, 1972. Exercises were added and the text was rewritten in 1975 and 1976. The first four chapters in their present form were used in a course at Ohio State University in the Fall quarter, 1975.

The first six chapters can be read, in conjunction with appendices 1 - 3, by anyone who is familiar with the most basic material covered in standard undergraduate courses in linear algebra and abstract algebra. Some complex analysis (meromorphic functions, series and products of functions) is required for chapters 7 and 8. Specific references are given.

The level of exposition rises as the book progresses. In chapter 2, for example, the degree of a field extension is defined, while in chapter 4 it is assumed that the reader knows Galois theory. The idea is to make it possible for someone with little experience to begin reading the book without difficulty and to be lured into reading further, consulting the appendices for background material when necessary.

I have attempted to present the mathematics in a straightforward, "down to earth" manner that would be accessible to the inexperienced reader but hopefully still interesting to the more sophisticated. Thus I have avoided local methods with no apparent disadvantages except possibly in exercises 20-21 of chapter 3 and exercises 19-22 of chapter 4. Even there I feel that it is worthwhile to have available "direct" proofs such as I present. Any awkwardness therein can be taken

by the reader as motivation to learn about localization. At the same time, it is assumed that the reader is reasonably adept at filling in details of arguments. In many places details are left as exercises, often with elaborate hints. The purpose of this is to make the proofs cleaner and easier to read, and to promote involvement on the part of the reader.

Major topics are presented in the exercises: fractional ideals and the different in chapter 3, ramification groups and the Kronecker-Weber Theorem in chapter 4, fundamental units in non-totally real cubic fields in chapter 5, cyclotomic class numbers and units in chapter 7. Many other results appear in step-by-step exercise form. Among these are the determination of the algebraic integers in pure cubic fields (chapter 2), the proof that prime divisors of the relative different are ramified over the ground field (chapter 4), and the Frobenius Density Theorem (chapter 7).

I have taken the liberty to introduce some new terminology ("number ring" for the ring of algebraic integers in a number field), a notational reform ($\|I\|$ for the index of an ideal I in a number ring, rather than the more cumbersome $N(I)$), and the concept of polar density, which seems to be the "right" density for sets of primes in a number field. Notice, for example, how easily one obtains Theorem 43 and its corollaries.

Chapter 8 represents a departure from tradition in several ways. The distribution of primes is handled in an abstract context (Theorem 48) and without the complex logarithm. The main facts of class field theory are stated without proof (but, I hope, with ample motivation) and without fractional ideals. Results on the distribution of primes are then derived from these facts. It is hoped that this chapter will be of some help to the reader who goes on to study class field theory.

Daniel A. Marcus
Columbus, Ohio
June, 1977

Table of contents

Chapter 1
A special case of Fermat's conjecture

Algebraic number theory is essentially the study of number fields, which are the finite extensions of the field $\mathbb{Q}$ of rational numbers. Such fields can be useful in solving problems which at first appear to involve only rational numbers. Consider, for example, this problem:

> Find all primitive Pythagorean triples: i.e., integer solutions of $x^2 + y^2 = z^2$ having no common factor.

Assuming that we have such a triple and considering the equation mod 4, we find immediately that z must be odd. This will be used later. Now comes the introduction of a number field (namely $\mathbb{Q}[i] = \{a + bi: a,b \in \mathbb{Q}\}$) into the problem: if we factor the left side of the equation we obtain

$$(x + yi)(x - yi) = z^2$$

and thus we have a multiplicative problem in the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi: a,b \in \mathbb{Z}\}$. It is well known (see exercise 7 at the end of this chapter) that $\mathbb{Z}[i]$ is a unique factorization domain: every nonzero Gaussian integer can be expressed in a unique way (up to order and unit factors) as a product of Gaussian primes. We will use this fact to show that $x + yi$ has the form $u\alpha^2$ for some Gaussian integer α and some Gaussian integer unit u. If we then write $\alpha = m + ni$ and observe that the only units in $\mathbb{Z}[i]$ are ± 1 and

