Lecture 8

7.3

This section is another chance for you to learn how to do quotients, only this time with rings and ideals instead of groups and normal subgroups. In fact, the normal subgroup is automatic since a ring R is an abelian group under addition and the non-zero elements of the ring may not form a group at all. The entire ring with identity cannot form a group because 0 has no inverse. In that sense, we abandon the concept of normality and replace it with the idea of ideal, which is a subring of R that has added properties, namely, closure by multiplication by elements of R on both the left and the right. In the same way all normal subgroups are kernels of group homomorpmisms, all ideals are kernels of ring homomorphisms.

Once we find out how to make quotient rings, all the same theorems go through with only having to check out the multiplication property of the proposed homomorphism. So the proofs of the various isomorphism theorems are omitted as they basically follow from the one given for the first isomorphism theorem.

Note that, since for a group homomorphism $\ker\phi = \{0\} \iff \phi$ is a injective, the same is true for a ring homomophism because all the proof uses in the group structure. Similarly, since all the subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ we need only see that $mn = nm \in m\mathbb{Z}$ to know that all the ideals are $n\mathbb{Z}$. Therefore, (exercise 7.3.3) the only homomorphic images of $\mathbb{Z}$ are $\mathbb{Z}/n\mathbb{Z}$.

Please use the exercises in this section to solidify your understanding of quotients. As usual, I will do some of the unassigned problems to help you learn.

7.3.6a: Define $\phi : M_2(\mathbb{Z}) \to \mathbb{Z}$ by $\phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a$. ϕ is not a homomorphism because $\phi(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2) = \phi(\begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}) = 10 \neq 1 \cdot 1 = \phi(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix})^2$.

7.3.6b: Define $\phi : M_2(\mathbb{Z}) \to \mathbb{Z}$ by $\phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a + d$. ϕ is not a homomorphism because $\phi(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2) = \phi(\begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}) = 29 \neq 5^2 = \phi(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix})^2$.

7.3.6b: $\phi : M_2(\mathbb{Z}) \to \mathbb{Z}$ by $\phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$. ϕ is not a homomorphism because $\phi(2\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}) = \phi(\begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}) = -8 \neq -4 = 2\phi(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix})$.

7.3.11: Let R be the ring of continuous real valued functions on the closed interval $[0, 1]$. Define $\phi :\to \mathbb{R}$ by $\phi(f) = \int_0^1 f(t)dt$. Since $\int_0^1 (f(t) + g(t))dt = \int_0^1 f(t)dt + \int_0^1 g(t)dt$, ϕ is a group homomorphism. But $\phi((t + 1)(t - 1) = \int_0^1 (t+1)(t-1)dt = \int_0^1 (t^2 - 1)dt = t^3/3 - t]_0^1 = 1/3 - 1 = -2/3$, $\int_0^1 (t+1)dt = t^2/2 + t]_0^1 = 1/2 + 1 = 3/2$, and $\int_0^1 (t - 1)dt = t^2/2 - t]_0^1 = 1/2 - 1 = -1/2$. Thus $\phi(t + 1)\phi(t - 1) = 3/2(-1/2) = -3/4 \neq -2/3$. Therefore ϕ is not a ring homomorphism.

7.3.19: Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals of a ring R. Let $I = \bigcup_1^\infty I_i$. Since $I_1 \subseteq I$, I is not empty. Let $a, b \in I$, $r \in R$. Then there exist positive intergers i, j such that $a \in I_i$ and $b \in I_j$. Without loss of generality, we may assume $i \geq j$, so $a, b \in I_i$. Since I_i is an ideal, for $r \in R$, $a - b, ra, ar \in I_i \subseteq I$. Therefore I is an ideal.

7.3.23: Let S be a subring of R. Let$I$ be an ideal of R such that $S \cap I = \{0\}$. Let $\pi : R \to R/I$ be the standard epimorphism. Then $\pi|_S(S) = \overline{S}$ is an epimorphism by definition, where $\pi|_S$ is the restriction of π to S. Let $s \in \ker(\pi|_S)$, then $\overline{0} = \pi|_S(s) = \pi(s)$, so $s \in I$. But $S \cap I = \{0\}$, thus $s = 0$ and $\pi|_S$ is an isomorphism. Therefore $\overline{S} \cong S$.

7.3.25: Assume R is a commutative ring with 1. First we need a Lemma.

Lemma: $\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}$.

Proof: $\binom{n-1}{i-1} + \binom{n-1}{i} = (n - 1)!/((i - 1)!(n - i)!) + (n - 1)!/(i!(n - i - 1)!) = [(n - 1)!/(i!)(n - i)!][i + n - i] = n!/(i!(n - i)!) = \binom{n}{i}$.

Proof of the Binomial Theorem: We proceed by induction on n. If $n = 1$, then $(a + b)^1 = a + b = \binom{1}{0}a + \binom{1}{1}b$. If $n = 2$, then $(a + b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2$. Assume that $(a + b)^{i-1} = \Sigma_{k=0}^{i-1}\binom{i-1}{k}a^k b^{i-1-k}$.

Then $(a+b)^i = (a+b)(a+b)^{i-1} = (a+b)(\Sigma_{k=0}^{i-1}\binom{i-1}{k}a^kb^{i-1-k}) = \Sigma_{k=0}^{i-1}\binom{i-1}{k}a^{k+1}b^{i-1-k}$ $+ \Sigma_{k=0}^{i-1}\binom{i-1}{k}a^kb^{i-k} = \Sigma_{j=1}^{i-1}\binom{i-1}{j-1}a^jb^{i-j} + \binom{i}{i}a^i + \Sigma_{k=0}^{i-2}\binom{i-1}{k}a^kb^{i-k} + \binom{i-1}{i-1}b^i =$ $\binom{i}{0}a^i+\Sigma_{j=1}^{i-1}\binom{i-1}{j-1}a^jb^{i-j}\Sigma_{j=1}^{i}\binom{i-1}{j}a^jb^{i-j}+\binom{i}{i}b^i = \binom{i}{0}a^i+\Sigma_{j=1}^{i-1}(\binom{i-1}{j-1}+\binom{i-1}{i})a^ib^{i-j}+$ $\binom{i}{i}b^i = \Sigma_{j=0}^{i}\binom{i}{j}a^ib^{i-j}$. By induction, the Binomial Theorem is now proven.

7.3.29: Let R be a commutative ring. Let S be the set of nilpotent elements of R, *i.e.*, $S = \{x \in R | x^n = 0$ for some $n \in \mathbb{Z}^+$. $0 \in S$ so S is not empty. Suppose $a, b \in S$. Then there exists $m, n \in \mathbb{Z}^+$ such that $a^m = 1 = b^n$. Thus, by 7.3.25 just done, $(a-b)^{m+n} = \Sigma_{i=0}^{m+n}\binom{m+n}{i}(-1)^{m+n-i}a^ib^{m+n-i} = \Sigma_{i=0}^{m-1}\binom{m+n}{i}(-1)^{m+n-i}a^ib^{m+n-i} + \Sigma_{i=m}^{m+n}\binom{m+n}{i}(-1)^{m+n-i}a^ib^{m+n-i} = 0+0 = 0$. Therefore $a - b \in S$. Let $a \in S$ and $r \in R$. Then $(ra)^m = r^m a^m = r^m \cdot 0 = 0$ and $ra \in S$. Therefore, S is an ideal of R called the nilradical of F and denoted by $\mathcal{N}(R)$.

7.3.30: Suppose R is a commutative ring and let $\mathcal{N}(R)$ be the nilradical of R. Let $\overline{a}$ be nilpotent in $R/\mathcal{N}(R)$. Then there exists a positive integer n such that $\overline{a}^n = \overline{0}$. This is equivalent to $a^n \in \mathcal{N}(R)$, whence there is an m such that $(a^n)^m = 0$. So $a \in \mathcal{N}(R)$, and $\overline{a} = \overline{0}$. Therefore, $\overline{0}$ is the only nilpotent element of $R/\mathcal{N}(R)$.

7.3.31: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2$. But $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Since $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2n+1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2n} = I$. Thus $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not nilpotent and the set of nilpotents in $M_2(R)$ is not an ideal.

7.4

For those of you unacquainted with Zorn's Lemma, please read the discussion in Appendix 1, pages 907-909. The fun part is that Zorn's Lemma is not really a Lemma but is equivalent to a lot of other equivalent things that we use every day such as the Axiom of Choice and the Well-ordering Principle of the positive integers. It's called a Lemma because it was proven from these before it was known that these were all equivalent and unprovable from the axioms of set theory we use. In algebra, Zorn's lemma is very useful as it is a way to show that a maximal element exists, possibly more that one, but at least one. The process usually uses set inclusion for the partial ordering. A chain, then, is simply $A_1 \subseteq A_2 \subseteq \cdots$. This proof part comes in showing that $\bigcup A_i$ has the desired property that all the A_i share. Once that is done, we invoke Zorn's Lemma which says that, if every chain in the partially order set has an upper bound in the set, then the set has a maximal element. In this section, this technique is used to show that a ring with identity has a maximal ideal.