$\pm i$ (see exercise 2), we obtain

$$\{x,y\} = \{\pm(m^2 - n^2), \pm 2mn\}$$

$$z = \pm(m^2 + n^2) .$$

It is obviously necessary that m and n be relatively prime and not both odd (otherwise x, y, and z would have a factor in common) and it is easy to see that a primitive Pythagorean triple results from any such choice of m and n, and a choice of signs. Furthermore it is clear that nothing is lost if we take only positive m and n.

Thus the problem will be solved if we can show that for any primitive solution, $x + yi$ has the form $u\alpha^2$. To do this, it is enough to show that if π is a Gaussian prime dividing $x + yi$, then in fact π divides $x + yi$ an even number of times: $\pi^e \mid x + yi$ and $\pi^{e+1} \nmid x + yi$ for some even e. Since $(x + yi)(x - yi) = z^2$ and π obviously divides z^2 an even number of times (twice as many times as it divides z), we need only show that $\pi \nmid x - yi$.

Thus, supposing that π divides both $x + yi$ and $x - yi$, we want a contradiction. Adding, we get $\pi \mid 2x$. Also we have $\pi \mid z$. But $2x$ and z are relatively prime integers (recall that z is odd, and if x and z had a non-trivial factor in common, then so would x, y, and z). So there exist integers m and n such that $2xm + zn = 1$. But then $\pi \mid 1$ in $\mathbb{Z}[i]$. This is impossible since π is a prime, not a unit.

Thus by working in the field $\mathbb{Q}[i]$ we have determined all primitive Pythagorean triples.

Since this was so successful, let us try to apply the same idea to the equation $x^n + y^n = z^n$ for $n > 2$. Fermat, in his famous marginal note, claimed that he had a proof that there are no solutions in nonzero integers when $n > 2$. This is known as "Fermat's last theorem" or more accurately, since no proof is known by anyone presently alive, "Fermat's conjecture."

Using our result on primitive Pythagorean triples, we can show that Fermat was right for $n = 4$ and hence (automatically) also for any multiple of 4. (See

exercise 15.) It is therefore sufficient to consider only the case in which n is an odd prime p, since if no solutions exist when $n = p$ then no solutions exist when n is a multiple of p. Thus the problem is to show that if p is an odd prime, then $x^p + y^p = z^p$ has no solution in nonzero integers x, y, z.

Suppose, for some odd prime p, there is a solution $x,y,z \in \mathbb{Z} - \{0\}$. Clearly we may assume that x, y, z have no common factor (divide it out if there is one). We want a contradiction. It is convenient to separate the argument into two cases: either p divides none of x, y, z (case 1), or else p divides exactly one of them (case 2). (If p divided more than one then it would divide all three, which is impossible.)

We will consider only case 1. It is easy to show that $x^3 + y^3 = z^3$ has no case 1 solutions: If x, y, and z are not multiples of 3, then in fact $x^3 + y^3 \not\equiv z^3 \pmod 9$ since each of these cubes is $\equiv \pm 1 \pmod 9$.

Now assume $p > 3$; x, y, and z are not multiples of p; and $x^p + y^p = z^p$. Factoring the left side, we obtain

$$(1) \qquad (x + y)(x + y\omega)(x + y\omega^2) \dots (x + y\omega^{p-1}) = z^p$$

where ω is the pth root of unity $e^{2\pi i/p}$. (To see why this is true, note that $1, \omega, \omega^2, \dots, \omega^{p-1}$ are the p roots of the polynomial $t^p - 1$, hence we have the identity

$$(2) \qquad t^p - 1 = (t - 1)(t - \omega)(t - \omega^2) \dots (t - \omega^{p-1}),$$

from which (1) follows by substituting the number $\frac{-x}{y}$ for the variable t.)