The idea of prime ideal is one that surprises people, but as the book notes, it gets its name from the property of prime numbers that, if p divides ab, then p divides a or p divides b, where p is a prime number.

Please notice that a lot of the propositions in this section require the ring to be commutative. For all the problems in this section, we assume that the ring R has an identity $1 \neq 0$.

7.4.5: Here we do not assume a ring R is commutative. Suppose M is an ideal of R such that R/M is a field. Let $M \subseteq I \subset R$. Note that $I \neq R$ by assumption, so there exists $r \in R$ such that $r \notin I$. Since R/M is a field, $\overline{I} = \overline{0}$ or R/M. If $\overline{I} = R/M$, then $\overline{r} \in \overline{I}$, so there exists $m \in M$ such that $m + r \in I$, whence $r \in I$ since $m \in I$. Contradiction. Therefore, $\overline{I} = \overline{0}$ and $I = M$. Thus, M is maximal.

7.4.8: Let R be an integral domain. Suppose that $< a >=< b >$ for some $a, b \in R$. Then $a = ub$ and $b = va = vub$ for some $u, v \in R$. Thus $vu = 1$ and u, v are units of R. Conversely, if $a = ub$ where u is a unit in R, then $rb = ru^{-1}a \in< a >$, so $< b >\subseteq< a >$. Similarly, for $ra \in< a >$, $ra = rub \in< b >$. Therefore, $< a >=< b >$.

7.4.11: Suppose R is commutative, and P is a prime ideal which contains no zero divisors. Suppose $a \neq 0$ and that $ab = 0$. Then $ab \in P$, whence $a \in P$ or $b \in P$. But P contains no zero divisors, so $b = 0$ and R is an integral domain.

7.4.13: Let $\phi : R \to S$ be a homomorphism of commutative rings.

7.4.13a: Suppose P is a prime ideal of S and $\phi^{-1}(P) \neq R$. Suppose $ab \in \phi^{-1}(P)$. Then $\phi(ab) = \phi(a)\phi(b) \in P$. Thus $\phi(a) \in P$ or $\phi(b) \in P$, whence $a \in \phi^{-1}(P)$ or $b \in \phi^{-1}(P)$. Therefore $\phi^{-1}(P)$ is a prime ideal of R.

Now assume that R is a subring of S and ϕ is the inclusion homomorphism.

Then $\phi^{-1}(P)$ is either R or a prime ideal of R. But $\phi^{-1}(P)$=$P \cap R$, so $P\cap$ is R or a prime ideal of R.

7.4.13b: Suppose M is a maximal ideal of S and ϕ is surjective. By part a, $\phi^{-1}(M)$ is R or a prime ideal of R. Since ϕ is surjective, $\phi^{-1}(M) \neq R$. Suppose $\phi^{-1}(M) \subseteq I \subset R$. Then $M \subseteq \overline{I} \subseteq S$. But M is maximal, so $\overline{I} = S = \phi(R)$ or $\overline{I} = M$. Since $I \neq R$, there exists $r \in R$, $r \notin I$. If $\overline{I} = S$, then $\overline{r} = \overline{i}$, so $r = i + m \in I$ for some $m \in M$. Contradiction. Therefore $\overline{I} = M$. Since $\phi^{-1}(M)$ contains $\ker \phi$, $\phi^{-1}(M) = I$ and $\phi^{-1}(M)$ is maximal in R.

Let $\phi : \mathbb{Z} \to \mathbb{Q}$ by $\phi(n) = n$, the inclusion map. ϕ is not surjective since $1/2$ is not in the image. Since $\mathbb{Q}$ is a field, $\{0\}$ is a maximal ideal. But $\phi^{-1}\{0\} = \{0\}$ is not maximal since it is contained in $n\mathbb{Z}$ for any n.

7.4.16:Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$. We will use the bar notation for the image in $E/ < x^4 - 16 >$.