Thus we have a multiplicative problem in the number field $\mathbb{Q}[\omega]$, and in fact in the subring $\mathbb{Z}[\omega]$.* Kummer attempted to prove Fermat's conjecture by assuming that the unique factorization property of $\mathbb{Z}$ and $\mathbb{Z}[i]$ generalizes to

*$\mathbb{Q}[\omega] = \{a_0 + a_1\omega + \dots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Q} \ \forall i\}$;

$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \dots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Z} \ \forall i\}$.

the ring $\mathbb{Z}[\omega]$. Unfortunately it does not. For example if $p = 23$, then not all members of $\mathbb{Z}[\omega]$ factor uniquely into irreducible elements: i.e., elements $\alpha \in \mathbb{Z}[\omega]$ which are not units and such that whenever $\alpha = \beta\gamma$, either β or γ is a unit (see exercise 20). In other words, $\mathbb{Z}[\omega]$ is not a unique factorization domain (UFD) for $p = 23$. It is, however, a UFD for all primes less than 23. For these primes Kummer's argument is valid, showing that $x^p + y^p = z^p$ has no case 1 solutions.

The argument can be organized as follows: Assuming that $\mathbb{Z}[\omega]$ is a UFD, it can be shown that $x + y\omega$ has the form $u\alpha^p$ for some $\alpha \in \mathbb{Z}[\omega]$ and some unit $u \in \mathbb{Z}[\omega]$. It can then be shown that the equation $x + y\omega = u\alpha^p$, with x and y not divisible by p, implies that $x \equiv y \pmod{p}$. (See exercises 16-28 for the details.) Similarly, writing $x^p + (-z)^p = (-y)^p$, we obtain $x \equiv -z \pmod{p}$. But then

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \pmod{p},$$

implying that $p \mid 3x^p$. Since $p \nmid x$ and $p \neq 3$, this is a contradiction. Thus case 1 of Fermat's conjecture can be established for all primes p for which $\mathbb{Z}[\omega]$ is a UFD.

What can be done for other primes? Unique factorization in $\mathbb{Z}[\omega]$ was needed only for the purpose of deducing $x + y\omega = u\alpha^p$ from equation (1); might it not be possible to deduce this in some other way? The answer is yes for certain values of p, including for example $p = 23$. This results from Dedekind's amazing discovery of the correct generalization of unique factorization: although the elements of $\mathbb{Z}[\omega]$ may not factor uniquely into irreducible elements, the ideals in this ring always factor uniquely into prime ideals. Using this, it is not hard to show that the principal ideal $(x + y\omega)$ is the pth power of some ideal I (see exercises 19 and 20). For certain p, called "regular" primes (defined below), it then follows that I must itself be a principal ideal, say (α), so that

$$(x + y\omega) = I^p = (\alpha)^p = (\alpha^p)$$

and thus again we have $x + y\omega = u\alpha^p$ for some unit u. As before, this implies $x \overset{\cdot}{\equiv} y \pmod p$ and a contradiction follows. Thus case 1 of Fermat's conjecture can be established for all regular primes, which we now define.

There is an equivalence relation $\sim$ on the set of ideals of $\mathbb{Z}[\omega]$, defined as follows: for ideals A and B

$$A \sim B \text{ iff } \alpha A = \beta B \text{ for some } \alpha, \beta \in \mathbb{Z}[\omega].$$

(Verify that this is an equivalence relation.)

It turns out (see chapter 5) that there are only finitely many equivalence classes of ideals under $\sim$. The number of classes is called the class number of the ring $\mathbb{Z}[\omega]$, and is denoted by the letter h. Thus h is a function of p.

DEFINITION: A prime p is regular iff $p \nmid h$.