7.4.16a: In $E/ < x^4 - 16 >$, $\overline{x^4} = \overline{1}6$. Thus, $\overline{x^8} = \overline{16^2} = \overline{256}$ and $\overline{x^{12}} = \overline{16^3} = \overline{4096}$. Therefore $\overline{7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3} =$ $\overline{7 \cdot 4096x - 11 \cdot 256x + 5 \cdot 16x - 2x^3 + 3} = \overline{28672 - 2816 + 80)x - 2x^3 + 3} =$ $\overline{-2x^3 + 25936x + 3}$.

7.4.16b: $\overline{x - 2} \cdot \overline{(x + 2)(x^2 + 4)} = \overline{x^4 - 16} = \overline{0}$ and $\overline{x + 2} \cdot \overline{(x - 2)(x^2 + 4)} = \overline{x^4 - 16} = \overline{0}$. Since the degree of $x - 2$ and $x + 2$ is 1, $\overline{x - 2} \neq \overline{0}$ and $\overline{x + 2} \neq \overline{0}$. Similarly, since the degree of $(x - 2)(x^+4)$ and $(x + 2)(x^2 + 4)$ is 3, $\overline{(x \pm 2)(x^2 + 4)} \neq \overline{0}$. Therefore, $\overline{x - 2}$ and $\overline{x + 2}$ are zero divisors in $E/ < x^4 - 16 >$.

7.5

Theorem 15 is the main content of this section. Unfortunately, the book does not prove the theorem, probably because the proof is long, tedious, and straightforward. But that does not excuse them. To make up for it, most of my "lecture" on this section will be giving a complete proof of Theorem 15.

Theorem 15: Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero-divisors, and is closed under multiplication, *i.e.,* for all $a, b \in D$, $ab \in D$. Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring A has the follwoing additional properties.

1. every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$.
2. (uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D are units, in the following sense. Let S be any commutative ring with identity and let $\phi : R \to S$ be any injective ring homomorphism such that $\phi(d)$ is a unit for all $d \in D$. Then there is an injective ring homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \phi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Proof: Let $\mathcal{F} = \{(r,d)|r \in R,\ d \in D\}$. Define the relation $\sim$ on $\mathcal{F}$ by $(r,d) \sim (s,e)$ if and only if $re = sd$. Since $rd = dr$, $\sim$ is reflexive. If $(r,d) \sim (s,e)$, then $re = sd$, so $sd = er$, whence $(s,e) \sim (r,d)$, and $\sim$ is symmetric. Suppose $(r,d) \sim (s,e)$ and $(s,e) \sim (t,f)$. Then $0 = re - sd = sf - te$. Thus, $0 = ref - sdf = dsf - dte$, whence $ref = dte$. Since $e \in D$, e is not a zero-divisor, so $rf = dt$ and $(r,d) \sim (t,f)$. Therefore, $\sim$ is transitive, whence an equivalence relations.

Let $Q = \mathcal{F}/\sim$ and denote (r,d) by r/d. Thus $r/d = \{(a/b \mid a \in R, b \in D,\ rb = ad\}$. Note that $r/d = re/de$ for all $e \in D$ since D is closed under multiplication. To make Q into a ring we need to define addition and multiplication. Since we are basing our construction on the rational numbers, let's define addition and multiplication similarly. For $a/b,\ c/d \in Q$, define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Note that we used the fact that D is multiplicatively closed in these definitions.

Now we need to show that our definitions are well-defined. Suppose $\frac{a}{b} = \frac{s}{t}$ and $\frac{c}{d} = \frac{u}{v}$. Then $at = bs$ and $cv = du$. To see that $\frac{ad+bc}{bd} = \frac{sv+tu}{tv}$, we need only show that $(ad+bc)tv = (sv+tu)bd$. Then $adtv + bctv = bsdv + dubt = (sv+uc)dt$ as required. Similarly $\frac{ac}{bd} = \frac{su}{tv}$ if and only if $actv = bdsu$. But $actv = bcst = bsdu$. Therefore addition and multiplication are well-defined.

$$\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}\frac{cf+de}{df}=\frac{adf+bcf+bde}{bdf}=\frac{ad+bc}{bd}+\frac{e}{f}=(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}$$

Therefore addition is associative.

$$\frac{a}{b}+\frac{c}{d}=\frac{(ad+bc)}{bd}=\frac{(cb+da)}{db}=\frac{c}{d}+\frac{a}{b}$$

Therefore addition is commutative.