To explain why I (in the equation $(x + y\omega) = I^p$) must be principal whenever p is a regular prime, we note first that the ideal classes can be multiplied in the obvious way: the product of two ideal classes is obtained by selecting an ideal from each; multiplying them; and taking the ideal class which contains the product ideal. This is well-defined: The resulting ideal class does not depend on the particular ideals chosen, but only on the two original ideal classes (prove this). Multiplied in this way, the ideal classes actually form a group. The identity element is the class C_0 consisting of all principal ideals (which really is a class; see exercise 31). The existence of inverses will be established in chapter 3. Thus the ideal classes form a finite abelian group, called the ideal class group. If p is regular then clearly this group contains no element of order p, and it follows that if I^p is principal then so is I: Let C be the ideal class containing I; then C^p is the class containing I^p, which is C_0. Since C_0 is the identity in the ideal class group and C cannot have order p, it follows that $C = C_0$, which shows that I is principal.

As we noted before, this leads to a contradiction, showing that $x^p + y^p = z^p$

has no case 1 solutions (i.e., solutions for which $p \nmid xyz$) when p is a regular prime. It is also possible, although somewhat more difficult, to show that no case 2 solutions exist for regular primes. (For this we refer the reader to Borevich and Shafarevich's Number Theory, p. 378-381.) Thus Fermat's conjecture can be proved for all regular primes p, hence for all integers n which have at least one regular prime factor. Unfortunately irregular primes exist (e.g. 37, 59, 67). In fact there are infinitely many. On the other hand, it is not known if there are infinitely many regular primes.

In any case our attempt to prove Fermat's conjecture leads us to consider various questions about the ring $\mathbb{Z}[\omega]$: What are the units in this ring? What are the irreducible elements? Do elements factor uniquely? If not, what can we say about the factorization of ideals into prime ideals? How many ideal classes are there?

The investigation of such problems forms a large portion of classical algebraic number theory. More accurately, these questions are asked in subrings of arbitrary number fields, not just $\mathbb{Q}[\omega]$. In every number field there is a ring, analogous to $\mathbb{Z}[\omega]$, for which there are interesting answers.

EXERCISES

1-9: Define $N: \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a + bi) = a^2 + b^2$.

1. Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using the fact that $N(a + bi) = (a + bi)(a - bi)$. Conclude that if $\alpha | \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) | N(\gamma)$ in $\mathbb{Z}$.

2. Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only units are ± 1 and $\pm i$.

3. Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.

4. Show that $1 - i$ is irreducible in $\mathbb{Z}[i]$ and that $2 = u(1 - i)^2$ for some unit u.

5. Notice that $(2 + i)(2 - i) = 5 = (1 + 2i)(1 - 2i)$. How is this consistent with unique factorization?

6. Show that every nonzero, non-unit Gaussian integer α is a product of irreducible elements, by induction on $N(\alpha)$.

7. Show that $\mathbb{Z}[i]$ is a principal ideal domain (PID); i.e., every ideal I is principal. (As shown in Appendix 1, this implies that $\mathbb{Z}[i]$ is a UFD.) Suggestion: Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized, and consider the multiplies $\gamma\alpha$, $\gamma \in \mathbb{Z}[i]$; show that these are the vertices of an infinite family of squares which fill up the complex plane. (For example, one of the squares has vertices 0, α, $i\alpha$, and $(1 + i)\alpha$; all others are translates of this one.) Obviously I contains all $\gamma\alpha$; show by a geometric argument that if I contained anything else then minimality of $N(\alpha)$ would be contradicted.

8. We will use unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

   (a) Use the fact that the multiplicative group $\mathbb{Z}_p^*$ of integers mod p is cyclic to show that if $p \equiv 1 \pmod 4$ then $n^2 \equiv -1 \pmod p$ for some $n \in \mathbb{Z}$.

   (b) Prove that p cannot be irreducible in $\mathbb{Z}[i]$. (Hint: $p \mid n^2 + 1 = (n + i)(n - i)$.)

   (c) Prove that p is a sum of two squares. (Hint: (b) shows that $p = (a + bi)(c + di)$ with neither factor a unit. Take norms.)

9. Describe all irreducible elements in $\mathbb{Z}[i]$.

10 - 14: Let $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Define $N: \mathbb{Z}[\omega] \to \mathbb{Z}$ by

$$N(a + b\omega) = a^2 - ab + b^2 .$$

10. Show that if $a + b\omega$ is written in the form $u + vi$, where u and v are real, then $N(a + b\omega) = u^2 + v^2$.

11. Show that for all $\alpha, \beta \in \mathbb{Z}[\omega]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using exercise 10. Conclude that if $\alpha | \gamma$ in $\mathbb{Z}[\omega]$, then $N(\alpha) | N(\gamma)$ in $\mathbb{Z}$.

12. Let $\alpha \in \mathbb{Z}[\omega]$. Show that α is a unit iff $N(\alpha) = 1$, and find all units in $\mathbb{Z}[\omega]$. (There are six of them.)

13. Show that $1 - \omega$ is irreducible in $\mathbb{Z}[\omega]$, and that $3 = u(1 - \omega)^2$ for some unit u.

14. Modify exercise 7 to show that $\mathbb{Z}[\omega]$ is a PID, hence a UFD. Here the squares are replaced by parallelograms; one of them has vertices 0, α, $\omega\alpha$, $(\omega + 1)\alpha$, and all others are translates of this one. Use exercise 10 for the geometric argument at the end.

15. Here is a proof of Fermat's conjecture for $n = 4$

If $x^4 + y^4 = z^4$ has a solution in positive integers, then so does $x^4 + y^4 = w^2$. Let x, y, w be a solution with smallest possible w. Then x^2, y^2, w is a primitive Pythagorean triple. Assuming (without loss of generality) that x is odd, we can write

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad w = m^2 + n^2$$

with m and n relatively prime positive integers, not both odd.

(a) Show that

$$x = r^2 - s^2, \quad n = 2rs, \quad m = r^2 + s^2$$

with r and s relatively prime positive integers, not both odd.

(b) Show that r s, and m are pairwise relatively prime. Using $y^2 = 4rsm$, conclude that r, s, and m are all squares, say a^2, b^2, and c^2.

(c) Show that $a^4 + b^4 = c^2$, and that this contradicts minimality of w.

16-28: Let p be an odd prime, $\omega = e^{2\pi i/p}$.

16. Show that

$$(1 - \omega)(1 - \omega^2) \ldots (1 - \omega^{p-1}) = p$$

by considering equation (2).

17. Suppose that $\mathbb{Z}[\omega]$ is a UFD and $\pi | x + y\omega$. Show that π does not divide any of the other factors on the left side of equation (1) by showing that if it did, then π would divide both z and yp (Hint: use 16); but z and yp are relatively prime (assuming case 1), hence $zm + ypn = 1$ for some $m,n \in \mathbb{Z}$. How is this a contradiction?

18. Use 17 to show that if $\mathbb{Z}[\omega]$ is a UFD then $x + y\omega = u\alpha^p$, $\alpha \in \mathbb{Z}[\omega]$, u, a unit in $\mathbb{Z}[\omega]$.

19. Dropping the assumption that $\mathbb{Z}[\omega]$ is a UFD but using the fact that ideals factor uniquely (up to order) into prime ideals, show that the principal ideal $(x + y\omega)$ has no prime ideal factor in common with any of the other principal ideals on the left side of the equation

$$(1') \qquad (x + y)(x + y\omega) \ldots (x + y\omega^{p-1}) = (z)^p$$

in which all factors are interpreted as principal ideals. (Hint: modify the proof of exercise 17 appropriately, using the fact that if A is an ideal dividing another ideal B, then $A \supset B$.)