Since $\frac{a}{b}=\frac{ae}{be}=\frac{a}{b}\frac{e}{e}$, $\frac{e}{e}$ is the identity for any $e\in D$.

Since $\frac{a}{b}+\frac{0}{c}=\frac{(ac+0b)}{bc}=\frac{ac}{bc}=\frac{a}{b}$, $\frac{0}{c}$ is the additive inverse of $\frac{a}{b}$ for any $c\in D$. Therefore Q is an additive group.

$$\frac{a}{b}(\frac{c}{d}\frac{e}{f})=\frac{a}{b}\frac{ce}{df}=\frac{ace}{bdf}=\frac{ac}{bd}\frac{e}{f}=(\frac{a}{b}\frac{c}{d})\frac{e}{f}$$

Therefore, multiplication is associative.

Since $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\frac{a}{b}$, multiplication is commutative and we need only check one of the distributive laws.

$$\frac{a}{b}(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}\frac{(cf+de)}{df}=\frac{a(cf+de)}{bdf}=\frac{acf+ade}{bdf}=\frac{abcf+abde}{b^2df}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}$$

Therefore Q is a commutative ring with identity.

Define $i:R\to Q$ by $i(r)=\frac{rd}{d}$ for some $d\in D$. Then $i(r+s)=\frac{(r+s)d}{d}=\frac{(rd+sd)d}{d^2}=\frac{rd}{d}+\frac{sd}{d}=i(r)+i(s)$. Also, $i(rs)=\frac{rsd}{d}=\frac{rsd^2}{d^2}=\frac{r}{d}\frac{s}{d}=i(r)i(s)$. Therefore i is a homomorphism. If $\frac{0}{d}=i(r)=\frac{rd}{d}$, then $0=0\cdot d=rd^2$. Since d is not a zero-divisor, neither is d^2. Thus $r=0$ and i is injective.

Let $d,e\in D$. The $\frac{de}{e}\frac{e}{de}=\frac{de}{de}$, the identity. Thus each $d\in D$ has an inverse in Q, whence each element of Q can be written as rd^{-1} with $r\in R,\ d\in D$.

It remains to prove the uniqueness property. Let S be a commutative ring with identity, and let $\phi:R\to S$ be a monomorphism such that $\phi(d)$ is a unit in S for all $d \in D$. Then define $\Phi(rd^{-1}) = \phi(r)\phi(d)^{-1}$. If $rd^{-1} = se^{-1}$, then in R, $re = sd$. Thus $\phi(r)\phi(e) = \phi(re) = \phi(sd) = \phi(s)\phi(d)$, whence $\phi(r)\phi(d)^{-1} = \phi(s)\phi(e)^{-1}$. Therefore Φ is well-defined.

$\Phi(rd^{-1} + se^{-1}) = \Phi((re + sd)(de)^{-1}) = \phi(re + sd)\phi(de)^{-1} = (\phi(re) + \phi(sd))\phi(d)^{-1}\phi(e)^{-1} = (\phi(r)\phi(e) + \phi(s)\phi(d))\phi(d)^{-1}\phi(e)^{-1} = \phi(r)\phi(d^{-1}) + \phi(s)\phi(e)^{-1} = \Phi(rd^{-1}) + \Phi(se^{-1})$. Also, $\Phi((rd^{-1})(se^{-1})) = \Phi(rs(de)^{-1}) = \phi(rs)\phi(de)^{-1} = \phi(r)\phi(d)^{-1}\phi(s)\phi(e^{-1}) = \Phi(rd^{-1})\Phi(se^{-1})$. Therefore, Φ is a homomorphism. If $0 = \Phi(rd^{-1}) = \phi(r)\phi(d^{-1})$, then $0 = \phi(r)$, whence $r = 0$. Therefore Φ is a monomorhpism as required.

Actually, the above is problem 7.5.1.

7.5.2: Let R be an integral domain, and let D be a non-empty subset of R that is closed under multiplication. Define $i : D^{-1}R \to Q$, where Q is the field of fractions of R, by $i(rd^{-1}) = rd^{-1}$ under the isomorphism which identifies R with its isomorphic image in Q. By definition of addition and multiplication in Q, i is a homomorphism. If $0 = i(rd^{-1}) = rd^{-1}$, then $r = 0$, whence $0d^{-1} = 0$. Thus i is injective. So $D^{-1}R$ is isomorphic to a subring of a field, whence an integral domain.