20. Use 19 to show that $(x + y\omega) = I^p$ for some ideal I.

21. Show that every member of $\mathbb{Q}[\omega]$ is uniquely representable in the form

$$a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{p-2}\omega^{p-2}, \quad a_i \in \mathbb{Q} \quad \forall i$$

by showing that ω is a root of the polynomial

21. (continued)

$$f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1$$

and that $f(t)$ is irreducible over $\mathbb{Q}$. (Hint: It is enough to show that $f(t+1)$ is irreducible, which can be established by Eisenstein's criterion (appendix 1). It helps to notice that $f(t+1) = ((t+1)^p - 1)/t$.)

22. Use 21 to show that if $\alpha \in \mathbb{Z}[\omega]$ and $p|\alpha$, then (writing $\alpha = a_0 + a_1\omega + \ldots + a_{p-2}\omega^{p-2}$, $a_i \in \mathbb{Z}$) all a_i are divisible by p. Define congruence mod p for $\beta, \gamma \in \mathbb{Z}[\omega]$ as follows:

$$\beta \equiv \gamma \pmod{p} \text{ iff } \beta - \gamma = \delta p \text{ for some } \delta \in \mathbb{Z}[\omega].$$

(Equivalently, this is congruence mod the principal ideal $p\,\mathbb{Z}[\omega]$.)

23. Show that if $\beta \equiv \gamma \pmod{p}$, then $\bar{\beta} \equiv \bar{\gamma} \pmod{p}$ where the bar denotes complex conjugation.

24. Show that $(\beta + \gamma)^p \equiv \beta^p + \gamma^p \pmod{p}$ and generalize this to sums of arbitrarily many terms by induction.

25. Show that $\forall\, \alpha \in \mathbb{Z}[\omega]$, α^p is congruent (mod p) to some $a \in \mathbb{Z}$. (Hint: write α in terms of ω and use 24.)

26-28: Now assume $p \geq 5$. We will show that if $x + y\omega \equiv u\alpha^p \pmod{p}$, $\alpha \in \mathbb{Z}[\omega]$, u a unit in $\mathbb{Z}[\omega]$, x and y integers not divisible by p, then $x \equiv y \pmod{p}$. For this we will need the following result, proved by Kummer, on the units of $\mathbb{Z}[\omega]$:

LEMMA: If u is a unit in $\mathbb{Z}[\omega]$ and $\bar{u}$ is its complex conjugate, then $u/\bar{u}$ is a power of ω. (For the proof, see chapter 2, exercise 12.)

26. Show that $x + y\omega \equiv u\alpha^p \pmod{p}$ implies

$$x + y\omega \equiv (x + y\omega^{-1})\omega^k \pmod{p}$$

26. (continued)

for some $k \in \mathbb{Z}$. (Use the Lemma on units and exercises 23 and 25. Note that $\bar{\omega} = \omega^{-1}$.)

27. Use exercise 22 to show that a contradiction results unless $k \equiv 1 \pmod{p}$. (Recall that $p \nmid xy$, $p \geq 5$, and $\omega^{p-1} + \omega^{p-2} + \ldots + \omega + 1 = 0$.)

28. Finally, show $x \equiv y \pmod{p}$.

29. Let $\omega = e^{2\pi i/23}$. Verify that the product

$$(1 + \omega^2 + \omega^4 + \omega^5 + \omega^6 + \omega^{10} + \omega^{11})(1 + \omega + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11})$$

is divisible by 2 in $\mathbb{Z}[\omega]$, although neither factor is. It can be shown (see chapter 3, exercise 17) that 2 is an irreducible element in $\mathbb{Z}[\omega]$; it follows that $\mathbb{Z}[\omega]$ cannot be a UFD.

30 - 32: R is an integral domain (commutative ring with 1 and no zero divisors).

30. Show that two ideals in R are isomorphic as R-modules iff they are in the same ideal class.

31. Show that if A is an ideal in R and if αA is principal for some $\alpha \in R$, then A is principal. Conclude that the principal ideals form an ideal class.

32. Show that the ideal classes in R form a group iff for every ideal A there is an ideal B such that AB is principal.